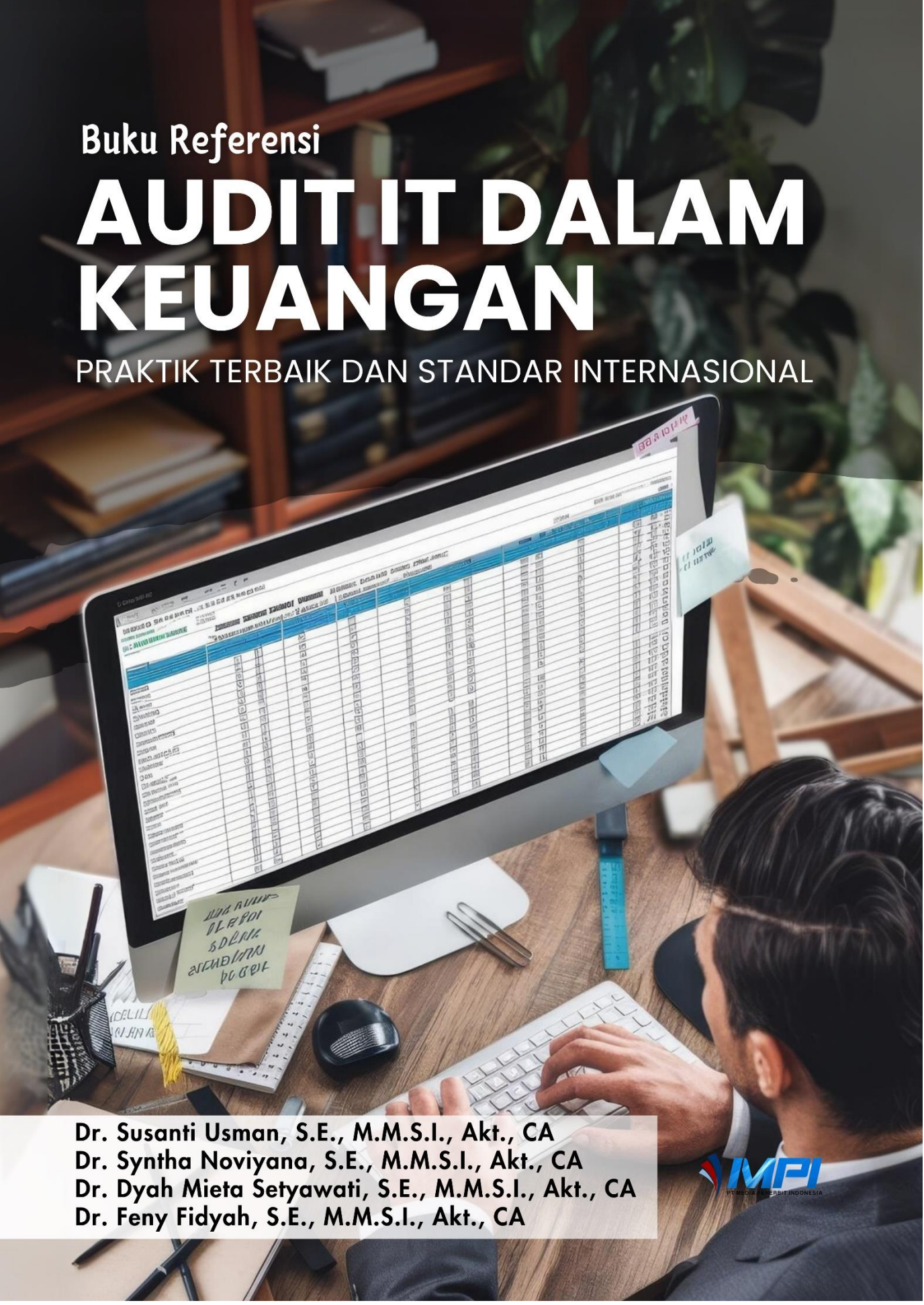
Buku Referensi

AUDIT IT DALAM KEUANGAN

PRAKTIK TERBAIK DAN STANDAR INTERNASIONAL



Dr. Susanti Usman, S.E., M.M.S.I., Akt., CA
Dr. Syntha Noviyana, S.E., M.M.S.I., Akt., CA
Dr. Dyah Mieta Setyawati, S.E., M.M.S.I., Akt., CA
Dr. Feny Fidyah, S.E., M.M.S.I., Akt., CA

MPI
PT MEDIA PENERBIT INDONESIA

BUKU REFERENSI

AUDIT IT DALAM KEUANGAN

PRAKTIK TERBAIK DAN STANDAR INTERNASIONAL

Dr. Susanti Usman, S.E., M.M.S.I., Akt., CA
Dr. Syntha Noviyana, S.E., M.M.S.I., Akt., CA
Dr. Dyah Mieta Setyawati, S.E., M.M.S.I., Akt., CA
Dr. Feny Fidyah, S.E., M.M.S.I., Akt., CA

IMPI
PT MEDIA PENERBIT INDONESIA

AUDIT IT DALAM KEUANGAN

PRAKTIK TERBAIK DAN STANDAR INTERNASIONAL

Ditulis oleh:

Dr. Susanti Usman, S.E., M.M.S.I., Akt., CA
Dr. Syntha Noviyana, S.E., M.M.S.I., Akt., CA
Dr. Dyah Mieta Setyawati, S.E., M.M.S.I., Akt., CA
Dr. Feny Fidyah, S.E., M.M.S.I., Akt., CA

ISBN: 978-634-7012-64-7
IV + 212 hlm; 18,2 x 25,7 cm.
Cetakan I, Januari 2025

Desain Cover dan Tata Letak:
Ajrina Putri Hawari, S.AB.

Diterbitkan, dicetak, dan didistribusikan oleh
PT Media Penerbit Indonesia
Royal Suite No. 6C, Jalan Sedap Malam IX, Sempakata
Kecamatan Medan Selayang, Kota Medan 20131
Telp: 081362150605
Email: ptmediapenerbitindonesia@gmail.com
Web: https://mediapenerbitindonesia.com
Anggota IKAPI No.088/SUT/2024

KATA PENGANTAR

Di era digitalisasi yang berkembang pesat, informasi teknologi menjadi bagian integral dari sistem keuangan global. Perkembangan ini memberikan banyak peluang, seperti efisiensi operasional, transparansi, dan peningkatan kualitas layanan. Namun, meluasnya penggunaan TI juga membawa tantangan, termasuk risiko keamanan data, ancaman terhadap regulasi, dan pengelolaan risiko teknologi. Oleh karena itu, peran audit TI menjadi sangat penting untuk memastikan bahwa informasi teknologi yang digunakan dalam proses keuangan dapat mendukung tujuan strategi organisasi, sesuai dengan standar internasional dan praktik terbaik yang berlaku.

Buku referensi ini membahas berbagai aspek penting dalam audit TI pada sektor keuangan, mulai dari kerangka kerja dasar, metodologi audit, hingga standar internasional yang diakui, seperti COBIT, ISO 27001, dan ITIL. Selain itu, buku referensi ini juga membahas praktik terbaik dalam mengelola keamanan informasi, menilai efektivitas kontrol internal, dan memitigasi risiko yang berhubungan dengan TI. Setiap bab dirancang untuk memberikan pemahaman yang mendalam dan aplikatif, sehingga pembaca dapat mengintegrasikan prinsip-prinsip audit TI ke dalam operasional keuangan.

Semoga buku referensi ini dapat memberikan manfaat yang luas serta menjadi bagian dari upaya bersama untuk meningkatkan tata kelola TI dan sistem keamanan informasi dalam sektor keuangan.

Salam Hangat,

Penulis

DAFTAR ISI

BAB I
PENDAHULUAN AUDIT IT DALAM KEUANGAN

Audit IT dalam sektor keuangan semakin penting seiring dengan pesatnya perkembangan teknologi informasi yang mempengaruhi hampir seluruh aspek operasional lembaga keuangan. Teknologi digital telah membawa perubahan besar dalam cara pengelolaan data dan transaksi keuangan, tetapi juga membawa risiko terkait dengan keamanan, privasi, dan integritas data. Audit IT dalam keuangan tidak hanya melibatkan pemeriksaan terhadap perangkat keras dan perangkat lunak, tetapi juga evaluasi terhadap kontrol internal dan prosedur yang diterapkan untuk melindungi data sensitif dan mencegah potensi kecurangan. Dalam dunia yang semakin digital, lembaga keuangan harus menghadapi tantangan seperti serangan siber, pelanggaran data, dan ancaman terhadap sistem yang dapat merusak reputasi serta stabilitas finansial.

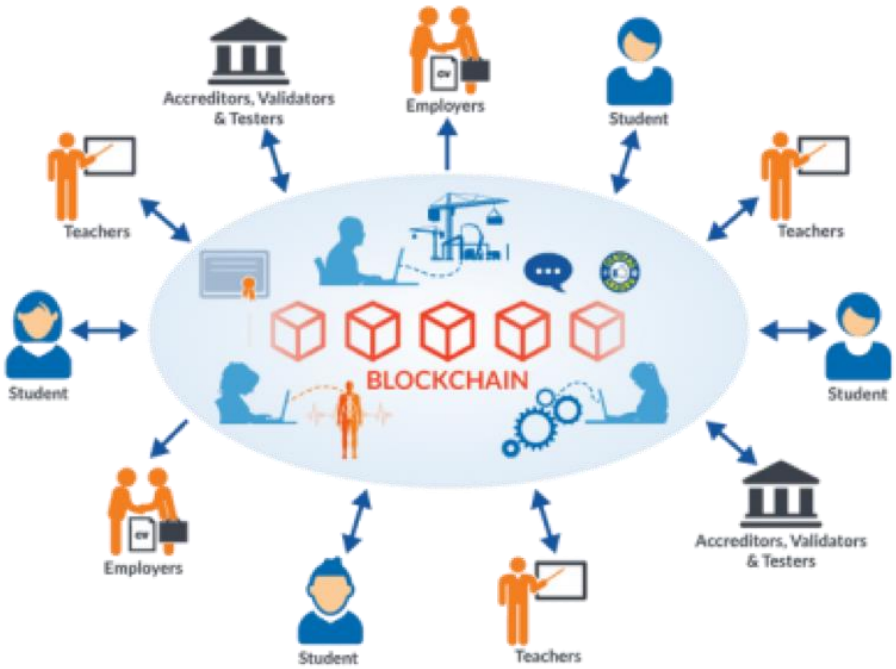
A. Definisi Audit IT dan Relevansinya dalam Sektor Keuangan

Audit Teknologi Informasi (IT) adalah proses sistematis yang dirancang untuk mengevaluasi infrastruktur, kebijakan, dan operasi TI guna memastikan efektivitas, efisiensi, dan keamanan sistem informasi yang mendukung aktivitas organisasi. Audit IT mencakup penilaian risiko, pengujian kontrol internal, dan verifikasi kepatuhan terhadap regulasi yang berlaku, seperti GDPR atau *Sarbanes-Oxley Act.* Dalam konteks keuangan, audit IT menjadi komponen vital karena sistem keuangan modern sangat bergantung pada teknologi digital, seperti transaksi perbankan elektronik, analisis big data, hingga *blockchain*. Audit IT memastikan integritas data, melindungi aset digital, dan mendukung pengambilan keputusan berbasis data yang andal.

1. Peran Sentral Teknologi dalam Industri Keuangan

Teknologi telah merubah secara signifikan cara sektor keuangan beroperasi, terutama dalam hal sistem pembayaran elektronik, transaksi daring, dan penggunaan *blockchain*. Inovasi-inovasi ini memungkinkan lembaga keuangan untuk mempercepat transaksi, mengurangi biaya operasional, dan meningkatkan aksesibilitas bagi pelanggan. Teknologi ini, meskipun memberikan banyak keuntungan, juga membawa tantangan dalam hal keandalan dan keamanan sistem, yang menjadikan audit IT sangat penting.

Gambar 1. *Blockchain*



Sumber: *Filsafat Teknologi*

Audit IT berfungsi untuk memastikan bahwa teknologi yang diterapkan dalam sektor keuangan berjalan dengan baik dan aman. Misalnya, dalam sistem pembayaran digital, audit dapat membantu mendeteksi kelemahan yang dapat menimbulkan kerugian finansial, baik akibat kesalahan sistem maupun potensi manipulasi oleh pihak yang tidak bertanggung jawab.

2. Meningkatnya Risiko Keamanan Siber

Mengingat pentingnya perlindungan data pelanggan dan aset digital, keamanan siber menjadi prioritas utama bagi lembaga keuangan.

Serangan siber dapat mengancam integritas sistem dan merusak reputasi perusahaan. Oleh karena itu, audit IT menjadi krusial untuk mengidentifikasi potensi kerentanannya dan mengurangi risiko yang terkait dengan ancaman eksternal dan internal (Camillo, 2017). Audit IT yang dilakukan secara rutin dapat membantu mendeteksi aktivitas mencurigakan dalam sistem, seperti yang terlihat pada analisis log server. Dengan mengidentifikasi pola yang tidak biasa atau anomali dalam data, auditor dapat mendeteksi potensi serangan atau pelanggaran data yang mungkin terjadi.

3. Kepatuhan terhadap Regulasi

Sektor keuangan tunduk pada berbagai regulasi yang mengatur pengelolaan data dan perlindungan privasi pelanggan, seperti *General Data Protection Regulation* (GDPR) di *Uni Eropa dan California Consumer Privacy Act* (CCPA) di AS. Regulasi ini menetapkan standar yang ketat terkait dengan pengelolaan informasi sensitif dan mewajibkan lembaga keuangan untuk menjaga keamanan dan privasi data pelanggan. Kepatuhan terhadap regulasi ini sangat penting untuk menghindari denda yang besar dan kerusakan reputasi yang dapat merugikan organisasi dalam jangka panjang.

Gambar 2. *General Data Protection Regulation*

Sumber: *Delta Gap*

Audit IT berperan yang sangat penting dalam memastikan kepatuhan terhadap regulasi tersebut. Menurut Safitri *et al*. (2021), audit IT dapat membantu organisasi mengidentifikasi potensi pelanggaran, seperti kegagalan dalam mengenkripsi data pelanggan, serta memberikan rekomendasi untuk perbaikan. Audit yang efektif membantu organisasi menilai apakah kontrol keamanan memadai dan apakah data pribadi dikelola sesuai dengan peraturan yang berlaku,

sehingga mengurangi risiko hukum dan memastikan kepercayaan pelanggan tetap terjaga.

4. Mitigasi Risiko Operasional

Kesalahan atau gangguan dalam sistem TI dapat menyebabkan dampak yang signifikan bagi operasional lembaga keuangan, seperti gangguan dalam proses pembayaran yang menghambat transaksi pelanggan dan merusak reputasi organisasi. Audit IT berfungsi untuk mendeteksi potensi masalah ini sejak dini, sehingga langkah-langkah pencegahan atau perbaikan dapat dilakukan sebelum gangguan tersebut berdampak besar. Dengan pemantauan dan evaluasi yang dilakukan selama audit, kelemahan atau ketidaksesuaian dalam sistem dapat diidentifikasi, yang memungkinkan organisasi untuk mengambil tindakan proaktif untuk mencegah insiden yang merugikan.

5. Mendukung Transparansi dan Akuntabilitas

Audit IT berperan penting dalam meningkatkan transparansi dan akuntabilitas dalam pengelolaan data keuangan. Sistem informasi yang diaudit secara berkala cenderung lebih sesuai dengan standar akuntabilitas yang diharapkan oleh pemangku kepentingan, termasuk investor, regulator, dan pelanggan. Audit membantu memastikan bahwa semua transaksi dan data keuangan tercatat dengan benar, serta bahwa kebijakan dan prosedur yang ada dipatuhi dengan ketat. Hal ini memberikan rasa aman bagi pemangku kepentingan karena dapat yakin bahwa organisasi beroperasi dengan cara yang sesuai dengan prinsip transparansi dan akuntabilitas.

B. Peran Teknologi dalam Sistem Keuangan Modern

Peran teknologi dalam sektor keuangan modern tidak hanya terbatas pada mendukung operasional bisnis tetapi juga menjadi penggerak utama transformasi industri. Teknologi telah memungkinkan pengembangan sistem pembayaran digital, layanan perbankan tanpa cabang (*branchless banking*), teknologi *blockchain*, dan integrasi kecerdasan buatan (AI) dalam analisis data keuangan. Transformasi ini tidak hanya meningkatkan efisiensi operasional tetapi juga menghadirkan tantangan baru, seperti risiko keamanan siber, perlindungan data, dan kepatuhan terhadap regulasi yang kompleks.

Teknologi telah memampukan institusi keuangan untuk mengakses pasar global dengan lebih mudah, mengurangi biaya transaksi, dan memberikan layanan yang lebih personal kepada konsumen. Namun, kemajuan ini juga membutuhkan pengawasan yang ketat melalui audit IT untuk memastikan keandalan dan keamanan sistem tersebut.

1. Digitalisasi Perbankan dan Layanan Keuangan

Digitalisasi dalam sektor perbankan telah membawa perubahan signifikan dalam cara layanan keuangan disampaikan kepada pelanggan. Perbankan digital memungkinkan nasabah untuk melakukan transaksi, mengakses laporan keuangan, dan mengelola investasi melalui platform *online* tanpa harus mengunjungi cabang fisik. Aplikasi seperti Revolut dan Monzo telah memimpin dalam menyediakan layanan perbankan sepenuhnya berbasis aplikasi, memungkinkan transaksi lebih cepat dan akses ke berbagai produk keuangan dari *smartphone* (Karim *et al*., 2023). Selain itu, manajemen risiko digital menjadi fokus utama dalam perbankan modern. Bank kini memanfaatkan perangkat lunak analitik untuk memantau dan mendeteksi pola-pola risiko secara *real-time*, membantu dalam pencegahan penipuan dan meningkatkan keamanan transaksi. Teknologi ini memungkinkan bank untuk mengidentifikasi potensi ancaman lebih cepat, memastikan pengalaman yang lebih aman bagi pelanggan dan mengurangi risiko kerugian finansial.

2. Sistem Pembayaran Digital

Sistem pembayaran digital, yang mencakup teknologi seperti QR *code, mobile payment*, dan dompet digital, telah mengubah cara konsumen melakukan transaksi. Teknologi ini memfasilitasi transaksi yang cepat, efisien, dan lebih murah, serta mendukung inklusi keuangan dengan memberikan akses yang lebih mudah ke layanan keuangan bagi yang sebelumnya tidak terjangkau oleh perbankan tradisional. Misalnya, penggunaan QR *code* memungkinkan pembayaran instan di berbagai titik penjualan tanpa perlu kartu fisik, sementara dompet digital seperti Apple Pay dan Google Wallet memberikan kemudahan transaksi hanya melalui *smartphone*. Hal ini membantu mempercepat transaksi sehari-hari dan mengurangi ketergantungan pada uang tunai.

Dengan semakin meningkatnya penggunaan sistem pembayaran digital, masalah keamanan menjadi hal yang krusial. Audit IT berperan penting dalam memastikan bahwa sistem ini memenuhi standar

keamanan yang ketat, terutama dalam hal perlindungan data pelanggan. Penggunaan enkripsi data menjadi sangat penting untuk mencegah kebocoran informasi pribadi dan finansial yang dapat berisiko tinggi. Auditor IT melakukan pengecekan terhadap sistem untuk memastikan bahwa kebijakan dan teknologi yang digunakan dalam pengelolaan data pelanggan sudah sesuai dengan regulasi yang berlaku, menjaga integritas dan keamanan transaksi digital.

3. *Blockchain* dan Teknologi Terdesentralisasi

Blockchain telah merevolusi industri keuangan dengan menyediakan sistem yang transparan, aman, dan efisien untuk pengelolaan transaksi tanpa memerlukan perantara. Teknologi ini memungkinkan terciptanya transaksi langsung antar pihak dengan jaminan keabsahan dan keamanan data yang tinggi, mengurangi biaya transaksi, serta meningkatkan efisiensi dalam berbagai aktivitas keuangan. Cryptocurrency, seperti Bitcoin dan Ethereum, adalah contoh penerapan *blockchain* yang paling terkenal. Mata uang kripto ini menggunakan teknologi *blockchain* untuk memastikan bahwa setiap transaksi tercatat secara permanen dan tidak dapat diubah, yang membuatnya lebih aman daripada sistem pembayaran tradisional.

Keuangan Terdesentralisasi (DeFi) mengandalkan teknologi *blockchain* untuk memungkinkan layanan keuangan tanpa lembaga keuangan sentral. DeFi menawarkan berbagai solusi keuangan seperti pinjaman, perdagangan, dan manajemen aset yang dilakukan secara langsung melalui *smart contracts* (kontrak pintar) di *blockchain*. Hal ini memungkinkan pengguna untuk mengakses layanan finansial tanpa perlu melalui perantara seperti bank atau lembaga keuangan lainnya. Pertumbuhan sektor DeFi yang pesat, dengan volume transaksi yang terus meningkat, menunjukkan kepercayaan pasar terhadap potensi teknologi ini dalam menciptakan sistem keuangan yang lebih inklusif dan efisien. *Blockchain* dan DeFi membawa perubahan besar dalam paradigma keuangan tradisional, mendorong adopsi teknologi yang lebih transparan dan terdesentralisasi.

4. Analisis Data Keuangan

Kecerdasan buatan (AI) telah merevolusi cara analisis data keuangan dilakukan, memungkinkan pemrosesan volume data yang sangat besar dengan kecepatan dan akurasi yang jauh melebihi

kemampuan manusia. Teknologi ini digunakan untuk menganalisis tren pasar, memprediksi pergerakan saham, dan melakukan analisis risiko yang lebih mendalam. AI menggabungkan teknik *machine learning* dan *deep learning* untuk mengevaluasi data historis dan mengidentifikasi pola-pola yang sulit terdeteksi oleh metode tradisional. AI juga berperan dalam identifikasi peluang investasi dengan lebih tepat dan efisien. Dengan memanfaatkan data *real-time* dan analisis prediktif, AI membantu investor dan lembaga keuangan membuat keputusan yang lebih informed dalam memilih aset atau mengelola portofolio. Teknologi ini tidak hanya mengurangi potensi kesalahan manusia tetapi juga memungkinkan strategi investasi yang lebih dinamis, beradaptasi dengan cepat terhadap perubahan pasar. Penerapan AI dalam analisis data keuangan terus berkembang dan diperkirakan akan menjadi semakin penting di masa depan, membantu menciptakan sistem keuangan yang lebih transparan dan efisien.

5. Deteksi Penipuan

Kecerdasan buatan (AI) semakin banyak digunakan untuk mendeteksi penipuan dalam sektor keuangan dengan memanfaatkan algoritma pembelajaran mesin yang mampu mengenali pola transaksi yang tidak biasa. Sistem AI ini dilatih dengan data transaksi historis dan dapat menganalisis berbagai jenis pola yang mungkin mengindikasikan potensi penipuan. Misalnya, sistem dapat mendeteksi transaksi yang dilakukan di luar kebiasaan pelanggan, seperti transaksi dengan jumlah besar atau dilakukan di lokasi yang tidak biasa. Dengan memanfaatkan teknik *anomaly detection*, AI dapat memberikan peringatan dini untuk memitigasi risiko penipuan yang lebih besar. Selain itu, AI dapat mempercepat proses identifikasi penipuan dengan memproses data transaksi secara *real-time*. Sebagai contoh, sistem berbasis AI dapat memeriksa ribuan transaksi dalam hitungan detik dan mengidentifikasi aktivitas yang mencurigakan tanpa keterlibatan manusia, yang sebelumnya memerlukan waktu lama untuk dianalisis.

C. Tujuan dan Manfaat Audit IT dalam Keuangan

Audit Teknologi Informasi (IT) dalam sektor keuangan adalah proses evaluasi independen terhadap sistem informasi dan teknologi untuk memastikan bahwa operasionalnya efektif, efisien, aman, dan

sesuai dengan peraturan yang berlaku. Dalam era digital, audit IT tidak hanya bersifat opsional tetapi menjadi komponen esensial dalam tata kelola organisasi keuangan. Tujuan utama audit IT adalah melindungi aset digital, memastikan keberlanjutan operasional, serta menjaga integritas data keuangan. Audit IT memberikan nilai strategis dengan meningkatkan pengawasan risiko teknologi dan mengoptimalkan penggunaan sumber daya teknologi untuk mendukung pertumbuhan organisasi.

1. Tujuan Audit IT dalam Keuangan

a. Menjamin Keamanan Data dan Sistem

Audit IT dalam sektor keuangan memiliki tujuan utama untuk memastikan bahwa data dan sistem informasi terlindungi dengan baik dari berbagai ancaman. Serangan siber, seperti ransomware, kebocoran data, atau peretasan, dapat menyebabkan kerugian finansial yang signifikan, baik dari segi biaya perbaikan maupun reputasi lembaga keuangan. Audit IT berperan untuk mengevaluasi pengaturan dan kebijakan keamanan yang ada, seperti enkripsi data, kontrol akses yang ketat, serta pengelolaan kata sandi yang aman, untuk mencegah kebocoran informasi dan memastikan integritas sistem.

Gambar 3. *Ransomware*

Sumber: *Security Inteligent*

Dengan audit IT, lembaga keuangan dapat mengidentifikasi celah keamanan dalam infrastruktur dan mengimplementasikan tindakan korektif yang diperlukan. Selain itu, audit ini juga membantu memastikan bahwa kebijakan keamanan data selalu diperbarui untuk menghadapi ancaman yang terus berkembang.

Dengan adanya evaluasi yang rutin terhadap sistem keamanan, lembaga keuangan dapat meningkatkan perlindungan terhadap data pelanggan, transaksi, dan aset digital, sekaligus menjaga kepercayaan publik. Pengawasan yang ketat dalam hal ini adalah kunci untuk meminimalkan potensi kerugian yang dapat ditimbulkan oleh serangan siber.

b. Meningkatkan Kepatuhan terhadap Regulasi

Audit IT berperan penting dalam memastikan bahwa lembaga keuangan mematuhi regulasi yang berlaku, seperti GDPR, PCI DSS, dan ISO/IEC 27001, yang mengatur pengelolaan data dan keamanan informasi. Regulasi ini dirancang untuk melindungi data pribadi pelanggan dan menjaga integritas sistem keuangan. Audit IT membantu organisasi untuk memverifikasi bahwa kebijakan dan prosedur yang diterapkan sesuai dengan standar yang ditetapkan oleh badan pengawas. Hal ini tidak hanya penting untuk melindungi informasi sensitif, tetapi juga untuk memastikan keberlanjutan operasional yang sah di pasar yang semakin diawasi ketat (Mondschein & Monda, 2019).

Kepatuhan terhadap regulasi sangat penting bagi lembaga keuangan karena pelanggaran dapat mengakibatkan denda besar yang merugikan. Audit IT membantu organisasi untuk mengidentifikasi dan memperbaiki potensi pelanggaran sebelum terjadinya denda atau reputasi yang rusak. Dengan melakukan audit secara rutin, lembaga keuangan dapat menjaga integritas dan keamanan data, sekaligus menghindari konsekuensi hukum dan finansial dari pelanggaran regulasi.

c. Mengidentifikasi dan Mengelola Risiko Teknologi

Audit IT memiliki tujuan yang sangat penting dalam mengidentifikasi dan mengelola risiko yang terkait dengan penggunaan teknologi dalam sektor keuangan. Salah satu risiko utama yang perlu diperhatikan adalah integrasi perangkat lunak baru ke dalam sistem yang ada, yang dapat mempengaruhi kinerja dan stabilitas operasional. Selain itu, penggunaan teknologi baru, seperti sistem pembayaran digital atau aplikasi perbankan, dapat memperkenalkan celah yang berpotensi digunakan oleh pihak yang tidak bertanggung jawab. Oleh karena itu, audit IT secara rutin diperlukan untuk mengevaluasi efektivitas kontrol yang diterapkan dalam setiap aspek teknologi,

memastikan bahwa sistem berjalan dengan lancar dan aman. Audit IT juga berfungsi untuk mengidentifikasi ancaman yang berasal dari potensi serangan siber dan kegagalan teknis. Audit IT yang dilakukan dengan baik akan mampu mendeteksi potensi kerentanannya lebih awal, memberikan rekomendasi untuk mitigasi, serta membantu manajemen risiko dengan mengelola ancaman yang muncul.

2. Manfaat Audit IT dalam Keuangan

a. Mencegah dan Mengurangi Risiko Penipuan

Audit IT berperan penting dalam mendeteksi dan mencegah aktivitas penipuan dalam sektor keuangan. Melalui pemantauan sistem secara menyeluruh, audit IT dapat mengidentifikasi transaksi yang tidak sah atau adanya manipulasi data, yang sering kali dilakukan oleh pihak internal atau eksternal untuk tujuan pribadi. Dengan teknologi seperti pembelajaran mesin dan analitik data, audit IT dapat mengidentifikasi pola transaksi yang mencurigakan dan memberikan peringatan dini mengenai potensi penipuan. Menurut laporan ACFE *Report to the Nations* (2022), penipuan dalam organisasi dapat merugikan hingga 5% dari pendapatan tahunan, yang menekankan pentingnya penerapan audit IT untuk mengurangi kerugian finansial tersebut.

Audit IT juga berkontribusi dalam memperkuat sistem pengendalian internal yang efektif, yang dapat mencegah praktik penipuan sejak awal. Dengan adanya audit yang teratur dan penilaian sistem TI yang menyeluruh, organisasi dapat meningkatkan deteksi dan pencegahan terhadap berbagai jenis penipuan, baik yang melibatkan pihak internal maupun eksternal. Keberhasilan audit IT dalam mengurangi risiko penipuan tidak hanya melindungi aset organisasi tetapi juga menjaga integritas dan kepercayaan pemangku kepentingan terhadap operasional keuangan.

b. Memastikan Keberlanjutan Bisnis

Audit IT memiliki peran krusial dalam memastikan keberlanjutan bisnis dengan menilai kesiapan teknologi dalam menghadapi potensi gangguan atau bencana. Dalam sektor keuangan, di mana sistem dan data sangat sensitif, keberlanjutan operasional bergantung pada seberapa baik organisasi

merencanakan pemulihan dari gangguan yang tidak terduga, seperti serangan siber atau kegagalan perangkat keras. Audit IT memastikan bahwa organisasi memiliki rencana pemulihan bencana (*disaster recovery plan*) yang komprehensif dan diuji secara teratur.

Dengan melakukan audit terhadap infrastruktur TI dan prosedur pemulihan, organisasi dapat memastikan bahwa dapat kembali beroperasi dengan cepat setelah gangguan, meminimalkan kerugian, dan melindungi reputasinya di mata pelanggan dan pemangku kepentingan. Selain itu, audit IT juga membantu memastikan bahwa data sensitif terlindungi dengan baik dan bahwa sistem yang ada dapat mengatasi ancaman yang mungkin muncul.

c. Meningkatkan Kepercayaan Pemangku Kepentingan

Audit IT yang berhasil dilaksanakan memberikan manfaat besar dalam meningkatkan kepercayaan pemangku kepentingan, termasuk investor, pelanggan, dan regulator. Proses audit yang transparan dan sistematis menunjukkan komitmen organisasi terhadap pengelolaan teknologi yang aman dan efisien. Investor akan lebih percaya untuk berinvestasi di organisasi yang dapat menunjukkan kontrol yang solid atas sistem teknologi, mengurangi risiko terkait dengan kegagalan operasional atau kebocoran data. Selain itu, pelanggan merasa lebih aman ketika tahu bahwa data pribadinya dilindungi dengan standar tinggi, yang juga berdampak positif terhadap retensi dan loyalitas pelanggan.

Bagi regulator, audit IT memberikan keyakinan bahwa organisasi mematuhi regulasi yang berlaku, seperti GDPR atau PCI DSS. Hal ini tidak hanya mengurangi risiko denda dan sanksi, tetapi juga memperkuat citra organisasi sebagai entitas yang bertanggung jawab dalam pengelolaan teknologi. Kepercayaan yang terbangun berkat audit IT ini dapat menghasilkan kemitraan yang lebih kuat, menarik investor baru, dan meningkatkan kredibilitas organisasi di pasar global yang semakin kompetitif.

D. Hubungan antara Audit IT dan Audit Keuangan

Di dunia keuangan modern, audit tidak lagi hanya berfokus pada laporan keuangan semata. Audit IT kini menjadi bagian integral dari proses audit keuangan, karena sistem teknologi informasi (TI) berperan sentral dalam pengelolaan data keuangan dan operasional organisasi. Hubungan antara audit IT dan audit keuangan dapat dilihat dari bagaimana kedua disiplin ini saling melengkapi dalam mengevaluasi integritas, akurasi, dan keamanan data yang digunakan untuk laporan keuangan. Audit keuangan bertujuan untuk memastikan bahwa laporan keuangan organisasi bebas dari salah saji material dan sesuai dengan standar akuntansi yang berlaku. Sementara itu, audit IT fokus pada sistem, proses, dan kontrol teknologi yang mendukung pembuatan laporan keuangan tersebut.

1. Keterkaitan Fungsi Audit IT dan Audit Keuangan

a. Saling Ketergantungan dalam Proses Audit

Audit IT dan audit keuangan memiliki keterkaitan yang erat, terutama dalam konteks laporan keuangan yang kini bergantung pada sistem teknologi informasi (TI) untuk pengelolaan data. Laporan keuangan modern, yang digunakan oleh perusahaan untuk mengambil keputusan bisnis, dihasilkan melalui data yang diproses dan disimpan dalam sistem TI. Tanpa sistem TI yang tepat, validitas data yang ada dalam laporan keuangan bisa dipertanyakan.

b. Penguatan Pengendalian Internal

Audit IT berperan penting dalam penguatan pengendalian internal, yang memastikan bahwa sistem teknologi yang digunakan dalam organisasi mendukung tujuan operasional, pelaporan, dan kepatuhan. Pengendalian internal bertujuan untuk memberikan kepastian yang wajar atas pencapaian tujuan tersebut. Dalam konteks ini, audit IT bertugas untuk memverifikasi apakah kontrol yang ada pada sistem teknologi berfungsi dengan baik, termasuk mekanisme pengamanan data, akses sistem, dan pemantauan aktivitas. Audit ini memastikan bahwa proses dan prosedur yang mendukung laporan keuangan

terkelola dengan baik dan bebas dari potensi kesalahan atau penipuan.

c. Deteksi dan Pencegahan Penipuan Keuangan

Kombinasi audit IT dan audit keuangan berperan penting dalam mendeteksi dan mencegah penipuan keuangan dengan memanfaatkan kekuatan masing-masing. Audit IT dapat memantau dan menganalisis log aktivitas dalam sistem, seperti akses tidak sah atau transaksi mencurigakan yang berpotensi mengindikasikan manipulasi data. Dengan teknologi seperti software pemantauan dan analisis pola, audit IT bisa mendeteksi anomali dalam data yang tidak mudah terlihat dalam audit keuangan tradisional. Sistem ini menyediakan lapisan keamanan tambahan untuk melindungi dari upaya penipuan atau pelanggaran data yang dapat merugikan organisasi.

2. Kontribusi Audit IT terhadap Audit Keuangan

a. Verifikasi Integritas Data Keuangan

Audit IT berkontribusi secara signifikan dalam memastikan integritas data keuangan yang digunakan dalam laporan keuangan organisasi. Salah satu area utama yang diperiksa dalam audit IT adalah aplikasi keuangan, seperti sistem ERP (*Enterprise Resource Planning*). ERP digunakan untuk mengelola berbagai fungsi bisnis, termasuk akuntansi dan pelaporan keuangan, yang sangat bergantung pada data yang dihasilkan oleh sistem ini. Audit IT mengevaluasi kontrol internal yang ada dalam sistem ERP untuk memastikan bahwa data yang dihasilkan akurat, konsisten, dan dapat dipercaya. Hal ini memastikan bahwa informasi yang digunakan dalam laporan keuangan mencerminkan keadaan yang sebenarnya, mengurangi kemungkinan terjadinya kesalahan atau manipulasi data.

b. Pengelolaan Risiko Teknologi yang Mempengaruhi Laporan Keuangan

Audit IT memiliki kontribusi penting dalam pengelolaan risiko teknologi yang dapat memengaruhi laporan keuangan. Salah satu risiko utama yang dapat timbul adalah gangguan sistem yang menghambat proses pencatatan dan pelaporan keuangan. Misalnya, kesalahan dalam algoritma otomatisasi akuntansi dapat menyebabkan perhitungan yang tidak akurat, seperti salah

saji dalam penilaian aset tetap atau kewajiban, yang pada akhirnya memengaruhi integritas laporan keuangan (EY, 2020). Audit IT secara sistematis mengevaluasi desain dan implementasi sistem teknologi untuk mengidentifikasi potensi kesalahan atau kelemahan dalam algoritma yang digunakan dalam proses akuntansi. Dengan cara ini, audit IT memastikan bahwa risiko yang ditimbulkan oleh sistem TI yang tidak tepat dapat diminimalisasi, mencegah dampak negatif pada laporan keuangan.

c. Efisiensi Proses Audit Keuangan

Audit IT memberikan kontribusi signifikan dalam meningkatkan efisiensi proses audit keuangan dengan memastikan keandalan sistem teknologi informasi yang mendukung pengelolaan data keuangan. Dengan adanya audit IT yang efektif, auditor keuangan dapat memfokuskan perhatian pada analisis dan verifikasi data daripada harus memeriksa sistem secara manual. Hal ini tidak hanya menghemat waktu tetapi juga meningkatkan kualitas audit, karena auditor dapat mengidentifikasi potensi masalah lebih cepat melalui teknologi yang lebih canggih.

E. Tantangan Utama dalam Audit IT di Industri Keuangan

Industri keuangan telah menjadi salah satu sektor yang paling bergantung pada teknologi informasi (TI) dalam mengelola data, transaksi, dan operasi harian. Dengan adopsi teknologi seperti *cloud computing*, *blockchain*, kecerdasan buatan (AI), dan sistem pembayaran digital, risiko dan kompleksitas dalam audit IT juga meningkat. Audit IT di sektor keuangan bertujuan untuk memastikan keamanan, integritas, dan keandalan sistem TI yang mendukung laporan keuangan dan operasional. Namun, proses ini dihadapkan pada berbagai tantangan, mulai dari kompleksitas teknologi hingga keterbatasan sumber daya.

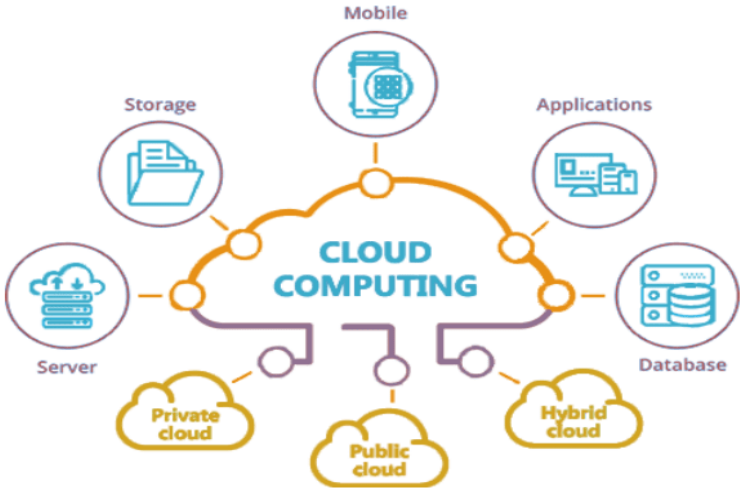
1. Kompleksitas Teknologi dalam Sistem Keuangan

a. Adopsi Teknologi Baru

Industri keuangan kini semakin mengadopsi teknologi canggih seperti *blockchain*, *machine learning*, dan *cloud computing* untuk meningkatkan efisiensi dan menciptakan inovasi. Meskipun teknologi ini membawa manfaat besar, seperti transparansi dan

otomatisasi, juga memperkenalkan tantangan baru dalam hal audit dan kontrol keamanan.

Gambar 4, *Cloud Computing*



Sumber: *Soft Edukasi*

Blockchain, misalnya, meskipun memiliki mekanisme keamanan yang kuat, mempersulit verifikasi transaksi karena sifatnya yang terdesentralisasi dan sulit diubah. Hal ini menimbulkan kesulitan dalam mengidentifikasi penyimpangan atau *fraud* yang mungkin terjadi dalam sistem, terutama ketika data bersifat sangat dinamis dan tersebar (Singh, 2023).

b. Integrasi Sistem Lama dengan Teknologi Baru

Banyak institusi keuangan masih mengandalkan sistem lama (*legacy systems*) yang sudah terpasang sejak lama, namun tetap digunakan karena biaya tinggi untuk mengganti atau memperbaharuinya. Masalah utama muncul ketika sistem ini diintegrasikan dengan teknologi baru, seperti aplikasi berbasis *cloud* atau sistem otomatisasi berbasis AI. *Legacy systems* sering kali tidak kompatibel dengan standar keamanan terbaru dan kurang fleksibel dalam menghadapi perubahan cepat pada infrastruktur teknologi. Hal ini dapat menciptakan celah keamanan yang sulit dideteksi, karena sistem lama tidak dirancang untuk menghadapinya. Kurangnya integrasi yang baik antara sistem lama dan baru dapat menyebabkan masalah signifikan terkait kontrol akses dan enkripsi data.

2. Ancaman Keamanan Siber

a. Meningkatnya Serangan Siber di Industri Keuangan

Industri keuangan menjadi target utama serangan siber karena pengelolaan data sensitif seperti informasi pribadi, rekening, dan transaksi keuangan. Serangan siber, termasuk peretasan, *ransomware*, dan *phishing*, mengancam integritas dan keamanan data, serta dapat merusak reputasi institusi keuangan. Serangan-serangan ini sering kali mengincar celah keamanan dalam sistem, yang jika tidak segera ditangani, dapat mengakibatkan kerugian finansial yang signifikan dan dampak jangka panjang terhadap kepercayaan nasabah.

b. Evaluasi Keamanan Berbasis Data Besar (*Big Data*)

Evaluasi keamanan dalam pengelolaan data besar (*big data*) merupakan tantangan utama dalam audit IT, terutama di sektor keuangan. Data besar mencakup volume informasi yang sangat besar dan bervariasi, seperti transaksi pelanggan, pola perilaku, dan informasi sensitif lainnya. Meskipun teknologi seperti big data menawarkan keuntungan dalam analisis dan pengambilan keputusan, risikonya adalah potensi kebocoran atau penyalahgunaan data tersebut. Audit IT harus memastikan bahwa sistem yang menyimpan, memproses, dan menganalisis data besar dilengkapi dengan mekanisme keamanan yang memadai untuk melindungi data dari akses yang tidak sah.

3. Tantangan Regulasi dan Kepatuhan

a. Regulasi yang Beragam dan Dinamis

Sektor keuangan dihadapkan pada tantangan besar dalam mematuhi regulasi yang beragam dan dinamis, seperti GDPR (*General Data Protection Regulation*) di Uni Eropa, CCPA (*California Consumer Privacy Act*) di AS, dan PSD2 (*Payment Services Directive* 2) untuk sistem pembayaran di Eropa. Regulasi ini sering kali mengharuskan organisasi untuk melakukan penyesuaian cepat dalam sistem teknologi untuk memenuhi standar yang ketat terkait dengan perlindungan data, privasi, dan transparansi. Namun, perubahan regulasi ini seringkali terjadi lebih cepat daripada kemampuan institusi untuk mengadaptasi sistem TI, yang dapat meningkatkan risiko ketidakpatuhan dan potensi denda atau sanksi.

b. Kesulitan dalam Memverifikasi Kepatuhan TI

Verifikasi kepatuhan TI dalam sektor keuangan menjadi tantangan besar bagi auditor karena sistem teknologi yang digunakan sangat kompleks dan tersebar di banyak aplikasi dan server. Institusi keuangan besar sering kali memiliki ribuan perangkat lunak dan sistem yang saling terhubung, yang membuat proses audit lebih sulit. Setiap aplikasi dan server mungkin memiliki kontrol keamanan yang berbeda, serta cara yang berbeda dalam memproses data sensitif, yang memerlukan pendekatan audit yang sangat teliti dan terstruktur. Hal ini memperburuk tantangan dalam memastikan bahwa sistem TI mematuhi berbagai regulasi yang terus berkembang, seperti GDPR, CCPA, atau PSD2.

4. Keterbatasan Sumber Daya dalam Audit IT

a. Kurangnya Tenaga Ahli dalam Audit IT

Kurangnya tenaga ahli dalam bidang audit IT merupakan salah satu tantangan utama yang dihadapi oleh institusi keuangan. Audit IT memerlukan keterampilan khusus yang menggabungkan pemahaman mendalam tentang teknologi informasi dan pengetahuan akuntansi untuk mengidentifikasi dan mengatasi risiko yang mungkin timbul dari penggunaan teknologi dalam laporan keuangan.

b. Keterbatasan Anggaran untuk Audit IT

Banyak organisasi keuangan masih memandang audit IT sebagai biaya tambahan yang tidak langsung berhubungan dengan operasi utama, sehingga sering kali anggaran untuk proses ini terbatas. Hal ini disebabkan oleh persepsi bahwa audit TI tidak memberikan kontribusi langsung terhadap pendapatan atau keuntungan perusahaan, padahal kenyataannya, audit TI memiliki peran krusial dalam memastikan keamanan, integritas data, dan kepatuhan terhadap regulasi yang dapat mempengaruhi kestabilan keuangan organisasi. Ketika anggaran terbatas, banyak organisasi yang terpaksa mengurangi frekuensi atau cakupan audit IT, sehingga meningkatkan risiko terkait dengan potensi kegagalan sistem atau pelanggaran kebijakan.

5. Keandalan dan Validitas Data

a. Volume Data yang Sangat Besar

Institusi keuangan memproses volume transaksi yang sangat besar setiap hari, yang menghasilkan sejumlah besar data yang harus diaudit untuk memastikan akurasi dan integritas. Tantangan utama bagi auditor adalah bagaimana menangani dan mengevaluasi data yang begitu besar dalam waktu yang terbatas. Setiap transaksi, baik itu pembayaran, transfer, atau pembelian, menghasilkan data yang perlu diverifikasi untuk memastikan bahwa tidak ada kesalahan atau manipulasi yang terjadi. Penggunaan teknologi analitik canggih, seperti kecerdasan buatan (AI) dan *machine learning*, dapat membantu mempercepat proses ini, namun tetap ada tantangan besar dalam mengelola dan mengaudit data yang sangat besar dalam jangka waktu yang terbatas.

b. Kualitas Data yang Tidak Konsisten

Kualitas data yang tidak konsisten sering kali menjadi tantangan utama dalam proses audit, terutama ketika sistem TI yang digunakan oleh institusi keuangan tidak terintegrasi dengan baik. Ketika data berasal dari berbagai sumber atau aplikasi yang berbeda, perbedaan format, duplikasi, atau inkonsistensi dalam data dapat terjadi, yang mengganggu kemampuan auditor untuk memverifikasi keakuratan informasi keuangan. Hal ini mengarah pada kesulitan dalam menentukan apakah laporan keuangan yang dihasilkan benar-benar mencerminkan posisi keuangan yang sesungguhnya, karena adanya potensi kesalahan atau ketidaksesuaian data yang belum terdeteksi. Ketidakcocokan antar sistem juga dapat menyebabkan informasi yang redundan atau tidak relevan muncul dalam laporan akhir.

BAB II
KERANGKA KERJA AUDIT IT

Kerangka kerja audit IT memberikan dasar yang terstruktur untuk menilai dan mengevaluasi efektivitas serta risiko yang terkait dengan sistem teknologi informasi dalam suatu organisasi, khususnya di sektor keuangan. Kerangka kerja ini melibatkan serangkaian standar, pedoman, dan metodologi yang digunakan oleh auditor untuk mengidentifikasi potensi kelemahan dan memastikan bahwa sistem IT berfungsi dengan baik, aman, dan sesuai dengan peraturan yang berlaku. Dalam konteks keuangan, kerangka ini sangat penting karena kesalahan atau kelemahan dalam sistem IT dapat menyebabkan kerugian finansial yang besar dan merusak reputasi institusi keuangan.

Penerapan kerangka kerja audit IT harus mempertimbangkan komponen utama seperti kontrol internal, manajemen risiko, dan sistem keamanan. Auditor IT perlu mengevaluasi sejauh mana kebijakan dan prosedur terkait teknologi informasi diterapkan, serta menganalisis bagaimana teknologi yang digunakan dapat mendukung tujuan bisnis secara keseluruhan. Pendekatan ini akan membantu auditor dalam memastikan bahwa organisasi tidak hanya memenuhi kewajiban hukum dan peraturan tetapi juga dapat mengelola risiko dengan cara yang lebih proaktif dan efisien.

A. Pengantar Kerangka Kerja IT Audit

Kerangka kerja IT audit adalah struktur metodologis yang mencakup pedoman untuk perencanaan, pelaksanaan, dan pelaporan hasil audit. Kerangka ini bertujuan untuk membantu auditor menilai kontrol internal, keamanan sistem, dan efektivitas operasional teknologi informasi. Kerangka kerja mencakup langkah-langkah seperti identifikasi risiko, penilaian kontrol, evaluasi data, dan pelaporan hasil audit. Kerangka kerja memberikan landasan yang konsisten bagi auditor

untuk mengidentifikasi dan menangani risiko teknologi. Dalam sektor keuangan, di mana teknologi digunakan secara intensif, kerangka kerja IT audit sangat penting untuk menjaga integritas data dan sistem.

1. Konsistensi dan Standarisasi Proses Audit

Konsistensi dan standarisasi dalam proses audit sangat penting untuk memastikan bahwa seluruh prosedur dijalankan secara seragam, meskipun kompleksitas sistem yang diaudit bervariasi. Kerangka kerja audit memberikan pedoman yang jelas dan terstruktur bagi auditor untuk mengidentifikasi dan menilai potensi risiko dalam sistem, serta memastikan bahwa proses audit dijalankan sesuai dengan standar internasional. Penggunaan kerangka kerja ini memungkinkan auditor untuk melakukan audit dengan pendekatan yang konsisten, meskipun terdapat perbedaan dalam teknologi yang digunakan oleh berbagai institusi keuangan atau organisasi lainnya (Safitri *et al*., 2021). Tanpa adanya pedoman standar ini, audit bisa menjadi kurang objektif dan mungkin menghasilkan kesimpulan yang berbeda dari auditor yang satu ke auditor lainnya.

Pada konteks audit IT, penerapan standar seperti COBIT atau NIST memberikan panduan yang dapat diikuti oleh auditor untuk mengevaluasi kebijakan dan prosedur yang ada dalam sistem teknologi informasi. Standarisasi ini memungkinkan para auditor untuk memahami dengan jelas apa yang harus dievaluasi, bagaimana mengidentifikasi kelemahan dalam sistem, dan memastikan bahwa prosedur yang diterapkan dapat membantu mencapai tujuan organisasi, yaitu kepatuhan terhadap regulasi dan meningkatkan efisiensi operasional. Dengan adanya panduan yang konsisten, proses audit menjadi lebih efisien dan dapat diterima secara internasional.

2. Fokus pada Risiko Utama

Dengan menggunakan kerangka kerja audit yang terstruktur, auditor dapat memusatkan perhatian pada risiko-risiko utama yang paling relevan bagi organisasi. Kerangka kerja ini membantu auditor untuk fokus pada area yang memiliki potensi dampak besar terhadap integritas sistem keuangan dan operasional. Misalnya, dalam audit IT, risiko terkait dengan akses data yang tidak sah, kesalahan dalam pemrosesan transaksi, atau kegagalan sistem yang dapat mengganggu kelancaran operasional. Dengan fokus pada area-area ini, auditor dapat

lebih efektif mendeteksi masalah sebelum menyebabkan kerugian besar bagi organisasi.

Kerangka kerja memungkinkan auditor untuk memetakan dan mengidentifikasi area kritis yang paling rentan terhadap risiko, mengurangi kemungkinan kelemahan operasional yang bisa terlewatkan jika audit dilakukan secara acak. Dalam industri keuangan, di mana perubahan regulasi dan teknologi terjadi dengan cepat, memprioritaskan risiko yang berpotensi mengganggu kepatuhan atau merusak reputasi menjadi sangat penting. Sebagai contoh, risiko terkait dengan ketidakpatuhan terhadap regulasi seperti GDPR atau CCPA menjadi sangat relevan, sehingga kerangka kerja audit berperan dalam mendefinisikan elemen-elemen yang harus diaudit secara lebih mendalam.

3. Meningkatkan Kepatuhan terhadap Regulasi

Kerangka kerja audit IT yang berbasis pada standar internasional seperti COBIT, ISO 27001, NIST, dan ITIL berperan penting dalam memastikan bahwa organisasi mematuhi regulasi yang berlaku. Standar-standar ini menyediakan pedoman yang jelas mengenai pengelolaan keamanan informasi, pengendalian risiko teknologi, dan pemenuhan kewajiban hukum. Misalnya, ISO 27001 menekankan pada pengelolaan sistem keamanan informasi yang menyeluruh, yang sangat relevan untuk organisasi yang beroperasi dalam lingkungan yang sangat teratur dan penuh dengan peraturan, seperti sektor keuangan. Dengan merujuk pada standar ini, auditor IT dapat memastikan bahwa kebijakan dan prosedur yang ada sesuai dengan peraturan yang berlaku, sehingga mengurangi risiko pelanggaran hukum.

Penggunaan kerangka kerja ini juga memperkuat kesadaran akan pentingnya kepatuhan terhadap regulasi yang berkembang. Sebagai contoh, kerangka kerja COBIT mengintegrasikan tata kelola TI dengan tujuan kepatuhan yang lebih luas, sementara NIST fokus pada pengelolaan risiko terkait dengan teknologi dan informasi. Dengan demikian, organisasi yang menggunakan kerangka kerja ini lebih siap untuk menanggapi tuntutan peraturan yang terus berubah, seperti yang tercermin dalam implementasi GDPR di Uni Eropa atau CCPA di California. Hal ini tidak hanya memastikan organisasi tetap memenuhi kewajiban hukum, tetapi juga memperkuat reputasinya sebagai entitas yang berkomitmen pada keamanan dan privasi data.

4. Meningkatkan Efisiensi dan Efektivitas Audit

Proses audit yang terstruktur dan terstandarisasi sangat penting dalam meningkatkan efisiensi dan efektivitas audit IT. Dengan mengikuti kerangka kerja yang jelas, auditor dapat dengan mudah mengidentifikasi area yang perlu diperiksa, mengurangi duplikasi pekerjaan, dan memastikan bahwa semua elemen yang relevan telah tercakup. Hal ini memungkinkan auditor untuk melakukan audit dengan lebih cepat tanpa mengurangi kualitas hasilnya. Misalnya, standar seperti COBIT dan NIST menyediakan pedoman yang komprehensif mengenai aspek-aspek yang harus dievaluasi dalam audit TI, sehingga auditor dapat fokus pada area yang paling kritis dan menghindari analisis yang berlebihan pada bagian yang kurang relevan (Taherdoost, 2022).

Penggunaan teknologi dalam audit IT, seperti perangkat analitik berbasis AI, dapat mempercepat proses audit dengan otomatisasi berbagai tugas repetitif. Audit berbasis teknologi memungkinkan auditor untuk mengidentifikasi pola atau anomali dalam data dengan lebih cepat daripada metode manual. Hal ini tidak hanya mengurangi waktu yang diperlukan untuk menyelesaikan audit, tetapi juga meningkatkan akurasi hasil audit karena alat ini mampu mendeteksi potensi masalah yang mungkin terlewat oleh auditor manusia. Penerapan teknologi ini, bersama dengan kerangka kerja yang sistematis, memungkinkan auditor untuk fokus pada analisis yang lebih mendalam terhadap temuan-temuan yang relevan.

B. COBIT (*Control Objectives for Information and Related Technologies*)

Control Objectives for Information and Related Technologies (COBIT) adalah kerangka kerja manajemen dan tata kelola teknologi informasi (TI) yang dikembangkan oleh ISACA. COBIT menyediakan panduan terstruktur untuk memastikan bahwa sistem TI organisasi selaras dengan tujuan bisnis, memberikan nilai tambah, dan dikelola dengan cara yang efisien serta terkendali. COBIT telah berkembang sejak pertama kali diperkenalkan pada tahun 1996 dan kini menjadi salah satu kerangka kerja paling populer di bidang audit TI, terutama di sektor keuangan. Pembaruan terbaru, COBIT 2019, menekankan pentingnya tata kelola TI yang adaptif terhadap perubahan teknologi dan kebutuhan bisnis global. COBIT pertama kali dikembangkan oleh ISACA untuk

menyediakan panduan dalam mengelola risiko TI dan meningkatkan efisiensi operasional. Versi awal berfokus pada kontrol internal dan kepatuhan terhadap regulasi. Setiap pembaruan COBIT memperkenalkan pendekatan yang lebih relevan dengan kebutuhan industri:

- COBIT 4.1 (2005): Penekanan pada kontrol TI dan kepatuhan.
- COBIT 5 (2012): Memperluas fokus pada tata kelola TI secara menyeluruh, mencakup nilai bisnis.
- COBIT 2019: Menyediakan fleksibilitas lebih besar, fokus pada prinsip tata kelola, dan mendukung kebutuhan transformasi digital.

1. Struktur dan Komponen Utama COBIT

a. Prinsip COBIT 2019

COBIT 2019 didasarkan pada enam prinsip utama:

1) Memenuhi Kebutuhan Pemangku Kepentingan: Tata kelola TI harus memberikan nilai kepada semua pemangku kepentingan.
2) Meliputi Seluruh Perusahaan: COBIT mencakup semua aspek tata kelola TI, tidak hanya operasional tetapi juga strategis.
3) Menggunakan Kerangka Tunggal Terpadu: Kerangka kerja ini terintegrasi dengan standar lain, seperti ISO 27001 dan ITIL.
4) Pendekatan Berbasis Risiko: Fokus pada identifikasi, evaluasi, dan mitigasi risiko TI.
5) Memisahkan Tata Kelola dan Manajemen: Tata kelola dan manajemen didefinisikan sebagai fungsi yang terpisah.
6) Disesuaikan dengan Kebutuhan Khusus Organisasi: COBIT fleksibel untuk berbagai skala dan jenis organisasi.

b. Domain COBIT 2019

COBIT 2019 mencakup lima domain tata kelola:

1) *Evaluate, Direct, and Monitor* (EDM): Memastikan arah strategis yang benar.
2) *Align, Plan, and Organize* (APO): Menyelaraskan tujuan TI dengan kebutuhan bisnis.

3) *Build, Acquire, and Implement* (BAI): Mengelola pengembangan dan penerapan solusi TI.
4) *Deliver, Service, and Support* (DSS): Memastikan layanan TI berjalan lancar.
5) *Monitor, Evaluate, and Assess* (MEA): Memantau dan mengevaluasi kinerja TI.

2. Penerapan COBIT dalam Audit TI

a. Mengidentifikasi Risiko TI

COBIT (*Control Objectives for Information and Related Technologies*) adalah kerangka kerja yang digunakan untuk mengelola dan mengaudit teknologi informasi (TI) dalam organisasi. Salah satu aspek penting dari COBIT adalah kemampuannya untuk membantu auditor dalam mengidentifikasi risiko TI yang dapat memengaruhi operasional dan pencapaian tujuan bisnis. COBIT menyediakan alat dan pedoman yang memungkinkan auditor untuk memetakan risiko TI terhadap tujuan strategis organisasi, serta memberikan panduan untuk menilai sejauh mana risiko ini dapat mengganggu pencapaian tujuan tersebut. Dengan pendekatan yang berbasis pada pengelolaan risiko, COBIT memfasilitasi identifikasi risiko TI yang berkaitan dengan sistem, aplikasi, dan data yang digunakan dalam operasional organisasi.

COBIT mengelompokkan risiko TI dalam berbagai kategori, termasuk risiko operasional, risiko keamanan, risiko ketidakpatuhan terhadap regulasi, dan risiko teknis. Melalui alat yang disediakan oleh COBIT, auditor dapat mengevaluasi apakah kontrol yang ada telah cukup untuk mengatasi berbagai jenis risiko ini. Misalnya, dalam hal keamanan data, COBIT memungkinkan auditor untuk menilai apakah kebijakan dan prosedur yang ada cukup kuat untuk mencegah ancaman seperti peretasan atau kebocoran data. Dengan demikian, COBIT membantu auditor dalam memahami konteks risiko dalam sistem TI dan bagaimana hal ini berinteraksi dengan tujuan bisnis yang lebih luas.

b. Evaluasi Kontrol Internal

Penerapan COBIT dalam audit TI berfokus pada evaluasi kontrol internal untuk memastikan bahwa sistem TI yang

digunakan oleh organisasi berjalan secara efektif, aman, dan efisien. COBIT menyediakan berbagai metrik dan pedoman yang dapat digunakan oleh auditor untuk menilai apakah kontrol internal yang ada dapat mengidentifikasi, mencegah, atau mengurangi risiko yang dapat merugikan operasional dan integritas data organisasi. Kontrol ini mencakup berbagai aspek, seperti keamanan data, kelangsungan operasional, dan kepatuhan terhadap regulasi yang relevan. Dengan menggunakan standar yang ada dalam COBIT, auditor dapat melakukan evaluasi sistematis terhadap efektivitas kontrol internal yang diterapkan dalam berbagai area TI organisasi (Safitri *et al*., 2021).

Salah satu elemen utama dari COBIT adalah kontrol keamanan yang berfokus pada perlindungan data sensitif dan pengelolaan risiko siber. Melalui pedoman COBIT, auditor dapat mengevaluasi apakah kebijakan dan prosedur keamanan yang ada cukup efektif untuk melindungi data dari ancaman internal maupun eksternal. Misalnya, kontrol keamanan yang mengevaluasi pengelolaan identitas pengguna, otorisasi akses, dan audit trail yang dapat digunakan untuk melacak aktivitas yang mencurigakan dalam sistem TI. Pedoman COBIT juga mendorong auditor untuk menilai apakah kebijakan backup dan pemulihan bencana telah diterapkan dengan benar, untuk memastikan kelangsungan operasional meskipun terjadi gangguan sistem.

c. Kepatuhan terhadap Regulasi

Penerapan COBIT dalam audit TI memberikan kerangka kerja yang sangat berguna untuk memastikan kepatuhan terhadap regulasi yang berlaku, seperti *Sarbanes-Oxley Act* (SOX), *General Data Protection Regulation* (GDPR), dan standar keuangan internasional lainnya. COBIT menawarkan pedoman yang terstruktur untuk menilai apakah kebijakan dan kontrol yang ada sudah memadai untuk memenuhi persyaratan regulasi yang kompleks ini. Sebagai contoh, SOX mengharuskan perusahaan untuk menjaga integritas laporan keuangan dan memastikan adanya kontrol internal yang efektif untuk mencegah kecurangan. COBIT mendukung kepatuhan ini dengan menyediakan kontrol yang dapat membantu organisasi mengelola dan melindungi data finansial, serta memastikan

laporan keuangan yang dihasilkan adalah akurat dan dapat dipertanggungjawabkan.

Pada konteks GDPR, COBIT membantu organisasi mengidentifikasi dan mengelola risiko yang terkait dengan perlindungan data pribadi. Kerangka kerja ini memberikan pedoman tentang bagaimana data pribadi harus dikelola, termasuk kontrol akses, enkripsi, dan prosedur untuk menangani permintaan subjek data. COBIT juga mendorong auditor untuk mengevaluasi sistem pengelolaan data pribadi yang ada dalam organisasi, memastikan bahwa data tersebut diproses dengan cara yang sesuai dengan persyaratan GDPR. Melalui evaluasi kontrol ini, auditor dapat menilai sejauh mana organisasi telah mengimplementasikan kebijakan dan prosedur untuk melindungi privasi individu dan memenuhi kewajiban pelaporan yang diatur dalam regulasi tersebut.

Gambar 5. *International Financial Reporting Standards*

COBIT juga mendukung organisasi dalam memastikan kepatuhan terhadap standar keuangan internasional lainnya, seperti *International Financial Reporting Standards* (IFRS). Kerangka ini memberikan pedoman untuk menilai apakah sistem TI yang mendukung laporan keuangan perusahaan dapat menghasilkan data yang akurat dan dapat dipertanggungjawabkan sesuai dengan persyaratan IFRS. Dengan menggunakan kontrol yang tersedia dalam COBIT, auditor dapat mengevaluasi apakah ada kontrol yang cukup untuk memastikan bahwa transaksi keuangan dicatat dan dilaporkan dengan benar, sesuai dengan prinsip akuntansi yang berlaku umum. Hal ini sangat penting untuk menjaga transparansi dan kredibilitas laporan keuangan di tingkat internasional.

d. Studi Kasus

Sebuah bank multinasional yang mengimplementasikan COBIT untuk mengaudit dan memperbaiki kontrol TI mengalami hasil yang signifikan dalam meningkatkan keamanan. Sebagai bagian dari upaya tersebut, bank ini menilai dan mengevaluasi sistem TI yang ada menggunakan prinsip-prinsip COBIT untuk mengidentifikasi potensi kerentanannya. Dengan pendekatan yang lebih sistematis dan terstruktur, memperkuat kontrol keamanan di seluruh infrastruktur TI, mencakup kebijakan akses data, pemantauan jaringan, dan kontrol keamanan fisik yang lebih ketat. Penerapan COBIT memungkinkan bank tersebut untuk mengukur efektivitas kebijakan yang ada serta menilai area-area yang memerlukan perbaikan untuk melindungi aset dan data sensitif.

Bank tersebut tidak hanya berfokus pada deteksi ancaman tetapi juga pada pencegahan dan pemulihan setelah insiden. Melalui integrasi kerangka COBIT, bank berhasil meningkatkan proses pengelolaan insiden dan mengurangi waktu respons terhadap potensi pelanggaran. Dengan menggunakan metrik yang terperinci untuk menilai setiap aspek keamanan TI, mengidentifikasi celah-celah yang sebelumnya tidak terdeteksi dalam sistem yang ada. Penggunaan kontrol yang lebih canggih dan strategi mitigasi yang lebih proaktif membantu mengurangi insiden keamanan secara signifikan, dengan penurunan insiden sebesar 30% dalam satu tahun, sebuah pencapaian yang mencerminkan efektivitas pendekatan COBIT dalam mengelola risiko TI.

Bank ini mengadopsi praktik terbaik yang diidentifikasi melalui evaluasi COBIT untuk memastikan bahwa kontrol tetap sesuai dengan perkembangan regulasi dan ancaman yang terus berubah. Dengan memastikan bahwa seluruh sistem TI selaras dengan standar internasional dan mengadopsi pendekatan berbasis risiko, dapat memitigasi ancaman secara lebih efektif dan menjaga kepatuhan terhadap regulasi yang berlaku. Implementasi COBIT memberikannya kerangka yang fleksibel dan dinamis untuk menanggapi tantangan TI yang selalu berubah, sehingga meningkatkan ketahanan operasional dan keamanan dalam jangka panjang.

3. Manfaat COBIT dalam Audit TI di Sektor Keuangan

a. Meningkatkan Transparansi

COBIT membantu meningkatkan transparansi dalam audit TI sektor keuangan dengan memberikan kerangka kerja yang sistematis dan terstruktur untuk menilai sistem informasi dan kontrol TI. Dengan menggunakan COBIT, auditor dapat menghasilkan laporan yang lebih rinci dan komprehensif mengenai kondisi kontrol TI yang ada, mengidentifikasi potensi risiko, serta memberikan rekomendasi perbaikan yang lebih spesifik. Laporan yang jelas ini tidak hanya memudahkan pemahaman bagi manajemen, tetapi juga meningkatkan akuntabilitas dalam pengelolaan sumber daya TI dan pengambilan keputusan berbasis data yang lebih kuat (Ewuga *et al*., 2023).

Pada konteks sektor keuangan, transparansi yang lebih tinggi sangat penting mengingat sifat industri yang sangat regulatif dan berisiko tinggi. COBIT memfasilitasi komunikasi yang lebih terbuka antara auditor dan manajemen dengan menyajikan temuan yang dapat dipahami secara langsung dan relevan dengan tujuan bisnis serta regulasi yang berlaku. Dengan demikian, manajemen dapat dengan cepat merespons temuan dan mengambil tindakan korektif yang diperlukan untuk memperbaiki kontrol TI yang kurang efektif atau rentan terhadap risiko.

b. Mengoptimalkan Nilai Bisnis

COBIT berperan penting dalam memastikan bahwa teknologi informasi (TI) yang diterapkan dalam sektor keuangan sejalan dengan tujuan strategis perusahaan. Dengan menyediakan kerangka kerja yang jelas untuk mengelola dan mengendalikan TI, COBIT membantu organisasi memanfaatkan teknologi untuk mendukung pencapaian tujuan bisnis jangka panjang, seperti meningkatkan efisiensi operasional, memperbaiki pelayanan pelanggan, dan mendorong inovasi. Implementasi COBIT memungkinkan bank dan institusi keuangan untuk mengukur seberapa baik sistem TI mendukung keberhasilan bisnis, dan jika perlu, memberikan rekomendasi untuk perbaikan yang lebih strategis.

Penerapan COBIT dalam audit TI di sektor keuangan juga memastikan bahwa teknologi tidak hanya diterapkan secara ad-hoc, tetapi dengan tujuan yang jelas yang mendukung prioritas strategis perusahaan. Sebagai contoh, teknologi yang diterapkan dalam sistem manajemen risiko atau sistem keuangan dapat diselaraskan dengan tujuan perusahaan untuk meminimalkan kerugian finansial dan mematuhi regulasi yang berlaku. Dengan demikian, COBIT memberikan wawasan tentang bagaimana TI dapat mengoptimalkan proses bisnis dan memberikan nilai tambah yang lebih besar bagi organisasi dalam menghadapi tantangan industri yang terus berkembang.

c. Efisiensi dalam Proses Audit

COBIT berperan penting dalam meningkatkan efisiensi proses audit TI, terutama di sektor keuangan, dengan menyediakan kerangka kerja yang terstruktur dan jelas. Panduan ini memudahkan auditor untuk mengikuti langkah-langkah audit yang telah terstandarisasi, mengurangi ketidakpastian, dan mempercepat proses verifikasi dan evaluasi. Dalam konteks sektor keuangan, yang menghadapi volume data besar dan sistem yang kompleks, efisiensi waktu menjadi sangat krusial. COBIT membantu mempercepat identifikasi dan pemahaman risiko, memungkinkan auditor untuk fokus pada area yang paling penting tanpa mengurangi kedalaman analisis.

Kerangka kerja COBIT mendukung proses audit dengan menyediakan alat untuk memitigasi potensi kesalahan atau kelalaian. Dengan adanya langkah-langkah yang sudah terdefinisi dengan baik, auditor dapat lebih cepat menilai apakah kontrol yang diterapkan efektif atau tidak, serta memprioritaskan isu-isu yang membutuhkan perhatian lebih mendalam. Hal ini sangat relevan dalam industri keuangan yang sangat tergantung pada sistem TI yang canggih dan memiliki regulasi ketat yang harus dipatuhi. COBIT juga mengarahkan auditor untuk memanfaatkan teknologi modern, seperti otomatisasi dan analitik data, yang memungkinkan untuk melakukan audit secara lebih efektif dan efisien.

C. ISO 27001 dan Keamanan Informasi

ISO/IEC 27001 adalah standar internasional untuk manajemen keamanan informasi yang dirancang untuk membantu organisasi melindungi data sensitif dari ancaman seperti pelanggaran keamanan, akses tidak sah, dan kehilangan data. Standar ini dikeluarkan oleh *International Organization for Standardization* (ISO) dan *International Electrotechnical Commission* (IEC), dengan edisi terbaru dirilis pada tahun 2022. Keamanan informasi adalah aspek kritis dalam audit TI, terutama di sektor keuangan di mana data sensitif seperti informasi nasabah dan transaksi keuangan sangat rentan terhadap ancaman siber. Implementasi ISO 27001 membantu organisasi mengidentifikasi, mengevaluasi, dan mengelola risiko keamanan informasi secara sistematis.

1. Konsep Dasar ISO 27001

ISO 27001 adalah kerangka kerja yang berfokus pada penerapan Sistem Manajemen Keamanan Informasi (*Information Security Management System*, ISMS). Tujuannya adalah:

a. Melindungi kerahasiaan, integritas, dan ketersediaan informasi.
b. Mengelola risiko keamanan informasi secara proaktif.
c. Memastikan kepatuhan terhadap regulasi dan persyaratan hukum.

ISO 27001 didasarkan pada prinsip manajemen keamanan informasi berikut:

a. Kerahasiaan (*Confidentiality*): Memastikan hanya pihak berwenang yang memiliki akses ke informasi.
b. Integritas (*Integrity*): Melindungi akurasi dan keandalan informasi.
c. Ketersediaan (*Availability*): Memastikan informasi tersedia saat dibutuhkan.

2. Struktur dan Komponen ISO 27001

a. Annex A: Kontrol Keamanan Informasi

Annex A ISO 27001 mencakup 93 kontrol keamanan yang terbagi dalam empat tema utama:

1) *Organizational Controls*: Termasuk kebijakan keamanan informasi, manajemen risiko, dan pengelolaan insiden keamanan.
2) *People Controls*: Pelatihan, kesadaran, dan manajemen hak akses.
3) *Physical Controls*: Keamanan fisik seperti akses ke server dan ruang data.
4) *Technological Controls*: Perlindungan data, enkripsi, dan firewall.

b. Proses Utama ISMS

ISO 27001 menggunakan pendekatan berbasis *Plan-Do-Check-Act* (PDCA) dalam manajemen keamanan informasi:

1) *Plan*: Identifikasi risiko dan rancang kebijakan keamanan.
2) *Do*: Implementasi kontrol keamanan yang dirancang.
3) *Check*: Monitor dan evaluasi efektivitas kontrol.
4) *Act*: Ambil tindakan korektif untuk perbaikan berkelanjutan.

3. Implementasi ISO 27001 dalam Audit IT

a. Audit Kesesuaian Standar

Implementasi ISO 27001 dalam audit IT sangat penting untuk memastikan bahwa organisasi mematuhi standar keamanan informasi internasional. ISO 27001 adalah standar yang mengatur sistem manajemen keamanan informasi (ISMS), yang berfokus pada pengelolaan risiko keamanan data dalam organisasi. Auditor IT menggunakan ISO 27001 untuk memverifikasi bahwa organisasi telah mengidentifikasi dan mengelola risiko yang berhubungan dengan keamanan informasi sesuai dengan pedoman standar. Proses audit ini umumnya mencakup berbagai tahapan, mulai dari pemeriksaan dokumen kebijakan hingga pengujian terhadap implementasi teknis di lapangan, untuk memastikan bahwa kontrol yang diterapkan efektif dan sesuai dengan kebijakan yang ditetapkan.

Langkah pertama dalam audit kesesuaian standar adalah memeriksa dokumentasi yang ada. Auditor akan meninjau kebijakan dan prosedur yang terkait dengan pengelolaan keamanan informasi untuk memastikan bahwa mencakup semua persyaratan ISO 27001. Selain itu, auditor akan melakukan wawancara dengan pemangku kepentingan yang terlibat dalam

pengelolaan ISMS untuk mengevaluasi pemahaman tentang kebijakan dan prosedur yang ada. Hal ini penting karena keberhasilan implementasi ISO 27001 sangat bergantung pada partisipasi aktif seluruh anggota organisasi dalam menjaga keamanan informasi.

Auditor akan melakukan pengujian sistem untuk memastikan bahwa kontrol teknis yang diterapkan dalam organisasi berfungsi sesuai dengan yang diharapkan. Pengujian ini melibatkan evaluasi terhadap berbagai sistem keamanan, seperti firewall, kontrol akses, enkripsi data, dan pemantauan jaringan. Auditor akan memeriksa apakah sistem tersebut mematuhi kebijakan yang ada dan apakah kontrol tersebut cukup efektif dalam mengurangi potensi ancaman terhadap keamanan informasi. Pengujian ini juga bertujuan untuk mengidentifikasi kelemahan atau celah dalam implementasi yang mungkin belum diatasi oleh organisasi.

b. Manajemen Risiko

Implementasi ISO 27001 dalam audit TI juga menekankan pentingnya manajemen risiko, yang menjadi bagian integral dari sistem manajemen keamanan informasi (ISMS). ISO 27001 mengharuskan organisasi untuk melakukan identifikasi, penilaian, dan mitigasi risiko yang dapat mengancam keamanan informasi. Auditor IT akan memeriksa proses ini untuk memastikan bahwa organisasi secara proaktif mengelola potensi ancaman terhadap data sensitif dan sistem TI. Proses ini dimulai dengan identifikasi risiko, yang mencakup identifikasi potensi ancaman seperti peretasan, kegagalan sistem, atau kebocoran data yang dapat merusak integritas dan kerahasiaan informasi organisasi.

Setelah risiko teridentifikasi, auditor akan memeriksa bagaimana organisasi mengevaluasi potensi dampak dan kemungkinan terjadinya risiko tersebut. ISO 27001 mengarahkan organisasi untuk menilai risiko berdasarkan dua dimensi: dampak yang mungkin ditimbulkan jika risiko tersebut terjadi dan kemungkinan terjadinya. Auditor akan menggunakan pendekatan ini untuk menilai apakah organisasi telah memprioritaskan risiko berdasarkan tingkat ancamannya, serta apakah telah mengalokasikan sumber daya yang cukup untuk mengelola

risiko-risiko tersebut. Penilaian ini penting karena memungkinkan organisasi untuk lebih fokus pada risiko yang paling signifikan bagi operasi dan reputasi.

Setelah risiko dinilai, langkah berikutnya adalah mitigasi. ISO 27001 mengharuskan organisasi untuk mengimplementasikan kontrol yang sesuai untuk mengurangi atau mengeliminasi risiko yang telah diidentifikasi. Auditor akan mengevaluasi apakah kontrol ini cukup memadai untuk menangani risiko yang terdeteksi, apakah kontrol tersebut telah diuji dan berfungsi dengan baik, serta apakah kontrol tersebut sesuai dengan standar internasional. Pengujian ini melibatkan pemeriksaan apakah kebijakan keamanan yang diterapkan telah efektif dalam mencegah terjadinya insiden keamanan atau memitigasi dampak jika insiden tersebut terjadi.

c. Penyelarasan dengan Kebijakan Organisasi

Penyelarasan kebijakan keamanan informasi dengan tujuan bisnis organisasi adalah salah satu aspek penting dalam implementasi ISO 27001. Auditor TI perlu memastikan bahwa kebijakan yang diterapkan sesuai dengan kebutuhan operasional dan strategis organisasi, serta tidak bertentangan dengan peraturan yang berlaku. Dalam konteks sektor keuangan, misalnya, kebijakan keamanan harus mematuhi regulasi seperti *General Data Protection Regulation* (GDPR) di Uni Eropa atau peraturan lokal yang mengatur perlindungan data dan keamanan transaksi keuangan. Penyelarasan ini memastikan bahwa kebijakan keamanan tidak hanya melindungi informasi organisasi, tetapi juga mendukung keberlanjutan bisnis dan kepercayaan pelanggan.

Pada audit ISO 27001, auditor juga mengevaluasi apakah kebijakan keamanan yang ada memadai dalam menghadapi ancaman yang relevan dengan industri tersebut. Di sektor keuangan, ancaman terhadap data pelanggan dan transaksi keuangan sangat tinggi, sehingga kebijakan yang tidak hanya mengikuti regulasi, tetapi juga memitigasi risiko secara efektif, menjadi penting. Auditor akan memverifikasi apakah kebijakan tersebut telah mencakup kontrol yang diperlukan untuk mengatasi risiko-risiko ini, seperti enkripsi data dan kontrol akses yang ketat. Jika kebijakan keamanan terlalu umum atau tidak

mencakup aspek-aspek kritikal dari industri, auditor akan memberikan rekomendasi untuk perbaikan.

4. Manfaat ISO 27001 untuk Keamanan Informasi di Industri Keuangan

a. Melindungi Data Sensitif

ISO 27001 memberikan kerangka kerja yang kuat bagi organisasi keuangan untuk melindungi data sensitif, seperti informasi nasabah, transaksi, dan informasi bisnis yang sangat berharga. Dalam sektor keuangan, data tersebut sangat rentan terhadap ancaman peretasan, pencurian identitas, dan manipulasi data yang dapat merusak reputasi serta kepercayaan publik. Dengan menerapkan ISO 27001, organisasi dapat memastikan bahwa sistem dan proses yang digunakan untuk menangani data sensitif telah dilengkapi dengan kontrol keamanan yang ketat, termasuk enkripsi, kontrol akses, dan pemantauan berkelanjutan. Hal ini membantu mencegah kebocoran data yang dapat merugikan nasabah dan merusak citra organisasi.

ISO 27001 juga menekankan pentingnya manajemen risiko yang berkelanjutan dalam menjaga data sensitif. Organisasi keuangan harus secara aktif mengidentifikasi potensi risiko dan mengembangkan kebijakan serta prosedur untuk mengurangi atau mengelola ancaman yang mungkin timbul. Dengan pendekatan ini, ISO 27001 memastikan bahwa organisasi dapat dengan cepat merespons insiden keamanan dan mengurangi dampaknya. Kebijakan ini mencakup prosedur pemulihan bencana yang efektif, yang meminimalkan kerugian dan memastikan bahwa operasi keuangan dapat terus berjalan meskipun terjadi pelanggaran keamanan.

b. Kepatuhan terhadap Regulasi

ISO 27001 berperan penting dalam membantu organisasi di sektor keuangan untuk mematuhi berbagai regulasi yang mengatur pengelolaan dan perlindungan data. Salah satu regulasi utama yang dihadapi banyak organisasi di Eropa adalah *General Data Protection Regulation* (GDPR), yang mewajibkan organisasi untuk melindungi data pribadi pelanggan dengan cara yang ketat dan transparan. Dengan menerapkan ISO 27001, organisasi dapat memastikan bahwa memiliki sistem manajemen

keamanan informasi yang komprehensif, yang selaras dengan persyaratan GDPR. Ini mencakup aspek seperti kontrol akses yang ketat, pengelolaan data yang sensitif, serta kebijakan yang jelas mengenai pengolahan dan penyimpanan data pribadi.

ISO 27001 juga mempermudah kepatuhan terhadap standar lain yang relevan dalam sektor keuangan, seperti *Payment Card Industry Data Security Standard* (PCI DSS). PCI DSS adalah standar yang dirancang untuk melindungi informasi kartu pembayaran dari ancaman kebocoran data. Organisasi yang beroperasi dalam sektor pembayaran, seperti bank dan penyedia layanan pembayaran, wajib memenuhi persyaratan ketat ini. ISO 27001 memberikan kerangka yang membantu organisasi tersebut memastikan bahwa kontrol keamanan yang diperlukan, seperti enkripsi dan pemantauan transaksi, diterapkan secara efektif. Penerapan standar ini juga memungkinkan organisasi untuk menjalani audit dengan lebih mudah dan mengurangi risiko pelanggaran keamanan yang dapat berujung pada denda atau kehilangan kepercayaan pelanggan.

c. Meningkatkan Kepercayaan Pemangku Kepentingan

Penerapan ISO 27001 dalam organisasi keuangan dapat secara signifikan meningkatkan kepercayaan pemangku kepentingan, termasuk nasabah, mitra bisnis, dan regulator. Kepercayaan ini dibangun melalui penerapan kebijakan dan prosedur yang transparan serta terukur terkait dengan pengelolaan dan perlindungan data. Dengan adanya sertifikasi ISO 27001, organisasi menunjukkan komitmen yang kuat terhadap keamanan informasi, yang sangat penting bagi nasabah yang mempercayakan data sensitif kepada lembaga keuangan. Keamanan data yang terjamin memberi rasa aman kepada nasabah dan mendorong loyalitas yang lebih tinggi.

Mitra bisnis yang bekerja dengan organisasi keuangan juga mendapatkan jaminan bahwa organisasi tersebut mematuhi standar internasional dalam hal pengelolaan data dan keamanan informasi. Dalam dunia bisnis yang saling terhubung, kerjasama yang aman dan terpercaya menjadi faktor utama dalam pemilihan mitra. Penerapan ISO 27001 menunjukkan bahwa organisasi tersebut dapat diandalkan untuk menjaga integritas data yang dipertukarkan, baik yang berkaitan dengan transaksi keuangan

maupun data operasional lainnya. Hal ini membantu dalam membangun hubungan bisnis yang lebih kuat dan berkelanjutan.

D. NIST *Cybersecurity Framework*

Kerangka kerja *cybersecurity* yang dirancang oleh *National Institute of Standards and Technology* (NIST) adalah panduan komprehensif untuk membantu organisasi mengelola risiko keamanan siber. Diperkenalkan pada tahun 2014, dan diperbarui terakhir kali pada tahun 2018, NIST *Cybersecurity Framework* (CSF) telah menjadi standar global untuk tata kelola keamanan siber yang berfokus pada identifikasi, perlindungan, deteksi, respons, dan pemulihan risiko keamanan informasi.

1. Dasar-Dasar NIST *Cybersecurity Framework*

NIST CSF dikembangkan untuk memperkuat infrastruktur kritis Amerika Serikat, tetapi telah diadopsi secara luas oleh berbagai industri di seluruh dunia, termasuk sektor keuangan. Tujuan utama dari kerangka ini adalah untuk:

a. Membantu organisasi memahami risiko siber.
b. Memberikan pendekatan terstruktur untuk melindungi aset informasi.
c. Memfasilitasi komunikasi risiko antara pemangku kepentingan internal dan eksternal.

Kerangka ini terdiri dari tiga elemen inti:

a. *Core*: Lima fungsi utama yang mencakup identifikasi, perlindungan, deteksi, respons, dan pemulihan.
b. *Tiers*: Tingkat kematangan organisasi dalam mengelola risiko keamanan siber.
c. *Profiles*: Penyesuaian kerangka kerja dengan kebutuhan spesifik organisasi.

2. Komponen Inti (*Core*) NIST *Cybersecurity Framework*

a. *Identify* (Identifikasi)

Langkah ini membantu organisasi memahami aset, sistem, dan risiko yang terkait dengan operasi bisnis. Elemen ini melibatkan:

1) Inventarisasi aset informasi.
2) Penilaian risiko terhadap aset kritis.

3) Identifikasi peraturan yang relevan, seperti GDPR atau PCI DSS.

b. *Protect* (Perlindungan)

Fokusnya adalah pada implementasi kontrol untuk melindungi aset kritis, termasuk:

1) Penggunaan enkripsi untuk data sensitif.
2) Pelatihan keamanan siber bagi karyawan.
3) Implementasi kebijakan pengelolaan akses.

c. *Detect* (Deteksi)

Meningkatkan kemampuan untuk mengidentifikasi ancaman keamanan dengan cepat, misalnya:

1) Pemantauan aktivitas jaringan secara *real-time*.
2) Penggunaan teknologi SIEM (*Security Information and Event Management*).

d. *Respond* (Respons)

Langkah ini bertujuan untuk meminimalkan dampak insiden keamanan dengan:

1) Merancang rencana respons insiden.
2) Melakukan investigasi mendalam setelah kejadian.

e. *Recover* (Pemulihan)

Tahap ini memastikan operasi bisnis dapat pulih dengan cepat setelah insiden keamanan:

1) Pemulihan data melalui cadangan.
2) Evaluasi proses untuk mencegah insiden serupa di masa depan.

3. Relevansi NIST CSF untuk Audit IT

a. Kerangka untuk Audit Keamanan Siber

NIST *Cybersecurity Framework* (CSF) menyediakan panduan yang komprehensif bagi auditor TI dalam menilai kesiapan organisasi untuk menghadapi ancaman keamanan siber. Framework ini terdiri dari lima fungsi inti: *Identify, Protect, Detect, Respond*, dan *Recover*, yang masing-masing menawarkan langkah-langkah jelas untuk menilai efektivitas kontrol keamanan siber yang ada. Auditor dapat menggunakan NIST CSF untuk melakukan penilaian terhadap struktur kebijakan dan prosedur keamanan yang ada, serta mengidentifikasi potensi celah dalam sistem yang dapat dimanfaatkan oleh ancaman

eksternal. Kerangka ini memberikan auditor peta yang jelas untuk mengevaluasi apakah kontrol keamanan yang diterapkan sesuai dengan standar dan best practices industri yang diakui.

Dengan penggunaan NIST CSF, auditor dapat memetakan kekuatan dan kelemahan kontrol keamanan yang ada dengan membandingkannya terhadap kategori dan subkategori yang ada dalam setiap fungsi inti. Fungsi "*Identify*", misalnya, menekankan pentingnya manajemen aset dan pemahaman risiko organisasi, yang memungkinkan auditor untuk memeriksa apakah inventaris sistem dan data yang sensitif sudah dikelola dengan benar. Selanjutnya, fungsi "*Protect*" menilai sejauh mana organisasi melindungi data dan infrastruktur dari ancaman yang dapat mengarah pada pelanggaran keamanan. Dengan pendekatan ini, auditor tidak hanya mengevaluasi efektivitas kontrol yang ada, tetapi juga memberikan rekomendasi perbaikan yang spesifik dan terarah.

b. Penilaian Risiko yang Terstruktur

NIST *Cybersecurity Framework* (CSF) memberikan pendekatan yang terstruktur untuk penilaian risiko dalam audit TI. Dengan memfokuskan pada identifikasi dan mitigasi risiko, framework ini memungkinkan auditor untuk mengevaluasi sejauh mana kebijakan dan prosedur yang diterapkan organisasi dapat melindungi aset informasi yang kritis. Dalam kerangka ini, proses identifikasi risiko dilakukan dengan memetakan potensi ancaman terhadap sistem dan infrastruktur organisasi, serta menilai kerentanannya. Auditor kemudian dapat menilai apakah kebijakan yang ada sudah mencakup semua aspek penting dalam perlindungan data dan apakah kebijakan tersebut cukup efektif dalam mengurangi dampak dari ancaman yang teridentifikasi.

Dengan pendekatan yang sistematis ini, auditor dapat memastikan bahwa organisasi tidak hanya mengenali risiko yang ada, tetapi juga memiliki prosedur yang memadai untuk mengelola dan memitigasi risiko tersebut. NIST CSF memberikan panduan tentang langkah-langkah mitigasi yang harus diterapkan, mulai dari penerapan kontrol teknis seperti enkripsi hingga kebijakan pengelolaan akses yang ketat. Dengan demikian, auditor dapat memberikan penilaian yang lebih

objektif tentang kesiapan organisasi dalam menghadapi ancaman serta mengidentifikasi area yang perlu diperbaiki atau diperkuat.

c. Kepatuhan terhadap Regulasi

NIST *Cybersecurity Framework* (CSF) berperan penting dalam membantu organisasi memenuhi persyaratan hukum dan regulasi yang relevan, seperti *Sarbanes-Oxley Act* (SOX) di Amerika Serikat dan *General Data Protection Regulation* (GDPR) di Uni Eropa. Framework ini memberikan pedoman yang dapat digunakan oleh organisasi untuk mengidentifikasi dan mengelola risiko yang dapat mempengaruhi kepatuhan terhadap peraturan-peraturan ini. Dalam konteks SOX, misalnya, organisasi diharuskan untuk memastikan bahwa sistem TI memiliki kontrol yang memadai dalam mencegah penipuan dan melindungi integritas laporan keuangan. NIST CSF membantu organisasi untuk mengevaluasi sistem keamanan guna memastikan bahwa kontrol tersebut efektif dan sesuai dengan persyaratan yang tercantum dalam SOX.

Begitu juga dalam hal GDPR, yang mengharuskan organisasi untuk melindungi data pribadi pengguna. NIST CSF menyediakan panduan untuk mengimplementasikan kontrol yang melindungi privasi data, seperti enkripsi, kontrol akses, dan kebijakan pengelolaan data pribadi. Framework ini memungkinkan organisasi untuk mengidentifikasi potensi risiko terhadap data pribadi dan memastikan bahwa kebijakan dan prosedur yang ada sudah cukup untuk mencegah kebocoran data atau pelanggaran lainnya yang dapat berakibat pada denda besar. Dengan demikian, NIST CSF mendukung organisasi dalam menciptakan sistem yang patuh terhadap peraturan ini.

4. Manfaat Implementasi NIST CSF di Sektor Keuangan

a. Pengelolaan Risiko yang Lebih Baik

Implementasi NIST *Cybersecurity Framework* (CSF) di sektor keuangan memberikan manfaat signifikan dalam pengelolaan risiko, terutama terkait dengan ancaman siber yang semakin kompleks. Kerangka ini memungkinkan organisasi keuangan untuk mengidentifikasi, menilai, dan mengelola risiko dengan cara yang lebih terstruktur dan komprehensif. NIST CSF menawarkan pendekatan berbasis risiko yang berfokus pada

penguatan kontrol dan pengurangan kerentanannya, memastikan bahwa teknologi yang digunakan, seperti kecerdasan buatan (AI) dan *blockchain*, dikelola dengan tepat. Dalam sektor keuangan, penggunaan teknologi baru sering kali memunculkan tantangan baru dalam hal keamanannya, yang dapat berisiko jika tidak diawasi dengan ketat.

NIST CSF membantu lembaga keuangan untuk memitigasi risiko yang terkait dengan peningkatan ancaman yang disebabkan oleh adopsi teknologi canggih. Misalnya, penggunaan *blockchain* dalam transaksi keuangan bisa rentan terhadap serangan siber jika tidak dilengkapi dengan kontrol yang memadai. Kerangka ini memberikan panduan yang jelas dalam menilai dan mengimplementasikan langkah-langkah mitigasi yang diperlukan untuk teknologi baru tersebut. Dengan cara ini, organisasi dapat lebih siap menghadapi potensi risiko yang mungkin timbul dari penggunaan teknologi yang semakin berkembang.

b. Kepercayaan Pelanggan yang Meningkat

Implementasi NIST *Cybersecurity Framework* (CSF) di sektor keuangan dapat secara signifikan meningkatkan kepercayaan pelanggan dan mitra bisnis. Dengan mengikuti standar keamanan yang ketat, organisasi menunjukkan komitmen terhadap perlindungan data sensitif yang dimiliki oleh pelanggan. Keamanan informasi menjadi salah satu faktor yang sangat dipertimbangkan dalam pengambilan keputusan oleh pelanggan. Organisasi yang dapat menunjukkan bahwa telah mengadopsi kerangka kerja yang terstruktur dan diakui secara internasional, seperti NIST CSF, memberikan bukti kuat bahwa serius dalam melindungi data dan informasi yang penting.

Kepercayaan pelanggan juga meningkat karena merasa lebih aman dalam bertransaksi dengan organisasi yang memiliki kebijakan dan prosedur keamanan yang jelas dan teruji. NIST CSF membantu organisasi mengidentifikasi potensi celah keamanan dan memberikan panduan untuk memperbaikinya. Sebagai hasilnya, pelanggan merasa lebih nyaman dan yakin bahwa organisasi yang dipilih untuk bekerja sama memiliki sistem yang tangguh untuk mencegah ancaman dan serangan siber yang dapat merugikan. Dengan adanya transparansi dan

tindakan nyata untuk meningkatkan keamanan, pelanggan akan lebih cenderung untuk membangun hubungan jangka panjang dengan organisasi tersebut.

c. Efisiensi Operasional

Implementasi NIST *Cybersecurity Framework* (CSF) dapat secara signifikan meningkatkan efisiensi operasional di sektor keuangan dengan menyelaraskan kebijakan keamanan siber dengan strategi bisnis secara keseluruhan. Kerangka ini membantu organisasi untuk melihat keamanan siber bukan hanya sebagai langkah mitigasi risiko, tetapi juga sebagai bagian integral dari operasional yang lebih luas. Dengan adanya pedoman yang jelas mengenai identifikasi, proteksi, deteksi, respons, dan pemulihan terhadap ancaman siber, organisasi dapat mengoptimalkan sumber daya dan merencanakan tindakan yang lebih efektif, sesuai dengan tujuan jangka panjang.

Proses yang sistematis dan terstruktur dalam NIST CSF memungkinkan organisasi untuk mengidentifikasi dan mengurangi redundansi dalam kebijakan dan prosedur yang ada, yang sering kali menyebabkan pemborosan waktu dan sumber daya. Efisiensi operasional meningkat karena pengelolaan risiko yang lebih terorganisir, yang pada gilirannya mengurangi beban administrasi. Penerapan kebijakan keamanan yang lebih terintegrasi juga membantu meminimalkan gangguan operasional yang sering terjadi akibat serangan siber, seperti downtime yang merugikan produktivitas perusahaan.

E. ITIL (*Information Technology Infrastructure Library*) dan Hubungannya dengan Audit

Information Technology Infrastructure Library (ITIL) adalah kerangka kerja terbaik yang diakui secara internasional untuk manajemen layanan TI. ITIL pertama kali dikembangkan oleh pemerintah Inggris pada tahun 1980-an, dan sejak itu telah berevolusi untuk memenuhi kebutuhan sektor TI yang terus berkembang. ITIL mengorganisir proses dan fungsi TI untuk memastikan layanan yang efisien dan efektif bagi organisasi. Dalam konteks audit TI, ITIL menyediakan pedoman yang berguna untuk menilai keberhasilan dan efisiensi pengelolaan layanan TI, serta bagaimana ini dapat mendukung

tujuan audit organisasi dalam menjaga keberlanjutan operasional dan kepatuhan terhadap standar dan regulasi yang berlaku.

1. Dasar-Dasar ITIL

ITIL adalah serangkaian praktik terbaik untuk manajemen layanan TI yang berfokus pada penyampaian nilai maksimal kepada pelanggan dan pengguna akhir melalui penggunaan TI. ITIL mengatur berbagai aspek layanan TI, mulai dari perencanaan hingga pemulihan bencana. Tujuan utamanya adalah untuk memastikan bahwa layanan TI yang disediakan sesuai dengan kebutuhan bisnis dan pelanggan. ITIL terdiri dari lima tahap inti dalam siklus hidup layanan, yaitu:

a. *Service Strategy* (Strategi Layanan) – Menetapkan pendekatan untuk desain dan pengelolaan layanan TI yang mendukung tujuan bisnis.
b. *Service Design* (Desain Layanan) – Menentukan spesifikasi untuk layanan TI, termasuk infrastruktur dan kebijakan.
c. *Service Transition* (Transisi Layanan) – Menjamin layanan baru atau yang diubah dapat diterapkan dengan lancar dan efektif.
d. *Service Operation* (Operasi Layanan) – Melibatkan penyampaian layanan TI sehari-hari kepada pengguna akhir.
e. *Continual Service Improvement* (Peningkatan Layanan Berkelanjutan) – Memastikan layanan yang ada terus ditingkatkan berdasarkan umpan balik dan evaluasi berkala.

ITIL pertama kali dikembangkan oleh *Office of Government Commerce* (OGC) di Inggris pada tahun 1980-an untuk meningkatkan manajemen layanan TI dalam sektor publik. Dengan waktu, ITIL berkembang menjadi referensi global yang diterima luas, baik di sektor publik maupun swasta, dan telah melalui beberapa edisi yang terus diperbarui untuk menanggapi tantangan teknologi terbaru, seperti *cloud computing* dan keamanan siber (Agutter & Villa, 2020).

2. ITIL dan Hubungannya dengan Audit TI

a. ITIL sebagai Kerangka Audit untuk Layanan TI

ITIL (*Information Technology Infrastructure Library*) memberikan kerangka yang sangat penting untuk audit TI dengan menyediakan struktur yang jelas dan proses yang terstandardisasi dalam pengelolaan layanan TI. ITIL berfokus pada siklus hidup layanan TI, yang dimulai dari perencanaan, desain, pengiriman,

hingga pengelolaan layanan yang ada. Masing-masing fase ini menyediakan titik evaluasi yang strategis, di mana auditor dapat menilai apakah layanan TI tersebut berjalan sesuai dengan tujuan dan kebijakan organisasi. Sebagai contoh, pada fase *Service Design*, auditor dapat mengevaluasi apakah perencanaan dan desain layanan TI sesuai dengan kebutuhan dan harapan pengguna serta apakah ada kontrol yang memadai untuk mengurangi risiko yang berpotensi mengganggu kelancaran operasional.

Proses dalam ITIL juga memungkinkan auditor untuk melakukan penilaian yang lebih mendalam mengenai efektivitas dan efisiensi layanan TI yang ada. Salah satu aspek penting dalam audit berbasis ITIL adalah continual service improvement yang mendorong evaluasi terus-menerus untuk menemukan area yang memerlukan perbaikan. Hal ini memungkinkan auditor untuk mengidentifikasi kelemahan dalam pengelolaan layanan TI dan memberi rekomendasi untuk peningkatan yang berkelanjutan. Dengan mendalami setiap tahap dalam siklus hidup layanan TI, auditor dapat mengukur apakah prosedur yang diikuti organisasi sudah mencakup kontrol yang tepat untuk mitigasi risiko, pengelolaan sumber daya, dan pencapaian sasaran organisasi.

b. Kepatuhan dan Pengendalian

Pada audit TI, ITIL memberikan panduan yang sangat penting untuk memastikan bahwa prosedur dan kebijakan organisasi sejalan dengan standar kepatuhan yang berlaku, baik yang berasal dari peraturan industri maupun standar internasional. Proses-proses utama dalam ITIL, seperti pengelolaan insiden, perubahan, dan risiko, membantu auditor untuk memverifikasi bahwa organisasi telah mengimplementasikan kontrol yang memadai untuk mematuhi persyaratan hukum yang berlaku. Misalnya, dalam pengelolaan perubahan, ITIL mengharuskan perubahan dilakukan melalui prosedur yang terkendali untuk menghindari gangguan pada operasi bisnis yang dapat melanggar regulasi yang ada (Calder, 2018).

ITIL menyediakan struktur yang jelas mengenai manajemen insiden, yang krusial untuk memastikan kepatuhan terhadap

standar industri. Proses ini memungkinkan auditor untuk menilai apakah organisasi memiliki prosedur yang tepat untuk menangani insiden TI, termasuk dalam hal pelaporan dan pemulihan. Prosedur yang tidak memadai dalam menangani insiden dapat mengakibatkan ketidakpatuhan terhadap regulasi yang mengharuskan organisasi untuk melindungi data sensitif dan menjaga kelangsungan operasional yang aman. Oleh karena itu, auditor menggunakan ITIL untuk memverifikasi bahwa setiap insiden telah ditangani dengan cara yang sesuai dan memenuhi standar kepatuhan yang berlaku.

3. ITIL dan Manajemen Layanan TI yang Efektif

a. Peningkatan Kinerja dan Efisiensi

ITIL (*Information Technology Infrastructure Library*) berperan penting dalam meningkatkan kinerja dan efisiensi manajemen layanan TI di organisasi. Dengan mengadopsi pendekatan berbasis proses, ITIL memfokuskan pada desain dan pengelolaan layanan TI yang dapat memenuhi tujuan bisnis dan kebutuhan pengguna. Pendekatan ini tidak hanya meningkatkan kualitas layanan tetapi juga membantu organisasi mengidentifikasi area yang perlu diperbaiki, seperti dalam manajemen insiden, perubahan, dan pemulihan. Melalui proses-proses yang sistematis dan terstruktur, ITIL memungkinkan organisasi untuk memberikan layanan yang lebih cepat, lebih baik, dan lebih efisien, sehingga mendukung tujuan strategis bisnis (Agutter & Villa, 2020).

Pada konteks audit TI, ITIL memberikan auditor alat yang tepat untuk mengevaluasi efektivitas proses manajemen layanan. Auditor dapat menggunakan ITIL untuk menilai seberapa baik organisasi mengelola setiap tahap dalam siklus hidup layanan TI, mulai dari perencanaan dan desain hingga pengoperasian dan pemeliharaan. Ini memungkinkan auditor untuk mengidentifikasi celah dalam proses yang dapat mempengaruhi kinerja layanan TI, serta memberikan rekomendasi perbaikan yang dapat meningkatkan efisiensi operasional. Dengan pendekatan berbasis bukti, auditor juga dapat memastikan bahwa semua proses berjalan sesuai dengan standar yang telah ditetapkan dan mencapai tujuan yang diinginkan.

b. Evaluasi Pengelolaan Risiko TI

Penerapan ITIL dalam audit TI memungkinkan auditor untuk mengevaluasi bagaimana organisasi mengelola risiko terkait dengan layanan TI. Dalam ITIL, risiko dapat berasal dari berbagai faktor, mulai dari gangguan operasional hingga ancaman keamanan yang dapat mempengaruhi kelangsungan layanan. Auditor menggunakan kerangka kerja ini untuk mengidentifikasi potensi risiko yang dapat memengaruhi kinerja layanan TI, seperti kegagalan infrastruktur, kesalahan manusia, atau serangan siber. Dengan mengevaluasi bagaimana organisasi mengelola risiko ini, auditor dapat memberikan gambaran yang jelas tentang kesiapan organisasi untuk menghadapi ancaman yang dapat merugikan operasi dan reputasinya.

ITIL menawarkan panduan yang sistematis untuk mengidentifikasi dan menilai dampak dari risiko yang terdeteksi. Auditor dapat menggunakan prinsip-prinsip ITIL untuk memastikan bahwa kontrol yang diterapkan sudah sesuai dengan potensi ancaman yang ada. Misalnya, dalam konteks manajemen insiden dan masalah, ITIL mendorong organisasi untuk memiliki prosedur yang tepat untuk mengidentifikasi, mengatasi, dan mengurangi dampak gangguan layanan. Dalam audit, ini memberikan kesempatan untuk menilai apakah prosedur yang ada cukup efektif dalam memitigasi risiko dan menjaga kelangsungan layanan.

c. Pengelolaan Sumber Daya TI

ITIL memberikan pedoman yang jelas untuk pengelolaan sumber daya TI, yang meliputi perangkat keras, perangkat lunak, dan personel. Dalam konteks audit, auditor akan mengevaluasi bagaimana organisasi mengelola sumber daya ini untuk mendukung keberlanjutan dan efisiensi operasional. Misalnya, auditor akan menilai apakah perangkat keras dan perangkat lunak yang digunakan masih relevan dan optimal, atau jika ada pemborosan pada infrastruktur yang tidak terpakai atau usang. Efisiensi dalam pemanfaatan sumber daya TI sangat penting untuk memastikan bahwa investasi yang dilakukan organisasi memberikan nilai maksimal bagi bisnis.

ITIL menekankan pentingnya manajemen konfigurasi dan pengelolaan kapasitas dalam pengelolaan sumber daya TI.

Auditor akan mengidentifikasi apakah organisasi memiliki proses yang memadai untuk mengelola inventaris sumber daya TI dan memastikan bahwa kapasitas yang tersedia mencukupi untuk memenuhi permintaan operasional tanpa menimbulkan pemborosan. Dalam audit, aspek ini sangat penting untuk menilai apakah organisasi telah merencanakan penggunaan sumber daya secara efektif, dengan meminimalkan risiko kekurangan atau kelebihan kapasitas yang dapat mempengaruhi kinerja layanan TI.

4. ITIL dalam Konteks Sektor Keuangan

a. Keamanan dan Kepatuhan dalam Keuangan

ITIL (*Information Technology Infrastructure Library*) memberikan kerangka yang sangat relevan untuk sektor keuangan dalam mengelola dan melindungi layanan TI. Keamanan dan kepatuhan adalah dua aspek penting yang harus dijaga dalam industri ini, mengingat data finansial sangat sensitif dan sangat diatur oleh berbagai peraturan. ITIL membantu memastikan bahwa kebijakan dan prosedur yang ada di dalam organisasi keuangan mematuhi regulasi terkait seperti peraturan perlindungan data pribadi (misalnya GDPR di Eropa atau peraturan lain yang relevan di pasar global). Dengan mendefinisikan dan mengimplementasikan kontrol keamanan yang ketat dalam siklus hidup layanan TI, ITIL memastikan bahwa organisasi dapat mengelola data dan transaksi keuangan dengan cara yang aman dan terlindungi.

Dengan proses manajemen risiko yang terintegrasi dalam ITIL, sektor keuangan dapat melakukan penilaian risiko secara berkelanjutan. ITIL menekankan pentingnya evaluasi risiko terhadap ancaman yang dapat merusak integritas data atau mempengaruhi keberlanjutan layanan. Organisasi dapat menggunakan pedoman ITIL untuk mengidentifikasi potensi kelemahan dalam infrastruktur TI dan mengembangkan solusi untuk mengatasi masalah yang dapat memengaruhi kepatuhan terhadap standar keamanan. Selain itu, kontrol perubahan dalam ITIL juga memberikan mekanisme yang ketat untuk memastikan bahwa perubahan yang diterapkan dalam sistem TI tidak

memperkenalkan kerentanannya terhadap pelanggaran data atau masalah kepatuhan.

b. Manajemen Risiko dalam Keuangan

Pada sektor keuangan, manajemen risiko menjadi hal yang sangat penting mengingat dampak signifikan yang bisa ditimbulkan dari gangguan layanan TI. ITIL memberikan kerangka yang terstruktur untuk menilai dan mengelola risiko tersebut. Dalam konteks ini, ITIL membantu organisasi untuk mengidentifikasi potensi ancaman terhadap layanan TI yang dapat mempengaruhi operasi bisnis, seperti ancaman keamanan data, gangguan sistem, atau kegagalan infrastruktur. Dengan menggunakan proses manajemen risiko yang jelas, organisasi dapat secara proaktif mengidentifikasi risiko, mengembangkan strategi mitigasi yang tepat, dan memonitor risiko yang ada agar tetap dalam batas yang dapat diterima.

Salah satu pendekatan yang diadopsi ITIL dalam pengelolaan risiko adalah melalui penilaian dan pengendalian risiko yang terintegrasi dalam seluruh siklus hidup layanan TI. Setiap fase, mulai dari perencanaan dan desain layanan hingga pengoperasian dan pemulihan, mencakup evaluasi risiko yang relevan dengan faktor-faktor yang mempengaruhi keberhasilan layanan TI dalam sektor keuangan. Misalnya, risiko yang terkait dengan kegagalan dalam mengelola perubahan sistem atau kurangnya pemulihan bencana yang efektif dapat dikendalikan dengan menggunakan prinsip-prinsip manajemen perubahan dan manajemen insiden dalam ITIL, memastikan bahwa semua risiko yang dapat mengganggu operasional atau melanggar kepatuhan diidentifikasi dan ditangani secara tepat waktu.

c. Integrasi dengan Kerangka Kerja Keamanan Siber

Pada sektor keuangan, ancaman siber terus berkembang dan semakin kompleks, sehingga memerlukan pendekatan yang lebih terintegrasi untuk melindungi data dan infrastruktur TI. ITIL, sebagai kerangka manajemen layanan TI, dapat diintegrasikan dengan kerangka kerja keamanan siber lainnya, seperti NIST *Cybersecurity Framework* (CSF) atau ISO 27001, untuk memberikan kontrol yang lebih komprehensif. ITIL fokus pada manajemen layanan TI, sementara NIST dan ISO 27001 memberikan pendekatan yang lebih mendalam dalam hal

perlindungan data, pengelolaan ancaman, dan pemulihan bencana. Integrasi antara ITIL dan kerangka keamanan siber ini memungkinkan organisasi untuk membangun sistem yang lebih tangguh dan responsif terhadap ancaman siber yang terus berkembang.

Dengan menggabungkan ITIL dengan NIST atau ISO 27001, organisasi keuangan dapat menciptakan pengelolaan layanan TI yang lebih aman dan efektif. Misalnya, ITIL memberikan panduan tentang pengelolaan insiden dan perubahan dalam layanan TI, sedangkan NIST memberikan pedoman untuk mengidentifikasi, melindungi, mendeteksi, merespons, dan memulihkan dari ancaman siber. ISO 27001, di sisi lain, menetapkan standar untuk sistem manajemen keamanan informasi, yang dapat diterapkan di seluruh organisasi keuangan. Melalui integrasi ini, organisasi dapat memastikan bahwa layanan TI tidak hanya memenuhi kebutuhan bisnis tetapi juga memenuhi standar keamanan yang ketat, memperkuat perlindungan terhadap data sensitif dan mencegah kebocoran atau pelanggaran data.

BAB III
STANDAR INTERNASIONAL DALAM AUDIT IT KEUANGAN

Audit IT dalam sektor keuangan diatur oleh berbagai standar internasional yang bertujuan untuk memastikan transparansi, keamanan, dan keandalan sistem keuangan. Standar ini memberikan pedoman yang jelas bagi auditor dalam menilai dan memverifikasi kontrol internal, manajemen risiko, serta kepatuhan terhadap regulasi. Standar internasional bukan hanya tentang penilaian risiko atau kontrol sistem, tetapi juga membantu organisasi menjaga integritas data dan kepercayaan pemangku kepentingan. Penerapan standar internasional memfasilitasi penerapan praktik terbaik dalam keamanan siber, perlindungan data, dan pengelolaan risiko yang menjadi semakin penting dalam era digital ini.

A. *International Standards on Auditing* (ISA) yang Terkait dengan IT

International Standards on Auditing (ISA) merupakan standar global yang bertujuan untuk menetapkan dasar yang jelas dan konsisten dalam pelaksanaan audit laporan keuangan. ISA memberikan panduan mengenai prosedur audit yang harus diikuti oleh auditor dalam menilai kewajaran laporan keuangan, serta mengidentifikasi potensi risiko yang berhubungan dengan material misstatement atau ketidakakuratan laporan keuangan.

1. Hubungan antara ISA dan Teknologi Informasi dalam Audit Keuangan

a. Relevansi IT dalam Audit Keuangan

Teknologi informasi (TI) telah mengubah cara organisasi mengelola dan melaporkan informasi keuangan. Sebagian besar organisasi modern menggunakan sistem komputer untuk menyimpan dan memproses data akuntansi, serta menghasilkan laporan keuangan yang digunakan untuk pengambilan keputusan. Dengan penerapan TI yang begitu mendalam dalam proses akuntansi dan pelaporan, peran auditor menjadi lebih kompleks. Auditor tidak hanya perlu menilai kewajaran laporan keuangan, tetapi juga harus mengevaluasi efektivitas dan keamanan sistem informasi yang digunakan untuk menghasilkan laporan tersebut. Oleh karena itu, dalam audit keuangan, relevansi TI tidak dapat dipandang sebelah mata, dan menjadi bagian penting dalam proses audit yang lebih luas.

International Standards on Auditing (ISA), khususnya ISA 315 dan ISA 330, memberikan panduan kepada auditor dalam mengevaluasi risiko yang berhubungan dengan teknologi informasi. Auditor perlu memahami bagaimana sistem TI mempengaruhi proses pengendalian internal dan mempengaruhi kewajaran laporan keuangan. Sebagai contoh, auditor perlu mengevaluasi apakah sistem TI yang digunakan memadai untuk mendeteksi dan mengoreksi kesalahan atau kecurangan yang mungkin terjadi dalam pengolahan data keuangan. Dalam hal ini, audit IT harus memastikan bahwa kontrol dalam sistem informasi, seperti akses yang terbatas dan pemantauan yang cukup, diterapkan dengan benar untuk melindungi integritas data.

b. Peran Teknologi dalam Proses Audit

Peran teknologi informasi (TI) dalam proses audit keuangan telah menjadi semakin penting seiring dengan meningkatnya ketergantungan organisasi terhadap sistem berbasis komputer untuk mengelola data keuangan. Auditor kini dihadapkan pada tantangan untuk memastikan bahwa informasi keuangan yang dihasilkan oleh sistem TI dapat dipercaya dan bebas dari kesalahan atau manipulasi. Teknologi telah mengubah cara transaksi dilakukan dan dilaporkan, menjadikan pengujian sistem TI sebagai bagian yang tidak terpisahkan dari proses audit.

Dengan memanfaatkan teknologi yang tepat, auditor dapat mengidentifikasi potensi masalah lebih awal dan memastikan bahwa laporan keuangan yang dihasilkan sesuai dengan standar yang berlaku.

Pada proses audit, auditor harus memiliki pengetahuan dan keterampilan yang cukup untuk memahami bagaimana sistem TI mempengaruhi pengelolaan dan pelaporan data keuangan. Perlu mengevaluasi kontrol teknologi yang ada dalam sistem informasi, termasuk perlindungan data dan pengelolaan akses pengguna. Risiko terkait dengan akurasi data dan potensi manipulasi informasi dapat ditangani melalui pemeriksaan sistem kontrol yang ada dalam perangkat lunak akuntansi atau sistem informasi lainnya. Ini mencakup verifikasi bahwa data yang dimasukkan ke dalam sistem akurat dan bahwa pengolahan serta pelaporan data dilakukan secara efisien dan tepat.

2. International Standards on Auditing yang Terkait dengan IT

Beberapa ISA yang berhubungan dengan audit TI dalam konteks keuangan mencakup standar-standar yang lebih spesifik, antara lain ISA 315, ISA 330, dan ISA 500. Berikut adalah penjelasan mengenai standar-standar yang relevan:

a. ISA 315 – Identifikasi dan Penilaian Risiko dalam Audit Laporan Keuangan

ISA 315 memberikan pedoman kepada auditor dalam mengidentifikasi dan menilai risiko kesalahan material dalam laporan keuangan, baik yang timbul dari faktor internal maupun eksternal, termasuk yang disebabkan oleh sistem informasi yang digunakan oleh organisasi. Dalam konteks IT, auditor perlu menilai apakah sistem informasi yang digunakan mengandung risiko yang dapat memengaruhi kewajaran laporan keuangan, seperti potensi kesalahan dalam pemrosesan transaksi atau ketidakamanan data yang disimpan.

ISA 315 mengharuskan auditor untuk melakukan pemahaman terhadap sistem TI yang digunakan organisasi, termasuk mengidentifikasi dan mengevaluasi kontrol yang ada untuk memitigasi risiko tersebut. Penilaian terhadap kontrol internal yang berhubungan dengan IT menjadi krusial untuk memastikan bahwa data yang dihasilkan oleh sistem tersebut

dapat dipercaya untuk digunakan dalam penyusunan laporan keuangan.

b. ISA 330 – Respons Auditor terhadap Risiko yang Diidentifikasi

ISA 330 mengatur bagaimana auditor harus merespons terhadap risiko yang telah diidentifikasi dalam audit. Dalam konteks audit TI, jika auditor menemukan bahwa sistem informasi memiliki potensi risiko yang tinggi terhadap laporan keuangan, auditor harus merancang prosedur audit tambahan untuk mengatasi risiko tersebut. Hal ini termasuk memeriksa pengendalian atas teknologi informasi yang digunakan, melakukan pengujian terhadap sistem, dan menilai apakah kontrol IT yang diterapkan memadai untuk mengurangi risiko kesalahan material.

c. ISA 500 – Bukti Audit

ISA 500 mengatur tentang pengumpulan bukti audit yang relevan dan dapat diandalkan. Dalam audit yang melibatkan sistem TI, auditor perlu memperoleh bukti bahwa data yang dihasilkan oleh sistem informasi adalah akurat, valid, dan tidak dimanipulasi. Oleh karena itu, audit TI harus melibatkan pengujian terhadap integritas data yang dihasilkan oleh sistem IT. Auditor dapat menggunakan teknik audit berbasis teknologi, seperti audit berbasis data (*data-driven audit*), untuk memeriksa transaksi yang tercatat dalam sistem informasi. Bukti audit yang relevan juga meliputi dokumentasi terkait kontrol TI, konfigurasi sistem, dan pengujian sistem. Jika ada perubahan yang signifikan dalam teknologi atau infrastruktur IT organisasi, auditor harus mengevaluasi bagaimana perubahan tersebut memengaruhi kualitas dan keamanan laporan keuangan.

3. Peran Standar Internasional dalam Kepatuhan Regulasi dan Pengendalian

a. Kepatuhan terhadap Regulasi

Kepatuhan terhadap regulasi adalah salah satu aspek penting dalam audit teknologi informasi (TI), terutama dalam konteks laporan keuangan. Banyak negara dan industri yang mengharuskan perusahaan untuk melaksanakan audit TI guna memastikan bahwa ia mematuhi peraturan dan standar akuntansi yang berlaku. Misalnya, di Amerika Serikat, perusahaan publik

diwajibkan untuk mematuhi *Sarbanes-Oxley Act* (SOX), yang menetapkan standar untuk pengelolaan laporan keuangan dan audit TI. Di Uni Eropa, perusahaan harus mematuhi peraturan seperti *General Data Protection Regulation* (GDPR) yang melindungi data pribadi dan mengatur bagaimana data tersebut dapat diproses dan disimpan. Negara-negara berkembang juga mulai menerapkan standar ini untuk memastikan keberlanjutan dalam sistem keuangan global yang semakin terdigitalisasi.

International Standards on Auditing (ISA) berperan krusial dalam memberikan pedoman bagi auditor untuk melaksanakan audit TI yang sesuai dengan standar internasional. ISA memberikan panduan tentang bagaimana auditor harus merencanakan dan melaksanakan audit teknologi, termasuk bagaimana mengevaluasi kontrol TI yang ada dalam suatu organisasi. Dengan mengikuti standar ini, auditor dapat memastikan bahwa ia mematuhi persyaratan hukum yang berlaku dan bahwa laporan keuangan yang dihasilkan adalah akurat dan dapat dipercaya. Hal ini sangat penting untuk mempertahankan integritas sistem keuangan global dan untuk menghindari risiko yang terkait dengan ketidakpatuhan.

b. Pengendalian Internal dan Sistem TI

Pengendalian internal dalam organisasi, khususnya yang berkaitan dengan teknologi informasi (TI), berperan kunci dalam memastikan akurasi dan keandalan laporan keuangan. Dalam audit laporan keuangan, *International Standards on Auditing* (ISA) menekankan bahwa pengendalian internal yang efektif harus mencakup semua aspek kritikal TI yang mendukung proses akuntansi dan pelaporan keuangan. Ini mencakup pengelolaan akses pengguna, perlindungan data, dan pengendalian terhadap potensi penipuan yang dapat mempengaruhi integritas laporan keuangan. Kontrol yang baik akan memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi sensitif dan bahwa data yang digunakan dalam laporan keuangan tetap utuh dan terlindungi.

Salah satu aspek pengendalian internal yang perlu diawasi dengan seksama adalah pengelolaan akses pengguna. Organisasi harus memastikan bahwa hanya pengguna yang memiliki otorisasi yang tepat yang dapat mengakses sistem TI yang

berhubungan dengan laporan keuangan. Ini mencegah potensi akses tidak sah yang bisa merusak data atau laporan keuangan. Di sisi lain, perlindungan data juga sangat penting. Penggunaan enkripsi data, pengamanan jaringan, dan kebijakan backup yang memadai adalah langkah-langkah yang perlu dipastikan oleh auditor untuk menjaga agar data tetap aman dan tidak mudah terakses oleh pihak yang tidak berwenang.

B. COSO *Internal Control Framework*

COSO *Internal Control Framework* pertama kali diterbitkan pada tahun 1992 oleh COSO, sebuah organisasi yang terdiri dari beberapa asosiasi profesional terkemuka di bidang akuntansi, audit, dan keuangan. Framework ini dikembangkan untuk memberikan pedoman yang sistematis mengenai pengendalian internal dalam organisasi. Di Indonesia, COSO Framework ini sangat berpengaruh dalam penetapan standar pengendalian internal yang digunakan oleh auditor dan profesional lainnya. Revisi terbesar dari COSO Framework terjadi pada tahun 2013, di mana framework ini diperbarui untuk mencerminkan perkembangan dalam praktik pengendalian internal, serta untuk mengakomodasi perubahan dalam lingkungan teknologi dan regulasi yang dihadapi oleh perusahaan.

1. Komponen-Komponen COSO *Internal Control Framework*

a. *Control Environment* (Lingkungan Pengendalian)

Lingkungan pengendalian adalah dasar dari seluruh sistem pengendalian internal, yang mencakup budaya organisasi, nilai-nilai etika, dan integritas manajemen. Dalam konteks audit TI, lingkungan pengendalian mencakup kebijakan dan prosedur yang diterapkan oleh organisasi untuk memastikan bahwa teknologi informasi digunakan dengan cara yang dapat dipercaya dan sesuai dengan tujuan organisasi. Beberapa faktor penting dalam komponen ini adalah:

1) Komitmen terhadap etika dan integritas dalam penggunaan teknologi informasi.
2) Struktur pengawasan dan tanggung jawab untuk pengelolaan TI.

3) Pendidikan dan pelatihan untuk karyawan agar memahami pentingnya pengendalian internal, khususnya terkait dengan sistem IT.

b. *Risk Assessment* (Penilaian Risiko)

Penilaian risiko adalah proses untuk mengidentifikasi dan menganalisis risiko yang mungkin memengaruhi pencapaian tujuan organisasi, termasuk risiko yang berkaitan dengan teknologi informasi. Dalam audit TI, penilaian risiko ini melibatkan identifikasi risiko yang mungkin timbul akibat kesalahan dalam pemrosesan data, pelanggaran keamanan informasi, atau ketidaksesuaian dalam penggunaan aplikasi perangkat lunak. Proses ini mencakup beberapa langkah:

1) Identifikasi Risiko: Menilai potensi ancaman yang mungkin timbul dalam pengelolaan sistem TI.
2) Analisis Dampak dan Probabilitas: Menilai seberapa besar dampak yang mungkin ditimbulkan oleh risiko tersebut terhadap laporan keuangan.
3) Pengelolaan Risiko: Mengembangkan strategi untuk mengurangi atau mengelola risiko yang teridentifikasi.

c. *Control Activities* (Kegiatan Pengendalian)

Control activities merujuk pada kebijakan dan prosedur yang diimplementasikan untuk memastikan bahwa langkah-langkah yang diambil untuk mengurangi risiko terjadi dengan cara yang efisien. Dalam konteks audit TI keuangan, kegiatan pengendalian ini meliputi berbagai tindakan yang diambil untuk memastikan integritas data, keandalan sistem, dan keamanan informasi. Beberapa contoh kegiatan pengendalian yang relevan dalam TI antara lain:

1) Pengendalian Akses: Pembatasan akses ke data sensitif berdasarkan tingkat kewenangan.
2) Pengendalian Otentikasi dan Otorisasi: Proses untuk memverifikasi identitas pengguna dan memberikan akses sesuai dengan hak pengguna.
3) Pemantauan dan Pencatatan: Mencatat setiap aktivitas di dalam sistem untuk memudahkan deteksi dan pencegahan penyalahgunaan.

d. *Information and Communication* (Informasi dan Komunikasi)

Informasi dan komunikasi yang efektif sangat penting untuk mendukung pengendalian internal dalam organisasi. Dalam konteks IT, hal ini mencakup pengelolaan dan pengaliran informasi yang relevan kepada pihak yang tepat, baik itu terkait dengan pengelolaan data, laporan keuangan, atau keamanan TI. Komponen ini melibatkan:

1) Sistem komunikasi yang efisien: Memastikan informasi yang relevan tentang sistem TI disampaikan secara tepat waktu dan akurat kepada pihak yang membutuhkan.
2) Keamanan informasi: Menjamin bahwa informasi sensitif dilindungi dan hanya dapat diakses oleh pihak yang berwenang.

e. *Monitoring Activities* (Kegiatan Pemantauan)

Pemantauan adalah proses untuk menilai apakah kontrol yang diterapkan dalam organisasi berjalan efektif. Dalam pengelolaan TI, pemantauan melibatkan evaluasi terhadap sistem TI dan kontrol yang diterapkan untuk mendeteksi dan mengoreksi masalah atau kelemahan yang ada. Kegiatan pemantauan ini bisa berupa:

1) Audit rutin: Pemeriksaan berkala terhadap pengendalian TI untuk menilai keefektifannya.
2) Pemantauan sistem otomatis: Penggunaan teknologi untuk memantau aktivitas sistem secara *real-time* dan mendeteksi potensi masalah.

2. Implementasi COSO dalam Audit IT Keuangan

a. Penerapan COSO dalam Audit TI

Penerapan COSO (*Committee of Sponsoring Organizations of the Treadway Commission*) dalam audit TI keuangan sangat penting untuk memastikan bahwa pengendalian internal yang diterapkan oleh organisasi dapat mendukung kewajaran laporan keuangan. COSO menyediakan kerangka kerja yang terdiri dari lima komponen utama, yaitu lingkungan pengendalian, penilaian risiko, aktivitas pengendalian, informasi dan komunikasi, serta pemantauan. Dalam konteks audit TI, auditor harus mengevaluasi apakah setiap komponen ini diterapkan dengan efektif untuk mengelola risiko yang berkaitan dengan teknologi

informasi, yang dapat mempengaruhi akurasi dan integritas laporan keuangan.

Salah satu langkah pertama dalam penerapan COSO adalah mengidentifikasi risiko yang berkaitan dengan TI. Risiko-risiko ini bisa meliputi kehilangan data yang disebabkan oleh bencana alam, kegagalan sistem, atau kesalahan manusia, serta potensi penipuan melalui penyalahgunaan akses pengguna terhadap sistem keuangan. Auditor harus menilai sejauh mana organisasi telah mengidentifikasi dan menilai risiko-risiko ini serta langkah-langkah yang telah diambil untuk mengurangi atau menghindari dampak negatifnya. Misalnya, pengendalian risiko dapat mencakup penggunaan enkripsi untuk melindungi data sensitif atau pengimplementasian kebijakan pengelolaan cadangan yang baik.

Setelah mengidentifikasi risiko, auditor harus mengevaluasi kegiatan pengendalian TI yang diterapkan oleh organisasi. Hal ini termasuk pengujian akses pengguna dan pengendalian otorisasi terhadap sistem keuangan. Misalnya, auditor akan menilai apakah ada kontrol yang membatasi akses pengguna hanya pada data dan sistem yang relevan dengan perannya, sehingga mengurangi risiko akses tidak sah atau manipulasi data. Pengendalian ini dapat mencakup penerapan sistem otentikasi yang kuat, pemisahan tugas (*segregation of duties*), serta audit trail untuk melacak aktivitas pengguna.

Pemantauan berkelanjutan adalah komponen penting dalam penerapan COSO. Auditor harus memastikan bahwa sistem pengendalian internal yang ada berfungsi sebagaimana mestinya dan dapat mendeteksi pelanggaran atau penyalahgunaan. Ini dapat dilakukan dengan menguji sistem secara berkala dan mengevaluasi laporan audit untuk memastikan bahwa kontrol yang ada efektif dalam mencegah kesalahan material atau penipuan. Jika ditemukan kelemahan atau kontrol yang tidak berfungsi dengan baik, auditor harus mengidentifikasi langkah-langkah perbaikan yang diperlukan untuk mengurangi risiko terhadap laporan keuangan.

b. Tantangan dalam Implementasi COSO untuk Audit TI Keuangan

Implementasi COSO dalam audit TI keuangan tidak tanpa tantangan, terutama dengan perkembangan pesat dalam teknologi

yang mempengaruhi sistem TI organisasi. Salah satu tantangan utama adalah kompleksitas teknologi yang terus berkembang. Sistem TI saat ini menjadi semakin canggih, melibatkan berbagai platform, perangkat lunak, dan infrastruktur yang saling terkait. Hal ini membuat auditor kesulitan dalam melakukan penilaian menyeluruh terhadap sistem TI. Sistem yang kompleks, seperti *cloud computing* atau teknologi berbasis *blockchain*, memerlukan pemahaman yang mendalam mengenai cara kerja teknologinya untuk mengidentifikasi potensi risiko dan kelemahan dalam pengendalian internal. Auditor harus mampu mengevaluasi risiko yang timbul dari integrasi berbagai sistem, serta dampaknya terhadap laporan keuangan.

Auditor menghadapi kesulitan dalam menilai pengendalian yang berbasis teknologi. Untuk mengevaluasi efektivitas pengendalian TI, auditor harus memiliki pengetahuan teknis yang kuat mengenai sistem yang digunakan oleh organisasi. Pengendalian yang mengandalkan teknologi, seperti sistem otentikasi dua faktor, enkripsi data, dan pemantauan *real-time*, membutuhkan pemahaman yang lebih dalam daripada sekadar prosedur manual atau berbasis dokumen. Tanpa pemahaman teknis yang cukup, auditor mungkin tidak dapat menilai dengan tepat apakah kontrol tersebut berfungsi sebagaimana mestinya atau bahkan mengidentifikasi kelemahan yang tersembunyi dalam pengaturan teknologi. Hal ini memerlukan pelatihan tambahan bagi auditor untuk memahami alat-alat TI yang digunakan dalam pengelolaan risiko.

C. Peraturan dan Standar Keuangan Global (SOX, Basel III, PCI DSS)

Di dunia yang semakin terhubung dan kompleks, regulasi dan standar internasional sangat penting dalam menjaga integritas dan transparansi sistem keuangan global. Salah satu aspek utama dalam audit IT keuangan adalah pemahaman terhadap standar dan peraturan yang mengatur pengelolaan informasi dan teknologi dalam sektor keuangan. Regulasi ini tidak hanya memastikan keandalan dan keamanan data keuangan, tetapi juga melindungi kepentingan semua pemangku kepentingan, baik itu pelanggan, investor, maupun lembaga pengawas.

Di antara regulasi yang paling penting dan berpengaruh dalam konteks audit IT keuangan adalah Sarbanes-Oxley Act (SOX), Basel III, dan Payment Card Industry Data Security Standard (PCI DSS).

1. *Sarbanes-Oxley Act* (SOX)

Sarbanes-Oxley Act (SOX) adalah sebuah undang-undang yang disahkan di Amerika Serikat pada tahun 2002 untuk melindungi investor dari kemungkinan penipuan perusahaan melalui peningkatan keandalan laporan keuangan perusahaan publik. SOX diterapkan setelah skandal keuangan besar seperti yang terjadi pada Enron dan WorldCom. Undang-undang ini memberikan pedoman yang jelas untuk pelaporan keuangan dan pengendalian internal yang harus diikuti oleh perusahaan publik. SOX memiliki tujuan utama untuk meningkatkan transparansi dalam laporan keuangan dan melindungi investor. Salah satu bagian yang paling penting dari SOX adalah ketentuan tentang pengendalian internal (*Internal Controls*) dalam laporan keuangan perusahaan. SOX mengharuskan perusahaan untuk membuktikan bahwa ia memiliki sistem pengendalian internal yang efektif untuk meminimalkan risiko penipuan dan memastikan keandalan data keuangan. Beberapa poin penting dalam SOX yang relevan dengan audit IT meliputi:

a. Section 404: Mengharuskan manajemen untuk menilai dan melaporkan efektivitas pengendalian internal, termasuk pengendalian TI yang terkait dengan integritas data dan pelaporan keuangan.
b. Section 302: Mengharuskan eksekutif perusahaan untuk menyatakan bahwa laporan keuangannya tidak mengandung informasi yang menyesatkan dan bahwa ia bertanggung jawab untuk memastikan keakuratan data.

SOX mempengaruhi audit IT karena sebagian besar aktivitas yang terkait dengan pengendalian internal perusahaan saat ini dilakukan menggunakan sistem informasi berbasis teknologi. Oleh karena itu, auditor perlu memverifikasi apakah pengendalian internal TI yang diterapkan memenuhi standar yang ditetapkan dalam SOX. Dalam audit IT keuangan, auditor harus:

a. Menilai pengendalian akses terhadap sistem TI yang digunakan dalam pelaporan keuangan.
b. Memastikan bahwa data tidak dimanipulasi oleh pihak yang tidak berwenang.

c. Memeriksa bahwa transaksi yang dilakukan dalam sistem TI tercatat dengan benar dan dapat diaudit.

2. Basel III

Basel III adalah serangkaian peraturan internasional yang ditetapkan oleh Bank for International Settlements (BIS) untuk memperkuat regulasi perbankan global dan memastikan stabilitas sistem keuangan internasional. Peraturan ini dimaksudkan untuk meningkatkan pengawasan terhadap bank-bank global, khususnya dalam hal pengelolaan risiko dan permodalan. Basel III adalah pengembangan dari Basel II, yang bertujuan untuk mengatasi kekurangan yang terungkap selama krisis keuangan global 2007-2008. Basel III bertujuan untuk meningkatkan daya tahan sektor perbankan terhadap gejolak ekonomi dan sistemik dengan memperkenalkan ketentuan yang lebih ketat mengenai pengelolaan risiko, likuiditas, dan permodalan. Beberapa ketentuan utama dari Basel III adalah:

a. Penguatan modal inti: Bank-bank harus memiliki lebih banyak modal untuk menahan potensi kerugian.
b. Peningkatan pengawasan risiko likuiditas: Bank diharuskan untuk memiliki sumber likuiditas yang cukup untuk bertahan dalam situasi krisis.
c. Peningkatan pengawasan terhadap risiko sistemik: Basel III berfokus pada pengawasan terhadap risiko yang dapat memengaruhi stabilitas sistem keuangan secara keseluruhan.

Basel III juga berfokus pada pentingnya sistem informasi yang kuat untuk memantau dan mengelola risiko keuangan. Dalam hal ini, audit TI berperan penting untuk memastikan bahwa teknologi informasi yang digunakan oleh bank-bank global memenuhi ketentuan yang ditetapkan oleh Basel III. Beberapa aspek yang relevan dengan audit IT dalam Basel III antara lain:

a. Pengelolaan risiko TI: Sistem TI harus mampu mendeteksi dan memitigasi risiko yang dapat memengaruhi stabilitas bank.
b. Keamanan dan integritas data: Data yang digunakan dalam perhitungan rasio modal dan risiko harus dijaga kerahasiaannya dan akurasinya.
c. Pemantauan transaksi: Penggunaan sistem informasi untuk memantau transaksi dan aktivitas yang dapat meningkatkan risiko sistemik.

3. *Payment Card Industry Data Security Standard* (PCI DSS)

PCI DSS adalah seperangkat standar yang dikembangkan oleh industri kartu pembayaran untuk melindungi data kartu pembayaran pelanggan dari potensi penyalahgunaan atau pencurian. Standar ini diterapkan untuk semua organisasi yang menyimpan, memproses, atau mentransmisikan informasi kartu pembayaran. PCI DSS bertujuan untuk memastikan bahwa informasi kartu pembayaran pelanggan tetap aman sepanjang proses transaksi. Tujuan utama dari PCI DSS adalah untuk mengurangi risiko kebocoran data kartu pembayaran dengan menerapkan serangkaian persyaratan keamanan yang ketat. PCI DSS mencakup berbagai aspek teknis dan prosedural yang dirancang untuk melindungi data sensitif, termasuk:

a. Pengamanan data yang disimpan: Mengharuskan organisasi untuk mengenkripsi data kartu yang disimpan.
b. Pengendalian akses: Memastikan hanya orang yang berwenang yang dapat mengakses data kartu.
c. Pemantauan dan pencatatan aktivitas: Semua transaksi yang melibatkan data kartu pembayaran harus tercatat dan dapat diaudit.

D. Prinsip-Prinsip Etika dalam Audit IT

Etika adalah seperangkat prinsip moral yang mengarahkan perilaku seseorang atau kelompok dalam suatu profesi. Dalam konteks audit TI, etika mengacu pada seperangkat norma yang harus diikuti oleh auditor dalam melaksanakan tugasnya untuk memastikan bahwa audit dilakukan dengan integritas, objektivitas, dan profesionalisme yang tinggi. Auditor TI memiliki tanggung jawab yang besar dalam memeriksa dan menilai sistem informasi yang mendasari laporan keuangan, sehingga prinsip-prinsip etika menjadi landasan untuk memastikan bahwa proses audit dilakukan dengan cara yang transparan dan akuntabel. Prinsip etika yang berlaku dalam audit TI dapat bervariasi berdasarkan regulasi dan pedoman profesional yang ada, seperti yang diatur oleh badan pengatur internasional dan asosiasi profesional seperti ISACA, ACFE, dan IFAC. Dalam praktik audit TI, ada beberapa prinsip etika yang harus dipegang teguh oleh setiap auditor. Prinsip-prinsip ini tidak hanya berfungsi untuk melindungi kepentingan semua pemangku

kepentingan, tetapi juga untuk menjaga kredibilitas dan profesionalisme profesi audit TI itu sendiri.

1. Integritas

Integritas adalah prinsip dasar dalam profesi audit, khususnya dalam audit teknologi informasi (TI), yang menuntut auditor untuk bertindak dengan kejujuran dan keterbukaan. Dalam konteks ini, auditor TI harus menyajikan temuan audit secara objektif dan akurat, tanpa terpengaruh oleh faktor eksternal yang dapat merusak integritas laporan. Menjaga integritas berarti auditor harus memastikan bahwa setiap informasi yang ditemukan selama proses audit disampaikan dengan jujur, meskipun hasil temuan tersebut dapat menimbulkan dampak negatif terhadap organisasi yang sedang diaudit. Jika ada ketidaksesuaian atau potensi risiko yang ditemukan, auditor harus melaporkannya secara jelas dan tepat.

Salah satu aspek penting dari integritas adalah kemampuan untuk menjaga kerahasiaan informasi yang diperoleh selama proses audit. Auditor TI seringkali bekerja dengan data yang sangat sensitif, seperti informasi keuangan, data pribadi, atau data pelanggan yang terkait dengan operasional TI perusahaan. Oleh karena itu, menjaga kerahasiaan ini adalah kewajiban yang sangat penting. Jika auditor tidak dapat menjaga kerahasiaan data yang diaudit, tidak hanya melanggar etika profesi, tetapi juga dapat merusak reputasi perusahaan dan mengurangi tingkat kepercayaan publik terhadap sektor audit itu sendiri.

2. Objektivitas

Objektivitas dalam audit TI adalah prinsip penting yang menuntut auditor untuk menjaga netralitas dan tidak terpengaruh oleh faktor eksternal atau pribadi saat melakukan evaluasi. Auditor TI harus menilai sistem dan data berdasarkan fakta yang ada, bukan berdasarkan preferensi pribadi atau opini yang mungkin mempengaruhi temuan audit. Hal ini penting agar hasil audit mencerminkan realitas objektif dari sistem yang diaudit, tanpa adanya distorsi yang dapat merugikan integritas laporan. Penerapan objektivitas ini mengharuskan auditor untuk fokus pada data yang akurat dan relevan, serta memastikan bahwa temuan audit tidak dipengaruhi oleh hubungan atau kepentingan pihak manapun.

Sebagai contoh dalam audit TI, auditor harus menghindari pengaruh pihak yang berkepentingan yang dapat mengarahkan hasil audit ke arah yang diinginkan oleh pihak tersebut, baik itu pihak manajemen atau pihak lain yang memiliki kepentingan tertentu. Jika auditor dipengaruhi oleh pihak-pihak ini, hasil audit bisa jadi tidak mencerminkan keadaan yang sebenarnya, dan ini bisa merusak kredibilitas temuan yang dibuat. Untuk itu, penting bagi auditor untuk tetap independen dan menjaga jarak dari segala bentuk tekanan yang dapat mempengaruhi penilaiannya.

3. Profesionalisme

Profesionalisme dalam audit TI adalah prinsip yang mengharuskan auditor untuk selalu mematuhi standar dan pedoman yang telah ditetapkan dalam profesinya. Auditor TI tidak hanya harus memahami teknologi informasi yang digunakan oleh organisasi, tetapi juga harus memiliki kemampuan teknis untuk mengevaluasi sistem TI dengan tepat. Hal ini mencakup pemahaman mendalam tentang infrastruktur TI, perangkat lunak yang digunakan, serta potensi risiko yang terkait dengan penggunaan teknologi tersebut dalam konteks laporan keuangan. Auditor juga harus memiliki keterampilan dalam menggunakan teknik dan alat audit yang efektif untuk menganalisis dan mengidentifikasi masalah dengan sistem TI yang ada.

Sebagai bentuk komitmen terhadap profesionalisme, auditor TI harus memiliki sertifikasi yang relevan seperti *Certified Information Systems Auditor* (CISA) atau *Certified Information Security Manager* (CISM). Sertifikasi ini tidak hanya menunjukkan bahwa auditor memiliki pengetahuan yang cukup, tetapi juga mengindikasikan bahwa auditor memiliki pemahaman yang mendalam tentang standar industri dan praktek terbaik dalam audit TI. Dengan sertifikasi yang diakui, auditor dapat memastikan bahwa ia mematuhi pedoman profesional yang dapat dipercaya dan diterima secara internasional.

4. Kerahasiaan

Kerahasiaan merupakan prinsip etika yang sangat penting dalam profesi audit, terutama dalam konteks audit TI. Auditor TI sering kali memiliki akses ke data yang sangat sensitif, seperti informasi keuangan perusahaan, data pribadi karyawan atau pelanggan, serta rincian teknis yang terkait dengan sistem TI organisasi. Oleh karena itu, menjaga

kerahasiaan informasi ini adalah tanggung jawab utama auditor. Setiap informasi yang diperoleh selama proses audit harus dilindungi agar tidak jatuh ke tangan yang salah atau disalahgunakan, yang dapat merugikan klien atau organisasi yang diaudit.

Penerapan kerahasiaan dalam audit TI tidak hanya melibatkan ketidakberterusan pengungkapan data, tetapi juga penggunaan langkah-langkah keamanan yang ketat. Auditor perlu memastikan bahwa data dan temuan yang diperoleh selama audit disimpan dan dikelola dengan aman. Hal ini mencakup penggunaan sistem keamanan siber yang canggih, seperti enkripsi data, kontrol akses berbasis peran, dan audit trail untuk melacak siapa yang mengakses informasi tersebut. Langkah-langkah ini mencegah akses yang tidak sah dan menjaga integritas data.

5. Tanggung Jawab

Tanggung jawab auditor TI sangat penting dalam menjamin bahwa audit yang dilakukan tidak hanya memenuhi standar yang ditetapkan, tetapi juga memberikan manfaat yang nyata bagi organisasi yang diaudit. Sebagai profesional, auditor harus memastikan bahwa temuan dan rekomendasi yang disampaikan kepada manajemen adalah akurat, jelas, dan tepat waktu. Temuan ini harus mencerminkan kenyataan yang ada di lapangan tanpa adanya bias atau pengaruh eksternal. Hal ini penting untuk memastikan bahwa manajemen dapat segera mengambil langkah perbaikan yang diperlukan untuk meningkatkan pengelolaan TI dan menjaga keamanan serta integritas sistem informasi organisasi (Hume *et al*., 2010).

Sebagai bagian dari tanggung jawab auditor juga harus mampu mengidentifikasi potensi masalah atau risiko yang mungkin tidak terlihat oleh organisasi. Dalam banyak kasus, organisasi mungkin tidak sepenuhnya menyadari adanya celah atau kelemahan dalam sistem TI, yang bisa berisiko besar jika tidak ditangani dengan tepat. Auditor TI harus memiliki kemampuan untuk menggali dan mengevaluasi sistem serta kontrol TI yang ada untuk menemukan potensi masalah yang dapat mengancam integritas dan keamanan data yang dimiliki oleh organisasi. Dengan pendekatan yang hati-hati dan teliti, auditor bisa memberikan gambaran yang lebih lengkap tentang kondisi sistem TI yang ada.

E. Studi Kasus: Implementasi Standar Internasional di Perusahaan Keuangan

Implementasi standar internasional dalam audit IT keuangan semakin penting seiring dengan semakin kompleksnya teknologi informasi dan kebutuhan akan transparansi yang lebih besar dalam pengelolaan data keuangan. Standar seperti ISO/IEC 27001, COBIT (*Control Objectives for Information and Related Technologies*), dan ITIL (*Information Technology Infrastructure Library*) telah menjadi kerangka utama dalam memastikan bahwa perusahaan keuangan mengelola sistem IT dengan aman, efektif, dan sesuai dengan regulasi yang berlaku.

1. Implementasi ISO/IEC 27001 oleh Bank HSBC

Implementasi ISO/IEC 27001 oleh HSBC merupakan langkah strategis untuk memastikan keamanan informasi di tengah kompleksitas operasional globalnya. ISO/IEC 27001 adalah standar internasional yang dirancang untuk menetapkan persyaratan sistem manajemen keamanan informasi (*Information Security Management System*/ISMS), termasuk kebijakan, prosedur, dan kontrol yang diperlukan untuk melindungi data organisasi dari ancaman siber. HSBC mengadopsi standar ini untuk memperkuat perlindungan data pelanggan, yang menjadi aset penting dalam industri keuangan. Penerapan ISO/IEC 27001 oleh HSBC diawali dengan identifikasi risiko keamanan informasi yang dihadapi perusahaan. Dalam proses ini, HSBC melakukan analisis risiko secara menyeluruh untuk memahami potensi ancaman terhadap sistem teknologi informasi dan data. Standar ISO/IEC 27001 memberikan kerangka kerja yang terstruktur untuk mengelola risiko ini, termasuk melalui pengendalian akses, pelatihan karyawan, dan pemantauan terus-menerus terhadap aktivitas sistem.

Langkah penting lainnya adalah integrasi proses audit IT secara teratur untuk menilai kepatuhan HSBC terhadap persyaratan ISO/IEC 27001. Proses ini mencakup pengujian sistem dan jaringan yang digunakan untuk memproses transaksi keuangan guna memastikan bahwa sesuai dengan standar keamanan yang tinggi. Audit ini membantu HSBC mengidentifikasi dan memperbaiki kelemahan keamanan sebelum dapat dieksploitasi oleh pihak tidak bertanggung jawab. Selain itu, HSBC mengimplementasikan kebijakan dan prosedur yang jelas

untuk pengelolaan keamanan informasi. ISO/IEC 27001 memberikan panduan untuk mendokumentasikan kebijakan, memastikan kepatuhan karyawan, dan mengintegrasikan manajemen risiko ke dalam strategi bisnis. Pendekatan ini memungkinkan HSBC untuk secara proaktif menangani ancaman yang muncul dan mempertahankan kepercayaan pelanggan.

Pentingnya ISO/IEC 27001 bagi HSBC tidak hanya terletak pada perlindungan data tetapi juga pada peningkatan efisiensi operasional. Dengan menerapkan kontrol yang konsisten di seluruh cabang globalnya, HSBC dapat memastikan bahwa semua proses terkait IT dan keamanan informasi dikelola dengan cara yang seragam dan optimal. Hal ini juga membantu mematuhi berbagai peraturan privasi data di berbagai negara tempatnya beroperasi. Keuntungan lain dari penerapan ISO/IEC 27001 adalah kemampuannya untuk meningkatkan transparansi dan akuntabilitas dalam pengelolaan data. Dengan memiliki sistem manajemen keamanan informasi yang terdokumentasi dengan baik, HSBC dapat menunjukkan kepada pemangku kepentingan bahwa ia serius dalam melindungi data pelanggan dan informasi sensitif lainnya. Ini menjadi faktor penting dalam mempertahankan kepercayaan investor dan klien.

2. Penerapan COBIT di Barclays

Penerapan COBIT di Barclays merupakan contoh nyata bagaimana framework tata kelola IT dapat mendukung pengelolaan data keuangan dan proses bisnis secara keseluruhan. COBIT (*Control Objectives for Information and Related Technologies*) adalah framework yang dirancang untuk memastikan pengelolaan dan pengendalian teknologi informasi secara efektif, dengan fokus pada keselarasan antara strategi IT dan tujuan bisnis. Dengan menggunakan COBIT, Barclays mampu memastikan bahwa tata kelola IT mendukung pengambilan keputusan yang strategis, melindungi aset digital, dan memenuhi persyaratan regulasi yang berlaku. Salah satu alasan utama Barclays mengadopsi COBIT adalah untuk memitigasi risiko yang berkaitan dengan pengelolaan data keuangan. Sebagai lembaga keuangan global, Barclays menghadapi tantangan besar dalam mengelola volume data yang besar dan sensitif. Framework COBIT memberikan panduan dalam mengevaluasi kontrol internal, mengelola risiko, dan menetapkan standar yang jelas untuk tata kelola IT. Dengan demikian, Barclays dapat

mengidentifikasi potensi kerentanan dalam sistem dan mengambil langkah proaktif untuk mengatasinya.

COBIT juga membantu Barclays dalam memenuhi persyaratan regulasi yang ketat dalam sektor keuangan. Regulasi seperti *General Data Protection Regulation* (GDPR) dan berbagai peraturan perbankan internasional memerlukan sistem tata kelola IT yang solid. Dengan menerapkan COBIT, Barclays dapat memastikan kepatuhan terhadap regulasi ini melalui dokumentasi yang transparan dan prosedur audit yang sistematis, sehingga meningkatkan kredibilitas di mata regulator dan pemangku kepentingan. Selain itu, framework COBIT memungkinkan Barclays untuk menyesuaikan prosedur audit dengan lebih baik. COBIT menyediakan metrik dan indikator kinerja yang membantu Barclays mengevaluasi efektivitas kontrol IT. Prosedur ini dirancang untuk memprioritaskan area-area dengan risiko tinggi, seperti keamanan data dan keberlanjutan operasional, sehingga mengoptimalkan alokasi sumber daya audit.

Penerapan COBIT di Barclays juga memperkuat transparansi dalam pengelolaan IT. Dengan adanya panduan yang terstandarisasi, Barclays dapat memastikan bahwa semua departemen IT bekerja dalam kerangka yang sama, yang tidak hanya meningkatkan efisiensi tetapi juga akuntabilitas. Hal ini sangat penting dalam sektor perbankan, di mana kepercayaan pelanggan sangat bergantung pada kemampuan lembaga untuk melindungi informasi sensitif. Selain untuk mitigasi risiko, Barclays juga menggunakan COBIT untuk mendukung inovasi dalam operasional. Framework ini memungkinkan organisasi untuk mengintegrasikan teknologi baru dengan lebih aman dan efisien, tanpa mengorbankan tata kelola atau kepatuhan. Dengan memanfaatkan teknologi modern seperti big data dan *cloud computing* dalam kerangka COBIT, Barclays dapat menciptakan nilai lebih besar bagi pelanggan dan pemegang saham.

3. Penerapan ITIL oleh JP Morgan Chase

JP Morgan Chase, salah satu bank investasi terbesar di dunia, telah berhasil menerapkan ITIL (*Information Technology Infrastructure Library*) untuk meningkatkan kualitas layanan teknologi informasi yang disediakan. ITIL adalah kumpulan praktik terbaik yang dirancang untuk memastikan bahwa pengelolaan layanan IT dilakukan secara efisien, konsisten, dan dapat diandalkan. Melalui pendekatan ITIL, JP Morgan

Chase dapat memanfaatkan berbagai proses, seperti manajemen insiden, pengelolaan masalah, serta manajemen perubahan, guna memastikan bahwa sistem dan infrastruktur IT berjalan dengan lancar dan mendukung operasional bisnis secara optimal. Dalam penerapan ITIL, JP Morgan Chase menekankan pentingnya manajemen insiden untuk mengidentifikasi dan menyelesaikan gangguan yang terjadi pada layanan IT dengan cepat. Hal ini penting untuk memastikan bahwa layanan keuangan, termasuk transaksi *real-time* dan analitik keuangan, tetap berjalan tanpa hambatan. Dengan pendekatan ini, tim IT JP Morgan dapat memitigasi dampak insiden pada waktu yang tepat, sehingga mengurangi risiko kerugian finansial maupun reputasi.

Pengelolaan masalah menjadi komponen penting dalam strategi ITIL JP Morgan Chase. Proses ini berfokus pada identifikasi akar penyebab insiden yang berulang, memungkinkan tim IT untuk mengambil langkah preventif dalam mengurangi risiko yang sama di masa depan. Dengan melakukan analisis mendalam terhadap masalah sistem, bank ini berhasil meningkatkan stabilitas dan keandalan layanan teknologi, memberikan pengalaman yang lebih baik bagi pelanggan dan pemangku kepentingan. Manajemen perubahan juga menjadi salah satu pilar utama dalam penerapan ITIL di JP Morgan Chase. Proses ini memastikan bahwa setiap perubahan dalam infrastruktur IT, seperti pembaruan perangkat lunak atau implementasi teknologi baru, dilakukan dengan perencanaan yang matang dan risiko yang minimal. Dengan demikian, JP Morgan dapat mengadopsi inovasi teknologi tanpa mengganggu operasional yang sudah berjalan, mendukung kebutuhan bisnis yang dinamis di sektor keuangan.

Untuk mendukung penerapan ITIL, JP Morgan Chase juga rutin melakukan audit terhadap infrastruktur IT. Audit ini bertujuan untuk memastikan bahwa proses yang diadopsi sudah sesuai dengan standar ITIL dan dapat mengidentifikasi area yang membutuhkan peningkatan. Dengan audit yang terstruktur, JP Morgan tidak hanya meningkatkan efisiensi operasional, tetapi juga mengurangi risiko terkait keamanan data dan kerentanan sistem. Penggunaan ITIL juga memberikan keuntungan bagi tim audit internal di JP Morgan. Framework ini membantu untuk mengevaluasi risiko teknologi dengan lebih terfokus, mengidentifikasi ketergantungan teknologi dalam proses bisnis, dan memastikan bahwa semua kontrol IT memenuhi standar keamanan dan keandalan. Hal ini menjadi penting di industri keuangan yang sangat

bergantung pada teknologi untuk mendukung operasional dan kepatuhan regulasi.

4. Penerapan ISO 20000 di Standard Chartered

Standard Chartered, sebagai salah satu bank internasional terkemuka, mengimplementasikan ISO 20000 untuk meningkatkan pengelolaan layanan TI. ISO 20000 adalah standar internasional yang berfokus pada manajemen layanan TI, memastikan bahwa organisasi mampu memberikan layanan yang konsisten, efisien, dan memenuhi kebutuhan bisnis serta pelanggan. Implementasi ini mencakup pengelolaan infrastruktur IT, manajemen insiden, dan pengelolaan perubahan, dengan tujuan utama menjaga kualitas dan keandalan layanan yang digunakan dalam proses perbankan. Melalui penerapan ISO 20000, Standard Chartered mampu mengidentifikasi kelemahan dalam pengelolaan layanan TI dan mengambil langkah-langkah untuk meningkatkan efisiensi operasional. Standar ini menyediakan kerangka kerja yang jelas untuk memastikan bahwa layanan IT dikelola sesuai dengan tujuan strategis organisasi. Selain itu, proses ini membantu mengurangi risiko yang terkait dengan kegagalan sistem atau pelanggaran keamanan data, yang menjadi perhatian utama di industri keuangan yang sangat bergantung pada teknologi.

Salah satu manfaat utama dari penerapan ISO 20000 di Standard Chartered adalah peningkatan kualitas audit TI. Dengan standar ini, audit internal dan eksternal dapat dilakukan dengan lebih terstruktur, memungkinkan auditor untuk mengevaluasi efektivitas layanan TI berdasarkan parameter yang terstandar. Hal ini menciptakan transparansi dalam pengelolaan layanan IT dan membantu memastikan kepatuhan terhadap regulasi yang berlaku di berbagai yurisdiksi. Penerapan ISO 20000 juga mendukung Standard Chartered dalam menjaga kepercayaan pelanggan. Dengan infrastruktur TI yang kuat dan pengelolaan layanan yang terstandar, bank ini dapat memberikan layanan perbankan yang andal dan aman. Standar ini juga memungkinkan untuk merespons kebutuhan pelanggan dengan cepat, terutama dalam menangani insiden yang dapat memengaruhi pengalaman pengguna atau integritas data pelanggan.

ISO 20000 memberikan keunggulan kompetitif bagi Standard Chartered. Bank ini dapat membedakan dirinya di pasar dengan menunjukkan komitmen terhadap kualitas layanan TI. Dalam konteks

persaingan global, standar internasional ini menjadi alat yang penting untuk memastikan bahwa layanan memenuhi ekspektasi pelanggan dan persyaratan regulator di berbagai negara. Proses implementasi ISO 20000 melibatkan perubahan signifikan dalam budaya kerja TI di Standard Chartered. Organisasi ini harus memastikan bahwa seluruh tim memahami pentingnya standar tersebut dan memiliki pelatihan yang memadai untuk menjalankannya. Kolaborasi lintas departemen menjadi kunci dalam memastikan bahwa seluruh aspek layanan TI mendukung tujuan strategis dan operasional organisasi.

BAB IV
PROSES DAN METODOLOGI AUDIT IT DALAM KEUANGAN

Audit IT dalam sektor keuangan berperan yang sangat penting dalam menjaga integritas dan keamanan sistem informasi yang mendukung operasi keuangan. Proses audit ini mencakup berbagai tahapan yang bertujuan untuk mengevaluasi efektivitas kontrol internal, keamanan data, dan kepatuhan terhadap regulasi yang relevan. Auditor IT harus memahami bagaimana sistem TI berinteraksi dengan sistem keuangan dan memastikan bahwa proses ini berjalan dengan efisien dan aman. Metodologi audit IT yang digunakan dalam industri keuangan melibatkan berbagai teknik dan alat untuk menilai risiko, efektivitas kontrol, serta kerentanannya terhadap ancaman atau kesalahan operasional. Salah satu metode yang sering digunakan adalah pendekatan berbasis risiko (*risk-based approach*), di mana auditor menilai dan memprioritaskan area yang memiliki risiko tertinggi. Metode lain yang digunakan adalah Continuous Monitoring, di mana audit dilakukan secara berkelanjutan untuk memantau perubahan dan mendeteksi anomali yang mungkin menunjukkan masalah keamanan atau ketidakpatuhan.

A. Tahapan Utama dalam Audit IT

Tahapan audit TI dalam sektor keuangan mengikuti metodologi tertentu yang bertujuan untuk mengidentifikasi, mengevaluasi, dan memperbaiki sistem TI yang ada. Audit ini dapat dilakukan baik secara internal oleh auditor internal maupun eksternal yang disewa oleh perusahaan untuk melakukan penilaian independen. Proses audit IT pada perusahaan keuangan secara umum melibatkan lima tahapan utama, yaitu perencanaan, pengumpulan bukti, evaluasi sistem, pengujian

kontrol, dan pelaporan hasil audit. Setiap tahapan memiliki tujuan yang jelas untuk memastikan bahwa sistem informasi di perusahaan keuangan berfungsi sesuai dengan yang diinginkan dan mematuhi regulasi yang berlaku.

1. Tahap Perencanaan Audit IT

Tahap perencanaan adalah fondasi dari setiap audit, termasuk audit IT dalam sektor keuangan. Di tahap ini, auditor dan manajemen TI bekerja sama untuk menetapkan tujuan audit dan ruang lingkupnya, yang mencakup area-area sistem TI yang akan diaudit, seperti aplikasi perangkat lunak, basis data, dan infrastruktur jaringan. Perencanaan yang baik memastikan bahwa auditor memiliki pemahaman yang jelas mengenai fokus audit, risiko yang ada, dan alat yang dibutuhkan untuk audit tersebut. Langkah-Langkah Perencanaan:

a. Pemahaman Terhadap Lingkungan TI: Auditor mulai dengan mempelajari sistem TI yang digunakan di perusahaan, termasuk perangkat keras, perangkat lunak, dan proses bisnis yang didukung oleh TI tersebut. Ini melibatkan wawancara dengan personel TI dan kajian dokumen yang ada.
b. Penilaian Risiko: Salah satu elemen penting dalam perencanaan adalah penilaian risiko yang berkaitan dengan TI. Auditor harus mengevaluasi potensi risiko yang dihadapi oleh sistem TI, seperti risiko kebocoran data, serangan siber, atau kesalahan dalam pengolahan data.
c. Menetapkan Tujuan dan Lingkup Audit: Setelah memahami risiko, auditor menentukan tujuan audit dan ruang lingkupnya. Tujuan ini bisa berkisar dari memastikan kepatuhan terhadap regulasi tertentu hingga mengevaluasi efektivitas kontrol internal di sistem TI.

2. Pengumpulan Bukti Audit

Pengumpulan bukti adalah tahapan yang sangat penting dalam audit TI. Auditor akan mengumpulkan informasi dan data yang relevan untuk mengevaluasi apakah sistem TI perusahaan berfungsi sebagaimana mestinya dan mematuhi standar yang berlaku. Pada tahap ini, auditor akan menggunakan berbagai metode untuk mengumpulkan bukti, seperti wawancara dengan staf TI, pemeriksaan dokumentasi,

pengujian transaksi, dan observasi langsung. Metode Pengumpulan Bukti:

a. Pemeriksaan Dokumentasi: Auditor akan memeriksa dokumen yang terkait dengan pengelolaan TI, seperti kebijakan keamanan informasi, prosedur pengendalian akses, dan manual operasi sistem TI. Pemeriksaan ini bertujuan untuk menilai apakah dokumentasi tersebut mencerminkan pengelolaan yang baik dan sesuai dengan kebijakan yang berlaku.
b. Wawancara dengan Personel TI: Auditor melakukan wawancara dengan personel TI dan staf lainnya untuk memperoleh pemahaman tentang proses, kontrol, dan kebijakan yang berlaku dalam pengelolaan TI. Wawancara juga memberikan wawasan tentang potensi masalah atau area yang memerlukan perhatian lebih lanjut.
c. Pengujian Transaksi: Auditor melakukan pengujian terhadap transaksi yang dilakukan dalam sistem TI untuk memastikan bahwa data yang diproses dan dicatat dalam sistem keuangan adalah akurat dan sesuai dengan ketentuan.
d. Observasi Sistem dan Infrastruktur: Auditor akan memeriksa infrastruktur TI yang ada, seperti jaringan, server, dan perangkat keras lainnya, untuk menilai apakah sistem tersebut cukup aman dan efektif dalam mendukung operasi keuangan.

3. Evaluasi Sistem dan Kontrol IT

Setelah bukti dikumpulkan, tahap selanjutnya adalah mengevaluasi sistem TI dan kontrol yang diterapkan. Auditor menilai apakah kontrol yang ada memadai untuk mengelola risiko yang telah diidentifikasi sebelumnya. Evaluasi ini mencakup penilaian terhadap berbagai jenis kontrol TI, termasuk kontrol fisik, logis, administratif, dan pengendalian akses. Langkah-Langkah Evaluasi:

a. Penilaian Pengendalian Akses: Auditor akan menilai kebijakan pengendalian akses yang diterapkan pada sistem TI, memastikan bahwa hanya personel yang berwenang yang dapat mengakses data dan aplikasi kritis. Ini mencakup pengujian otentikasi dan otorisasi dalam sistem.
b. Uji Keamanan Sistem: Auditor juga menguji apakah sistem TI dilindungi dari ancaman luar, seperti serangan dunia maya. Ini

meliputi pengujian terhadap kebijakan dan praktik keamanan data, serta ketahanan infrastruktur TI terhadap serangan siber.

c. Penilaian Integritas Data: Auditor memverifikasi apakah data yang diproses oleh sistem TI adalah akurat dan tidak terkontaminasi oleh kesalahan atau manipulasi. Ini termasuk memeriksa data transaksi dan pelaporan keuangan yang dihasilkan oleh sistem.

4. Pengujian Kontrol

Pengujian kontrol dilakukan untuk mengevaluasi apakah kontrol yang ada berfungsi sebagaimana mestinya dan efektif dalam memitigasi risiko yang teridentifikasi. Auditor akan menguji berbagai jenis kontrol, termasuk kontrol akses, kontrol pengolahan data, dan kontrol pelaporan keuangan. Pengujian ini memastikan bahwa kontrol TI yang diterapkan dapat mendeteksi dan mencegah kesalahan atau penyimpangan dalam sistem. Jenis Pengujian Kontrol:

a. Pengujian Pengendalian Proses: Auditor menguji kontrol yang diterapkan untuk memastikan bahwa data dan transaksi diproses dengan benar dalam sistem TI. Ini mencakup uji integritas data dan kelengkapan pelaporan keuangan.
b. Pengujian Keamanan: Pengujian keamanan melibatkan evaluasi kontrol perlindungan data dan pertahanan terhadap ancaman eksternal, seperti serangan dunia maya. Auditor menguji apakah kontrol yang diterapkan cukup kuat untuk menjaga kerahasiaan dan integritas data.
c. Pengujian Kepatuhan terhadap Regulasi: Auditor juga memverifikasi apakah sistem TI mematuhi regulasi yang berlaku, seperti SOX (*Sarbanes-Oxley*) atau GDPR, yang mengatur perlindungan data dan akuntabilitas pelaporan keuangan.

5. Pelaporan Hasil Audit

Tahap terakhir dari audit IT adalah pelaporan hasil audit kepada manajemen perusahaan dan pemangku kepentingan lainnya. Dalam tahap ini, auditor menyusun laporan yang menjelaskan temuan-temuan audit, termasuk hasil pengujian kontrol, identifikasi kelemahan dalam sistem, dan rekomendasi untuk perbaikan. Komponen Laporan Audit:

a. Ringkasan Temuan: Laporan audit berisi ringkasan temuan-temuan utama yang ditemukan selama audit, termasuk masalah

yang diidentifikasi terkait dengan kontrol, keamanan, atau integritas sistem TI.

b. Rekomendasi Perbaikan: Auditor memberikan rekomendasi perbaikan untuk memperbaiki kelemahan dalam sistem TI yang telah ditemukan. Rekomendasi ini dapat mencakup peningkatan kontrol akses, implementasi teknologi baru, atau perubahan prosedur operasional.
c. Penilaian Kepatuhan: Auditor juga menilai apakah sistem TI perusahaan mematuhi regulasi yang relevan, seperti Sarbanes-Oxley atau Basel III, serta memberikan rekomendasi untuk memastikan bahwa sistem TI selalu mematuhi standar yang berlaku.

B. Identifikasi Risiko dan Pengendalian IT

Identifikasi risiko dan pengendalian TI dalam audit IT di sektor keuangan merujuk pada proses untuk mengenali dan menilai potensi ancaman terhadap sistem TI yang dapat memengaruhi keandalan dan kepatuhan pelaporan keuangan. Risiko ini dapat datang dari berbagai sumber, termasuk ancaman eksternal seperti serangan dunia maya, serta ancaman internal terkait dengan kesalahan manusia atau kegagalan sistem. Pengendalian TI, yang terdiri dari kebijakan, prosedur, dan alat teknologi, digunakan untuk mencegah, mendeteksi, dan mengatasi risiko-risiko ini. Dalam konteks audit IT, auditor bertugas untuk mengevaluasi efektivitas pengendalian yang diterapkan oleh organisasi dan memastikan bahwa pengendalian tersebut sesuai dengan standar yang berlaku serta mampu mengurangi risiko yang ada.

1. Jenis-Jenis Risiko TI dalam Keuangan

Sebelum membahas pengendalian TI, penting untuk memahami jenis-jenis risiko yang mungkin muncul dalam sistem TI di sektor keuangan. Risiko-risiko ini dapat dibagi ke dalam beberapa kategori utama yang berhubungan langsung dengan keuangan dan operasional perusahaan.

a. Risiko Keamanan (*Security Risk*)

Risiko keamanan adalah salah satu jenis risiko TI yang paling kritikal. Risiko ini terkait dengan potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan data yang diproses oleh

sistem TI. Ancaman seperti peretasan, virus, dan serangan ransomware dapat merusak data dan menyebabkan kerugian finansial yang besar, serta merusak reputasi organisasi.

b. Risiko Keandalan Sistem (*System Reliability Risk*)

Keandalan sistem TI dalam sektor keuangan sangat penting karena setiap gangguan dapat menghambat transaksi keuangan dan memengaruhi kualitas laporan keuangan. Risiko ini berkaitan dengan potensi kegagalan teknis atau kerusakan perangkat keras dan perangkat lunak yang dapat memengaruhi kelangsungan operasional.

c. Risiko Kepatuhan (*Compliance Risk*)

Risiko kepatuhan berhubungan dengan pelanggaran terhadap regulasi dan standar yang berlaku, seperti SOX (*Sarbanes-Oxley Act*), GDPR (*General Data Protection Regulation*), atau regulasi yang lebih spesifik dalam sektor keuangan. Pelanggaran dapat mengarah pada sanksi hukum dan denda yang signifikan.

d. Risiko Operasional (*Operational Risk*)

Risiko operasional dalam konteks TI merujuk pada risiko yang muncul dari kesalahan atau kelalaian dalam pengelolaan dan penggunaan sistem TI. Ini termasuk kesalahan manusia, kesalahan proses, atau kegagalan dalam proses otomatisasi yang memengaruhi transaksi keuangan.

2. Pengendalian IT dalam Keuangan

Pengendalian TI digunakan untuk mengelola dan memitigasi risiko yang teridentifikasi dalam sistem TI. Pengendalian ini terdiri dari langkah-langkah yang dirancang untuk memastikan bahwa sistem TI berfungsi dengan baik, mengamankan data, dan mematuhi peraturan yang berlaku. Pengendalian TI dapat dibagi dalam beberapa kategori utama:

a. Pengendalian Akses (*Access Control*)

Pengendalian akses adalah salah satu jenis pengendalian yang paling fundamental dalam sistem TI. Pengendalian ini memastikan bahwa hanya individu yang berwenang yang dapat mengakses data dan aplikasi sensitif. Pengendalian akses yang baik mencakup otentikasi, otorisasi, dan audit trail untuk memastikan bahwa aktivitas di dalam sistem dapat dipantau dan dikendalikan.

b. Pengendalian Keamanan Data (*Data Security Controls*)

Pengendalian keamanan data bertujuan untuk melindungi data dari ancaman eksternal dan internal. Ini termasuk penggunaan enkripsi untuk melindungi data dalam transmisi dan penyimpanan, serta pengaturan hak akses yang ketat untuk mencegah pengungkapan data yang tidak sah.

c. Pengendalian Integritas Sistem (*System Integrity Controls*)

Pengendalian integritas sistem memastikan bahwa data dan transaksi yang diproses oleh sistem TI adalah akurat dan tidak rusak. Ini termasuk pengujian terhadap kesalahan atau ketidaksesuaian dalam pengolahan data serta penerapan prosedur untuk menjaga keandalan data yang diproses.

d. Pengendalian Kepatuhan (*Compliance Controls*)

Pengendalian kepatuhan memastikan bahwa sistem TI dan operasi keuangan organisasi mematuhi regulasi yang berlaku. Pengendalian ini dapat mencakup kebijakan dan prosedur untuk melaksanakan audit internal secara berkala, memastikan kepatuhan terhadap regulasi pelaporan keuangan, serta memitigasi risiko terkait privasi data.

3. Proses Identifikasi Risiko dan Pengendalian TI dalam Audit

Audit TI yang efektif melibatkan identifikasi dan evaluasi risiko serta pengendalian yang diterapkan untuk mengurangi risiko-risiko tersebut. Proses identifikasi risiko dan pengendalian TI umumnya mengikuti beberapa langkah utama:

a. Penilaian Risiko (*Risk Assessment*)

Setelah ancaman diidentifikasi, auditor melanjutkan dengan penilaian dampak dari risiko tersebut. Penilaian ini bertujuan untuk mengevaluasi seberapa besar kerugian yang dapat ditimbulkan jika risiko tersebut terjadi. Dampak yang ditimbulkan bisa bersifat finansial, seperti kerugian akibat pencurian data atau transaksi tidak sah, atau dapat berdampak pada reputasi organisasi, misalnya kerusakan kepercayaan klien atau pemangku kepentingan lainnya. Penilaian dampak juga meliputi aspek operasional, seperti gangguan dalam kelancaran proses bisnis yang diakibatkan oleh kegagalan sistem (Otero, 2020).

b. Evaluasi Pengendalian TI (*Control Evaluation*)

Setelah risiko TI diidentifikasi, langkah berikutnya dalam audit TI adalah evaluasi pengendalian TI yang diterapkan oleh organisasi. Pengendalian ini harus diuji untuk memastikan bahwa ia efektif dalam mengurangi atau mengelola risiko yang telah teridentifikasi. Auditor akan melakukan uji pengendalian untuk menilai sejauh mana kontrol yang diterapkan berfungsi sesuai dengan tujuan yang telah ditetapkan. Ini melibatkan pemeriksaan terhadap prosedur pengendalian yang ada, seperti kontrol akses, pengamanan data, atau pemantauan aktivitas sistem, untuk memastikan bahwa kontrol tersebut dijalankan dengan benar dan konsisten.

c. Pengujian Kesesuaian (*Compliance Testing*)

Pengujian kesesuaian (*compliance testing*) merupakan salah satu tahap penting dalam audit TI untuk memastikan bahwa sistem informasi yang digunakan oleh organisasi mematuhi regulasi dan standar yang berlaku. Pengujian ini bertujuan untuk memverifikasi bahwa pengendalian yang diterapkan oleh organisasi sesuai dengan ketentuan yang ditetapkan oleh regulator dan standar internasional. Sebagai bagian dari audit ini, auditor akan memeriksa apakah organisasi mengikuti regulasi yang terkait dengan perlindungan data, privasi, dan keamanan informasi. Misalnya, jika organisasi beroperasi di Uni Eropa, auditor akan memastikan bahwa sistem TI mematuhi ketentuan dalam GDPR (*General Data Protection Regulation*) terkait pengelolaan data pribadi.

C. Pengumpulan dan Analisis Data Digital

Pada audit TI di sektor keuangan, pengumpulan dan analisis data digital adalah komponen yang sangat penting untuk menilai integritas dan keamanan sistem informasi yang digunakan oleh organisasi. Proses ini bertujuan untuk memperoleh bukti yang cukup dan relevan mengenai kinerja sistem TI, mengidentifikasi potensi risiko, dan memastikan kepatuhan terhadap regulasi yang berlaku, baik internal maupun eksternal. Dengan berkembangnya teknologi digital, semakin banyak data yang dihasilkan, yang memerlukan pendekatan sistematis untuk mengumpulkan, menganalisis, dan memverifikasi informasi tersebut

dalam audit IT keuangan. Pengumpulan dan analisis data digital tidak hanya mencakup data keuangan, tetapi juga data yang terkait dengan sistem, aplikasi, infrastruktur TI, dan catatan operasional yang dapat memberikan wawasan tentang keadaan dan efektivitas pengendalian TI. Penggunaan teknik analitik dan forensik dalam audit TI semakin berkembang untuk memastikan data yang dihasilkan dapat diandalkan dan relevan dengan tujuan audit.

1. Pengumpulan Data Digital dalam Audit TI

Pengumpulan data digital dalam audit TI mencakup proses untuk mendapatkan informasi yang relevan dari berbagai sumber dalam sistem TI, termasuk perangkat keras, perangkat lunak, aplikasi, dan catatan transaksi. Pengumpulan data ini dapat dilakukan melalui berbagai metode, yang masing-masing memiliki tujuan spesifik tergantung pada aspek yang sedang diaudit.

a. Sumber Data Digital dalam Audit TI

Data digital yang dikumpulkan dalam audit TI dapat mencakup berbagai jenis informasi, seperti:

1) Data Transaksi Keuangan

Ini termasuk semua data terkait transaksi keuangan yang diproses oleh sistem TI, seperti transaksi perbankan, pemrosesan pembayaran, atau pencatatan investasi. Data ini biasanya tersedia dalam sistem database yang terintegrasi dengan aplikasi keuangan.

2) Log Aktivitas Pengguna (*User Logs*)

Log aktivitas yang tercatat selama penggunaan sistem penting untuk audit. Log ini mencakup informasi tentang login, logout, perubahan akses, dan perintah sistem yang dilakukan oleh pengguna. Auditor dapat menganalisis log untuk mendeteksi perilaku yang mencurigakan atau tidak sah.

3) Data Sistem dan Infrastruktur TI

Ini meliputi catatan dan konfigurasi sistem TI, termasuk pengaturan server, aplikasi, dan database. Data ini memberikan gambaran tentang struktur teknis organisasi dan potensi kerentanannya.

4) Backup Data

Data cadangan (*backup*) sering kali digunakan untuk memulihkan sistem yang rusak atau hilang. Pemeriksaan

backup ini penting untuk memastikan bahwa data tersebut dapat dipulihkan dan diandalkan jika terjadi kegagalan sistem.

5) Dokumentasi Pengendalian Internal

Dokumentasi terkait kebijakan dan prosedur TI yang diterapkan oleh organisasi. Ini mencakup dokumentasi tentang prosedur keamanan, kontrol akses, serta audit dan pemantauan sistem yang ada.

b. Metode Pengumpulan Data Digital

Pengumpulan data dalam audit TI dapat dilakukan dengan berbagai teknik dan alat. Beberapa metode yang umum digunakan dalam pengumpulan data digital adalah sebagai berikut:

1) Forensik Digital

Forensik digital adalah proses yang digunakan untuk mengidentifikasi, mengumpulkan, dan memulihkan data yang tersembunyi atau hilang dari perangkat digital. Teknik ini sangat penting dalam audit TI untuk memperoleh bukti yang mungkin tidak dapat diakses melalui metode konvensional. Dalam konteks audit, forensik digital membantu auditor untuk menemukan data yang mungkin telah dihapus, rusak, atau sengaja disembunyikan. Hal ini dilakukan melalui penggunaan perangkat lunak khusus yang dapat mengekstrak data dari sistem yang tampaknya tidak dapat diakses atau rusak.

Proses forensik digital melibatkan langkah-langkah seperti pengambilan citra disk, yang merupakan salinan bit-by-bit dari media penyimpanan, termasuk data yang telah dihapus atau tersembunyi. Setelah citra diambil, auditor dapat menganalisisnya untuk menemukan informasi yang relevan. Misalnya, meskipun data telah dihapus, jejak digital atau file yang tersisa mungkin masih ada di sistem, dan teknik pemulihan data dapat digunakan untuk mengakses informasi tersebut. Proses ini juga memastikan bahwa bukti yang ditemukan tetap utuh dan tidak rusak, menjaga integritas data yang akan digunakan dalam proses audit.

2) Pengumpulan Data Menggunakan Alat Otomatisasi

Pengumpulan data menggunakan alat otomatisasi adalah teknik yang sangat efisien dalam proses audit TI. Alat otomatisasi memungkinkan auditor untuk secara cepat dan akurat mengumpulkan data dari berbagai sistem yang terhubung, termasuk sistem keuangan, aplikasi manajemen sumber daya perusahaan (ERP), dan platform lainnya yang menyimpan informasi kritis. Dengan menggunakan alat otomatisasi, auditor dapat mengekstrak data transaksi keuangan, log sistem, dan laporan lainnya secara langsung dari sumber data tanpa harus bergantung pada proses manual yang rawan kesalahan dan memakan waktu.

Alat otomatisasi juga membantu meningkatkan cakupan dan akurasi pengumpulan data. Alat ini dapat secara otomatis mengakses dan mengekstrak data dalam jumlah besar dari berbagai aplikasi dan perangkat yang digunakan dalam organisasi. Hal ini sangat penting dalam audit TI karena data yang relevan tidak hanya terletak pada satu sumber atau aplikasi, melainkan tersebar di berbagai sistem. Dengan alat otomatisasi, auditor dapat dengan mudah mengakses data dari berbagai platform dan memastikan bahwa informasi yang diambil adalah lengkap dan konsisten, tanpa kehilangan detail yang penting.

3) Pemantauan Sistem secara Langsung (*Real-time Monitoring*)

Pemantauan sistem secara langsung (*real-time monitoring*) adalah metode yang efektif dalam pengumpulan data digital yang memungkinkan auditor untuk memantau aktivitas sistem TI secara langsung dan kontinu. Dengan pemantauan *real-time*, auditor dapat mengidentifikasi setiap anomali atau masalah yang muncul selama operasi normal sistem. Teknik ini sangat berguna untuk mendeteksi potensi masalah atau ancaman yang dapat mengganggu integritas data atau operasi sistem. Misalnya, pemantauan dapat membantu dalam mendeteksi aktivitas yang mencurigakan, seperti percobaan akses tidak sah atau perubahan data yang tidak terotorisasi.

Salah satu keuntungan utama dari pemantauan *real-time* adalah kemampuannya untuk memberikan wawasan yang

lebih mendalam dan akurat tentang aktivitas yang sedang berlangsung dalam organisasi. Data yang dikumpulkan selama pemantauan ini memungkinkan auditor untuk segera menilai apakah sistem berjalan sesuai dengan kebijakan dan prosedur yang telah ditetapkan. Ini juga memberi auditor kesempatan untuk melakukan intervensi lebih awal, sebelum masalah tersebut berkembang menjadi risiko yang lebih besar. Selain itu, pemantauan *real-time* memungkinkan auditor untuk memverifikasi keandalan dan efektivitas kontrol yang diterapkan pada sistem TI organisasi.

4) Analisis Laporan Sistem

Analisis laporan sistem merupakan metode penting dalam pengumpulan data digital, khususnya dalam audit TI yang berkaitan dengan aplikasi keuangan. Sistem TI modern, terutama yang digunakan untuk pengelolaan keuangan, sering kali menghasilkan laporan otomatis yang mencatat berbagai transaksi dan status keuangan secara terperinci. Laporan ini mencakup ringkasan data transaksi, posisi akun, dan rekonsiliasi data yang digunakan oleh auditor untuk menilai akurasi dan kepatuhan proses bisnis. Sebagai contoh, laporan otomatis dapat mencakup informasi tentang pembayaran yang belum diproses, status piutang, dan transaksi yang mungkin memerlukan klarifikasi lebih lanjut.

Dengan menggunakan laporan sistem, auditor dapat melakukan analisis mendalam terhadap data transaksi yang tercatat dalam aplikasi TI. Laporan ini memberikan gambaran yang lebih jelas tentang aliran data dan proses pemrosesan informasi dalam organisasi. Auditor dapat menilai apakah sistem tersebut dapat dipercaya dalam menghasilkan data yang akurat dan relevan untuk tujuan laporan keuangan. Misalnya, laporan otomatis dapat mencakup peringatan tentang transaksi yang tidak sesuai dengan kebijakan perusahaan, atau kesalahan dalam pengelolaan data, yang memudahkan auditor untuk segera mengidentifikasi potensi masalah sebelum menjadi risiko material bagi organisasi.

2. Analisis Data Digital dalam Audit TI

Setelah data digital dikumpulkan, langkah berikutnya adalah melakukan analisis untuk menilai integritas dan keamanan data tersebut. Analisis ini bertujuan untuk memverifikasi kebenaran data yang diproses oleh sistem TI dan untuk mengidentifikasi potensi ketidaksesuaian, kerentanannya, atau pelanggaran kebijakan internal.

a. Teknik Analisis yang Digunakan dalam Audit TI

1) Analisis Data Historis

Analisis data historis merupakan salah satu teknik utama dalam audit TI untuk mendeteksi anomali atau pola transaksi yang tidak biasa. Dengan memeriksa data yang sudah ada, auditor dapat mengidentifikasi perilaku yang tidak sesuai atau transaksi yang tidak wajar yang mungkin menunjukkan adanya masalah, seperti kesalahan dalam pengolahan data atau tindakan kecurangan. Misalnya, jika terdapat transaksi yang tidak konsisten dengan pola bisnis sebelumnya, auditor dapat menyelidiki lebih lanjut untuk mengetahui apakah transaksi tersebut sah atau melibatkan aktivitas yang tidak sah.

Pentingnya analisis data historis terletak pada kemampuannya untuk memberikan gambaran yang jelas tentang kinerja sistem TI dalam periode tertentu. Auditor akan mencari pola yang berulang dalam transaksi atau log aktivitas yang mungkin menunjukkan risiko atau masalah yang belum terdeteksi. Dengan membandingkan data historis dengan standar atau tren yang diharapkan, auditor dapat mendeteksi penyimpangan yang mungkin menjadi indikasi adanya ketidaksesuaian atau manipulasi data yang dilakukan oleh pihak internal atau eksternal. Ini membantu auditor untuk lebih cepat merespons potensi masalah dalam sistem.

2) Pengujian Substantif

Pengujian substantif adalah teknik audit yang digunakan untuk menguji kebenaran dan kelengkapan data yang dikumpulkan selama audit TI. Teknik ini biasanya melibatkan verifikasi transaksi atau data dengan membandingkannya dengan sumber lain yang terpercaya. Tujuan dari pengujian substantif adalah untuk memastikan

bahwa data yang tercatat dalam sistem TI organisasi sesuai dengan bukti atau dokumentasi yang mendukungnya. Misalnya, auditor dapat membandingkan data transaksi yang tercatat dalam sistem dengan faktur atau dokumen pembayaran yang terkait untuk memastikan kebenarannya.

Proses pengujian substantif juga dapat melibatkan verifikasi langsung terhadap transaksi yang terjadi, misalnya dengan melakukan konfirmasi kepada pihak ketiga. Sebagai contoh, auditor dapat menghubungi pelanggan atau pemasok untuk memverifikasi transaksi atau saldo yang tercatat dalam sistem TI perusahaan. Ini berguna untuk memastikan bahwa data yang ada dalam sistem tidak hanya lengkap, tetapi juga valid dan akurat. Teknik ini sering digunakan untuk mendeteksi kecurangan atau kesalahan yang mungkin tersembunyi dalam laporan keuangan atau transaksi yang diproses oleh sistem TI.

3) Analisis Forensik

Analisis forensik dalam audit TI berfokus pada pencarian bukti digital yang dapat mengidentifikasi insiden yang mencurigakan, seperti perubahan data yang tidak sah atau manipulasi transaksi yang dapat merugikan organisasi. Proses ini melibatkan penggunaan perangkat dan teknik analitik forensik untuk mengidentifikasi dan memulihkan bukti yang tersembunyi dalam sistem TI. Auditor forensik akan menyelidiki jejak digital, termasuk log sistem, jejak akses pengguna, dan metadata file, untuk menemukan petunjuk yang dapat mengungkapkan siapa yang terlibat dan bagaimana perubahan atau penghilangan data terjadi.

Selama proses analisis forensik, auditor juga memeriksa data yang tampaknya telah dihapus atau diubah untuk mencari jejak digital yang tersisa. Dengan bantuan perangkat forensik, seperti software pemulihan data, auditor dapat memperoleh bukti yang sebelumnya tidak dapat diakses, memungkinkan untuk menyusun gambaran yang lebih lengkap tentang kejadian tersebut. Sebagai contoh, dalam kasus kecurangan internal, auditor dapat melacak transaksi yang telah dimanipulasi, serta mengidentifikasi apakah ada upaya untuk menyembunyikan jejak tersebut.

4) Audit Kontrol dan Pengendalian TI

Audit kontrol dan pengendalian TI adalah salah satu teknik yang penting dalam audit TI, yang berfokus pada penilaian efektivitas pengendalian internal yang diterapkan dalam sistem informasi organisasi. Auditor TI akan memeriksa prosedur dan kebijakan pengamanan yang ada, seperti kontrol akses pengguna, prosedur otorisasi transaksi, dan pengelolaan data sensitif. Tujuan dari audit ini adalah untuk memastikan bahwa kontrol yang ada cukup kuat untuk mencegah akses tidak sah, kebocoran data, atau manipulasi sistem yang dapat merugikan organisasi (ISACA, 2012).

Selama audit kontrol dan pengendalian TI, auditor juga mengevaluasi sejauh mana prosedur yang diterapkan sesuai dengan standar yang ditetapkan oleh organisasi maupun regulasi yang berlaku. Sebagai contoh, auditor akan memeriksa apakah kontrol akses sudah mengikuti prinsip-prinsip minimisasi hak akses dan pembatasan akses berdasarkan kebutuhan pekerjaan (*least privilege*), juga akan memastikan bahwa kebijakan keamanan yang ada sudah mencakup prosedur untuk mendeteksi dan menangani insiden keamanan dengan cepat dan efektif.

5) Analisis Performa Sistem

Analisis performa sistem dalam audit TI bertujuan untuk mengevaluasi sejauh mana sistem informasi berfungsi dengan efisien dan efektif dalam mendukung operasi organisasi. Auditor TI melakukan pengujian terhadap berbagai aspek kinerja, seperti waktu respons sistem, ketahanan terhadap beban tinggi, dan kapasitas sistem untuk menangani volume transaksi yang besar. Evaluasi ini penting untuk memastikan bahwa sistem tidak hanya memenuhi kebutuhan saat ini tetapi juga dapat bertahan dalam menghadapi peningkatan beban di masa depan.

Pada analisis performa sistem, auditor akan menggunakan berbagai alat dan teknik untuk mengukur kecepatan pemrosesan data dan waktu tanggap sistem. Misalnya, dapat melakukan uji beban (*load testing*) untuk mengetahui bagaimana sistem bereaksi saat dipaksa untuk memproses sejumlah besar data atau transaksi dalam waktu

yang singkat. Jika sistem menunjukkan penurunan kinerja yang signifikan atau gagal menangani beban tersebut, auditor akan memberikan rekomendasi untuk perbaikan, seperti peningkatan kapasitas server atau optimisasi aplikasi.

b. Alat dan Teknologi untuk Analisis Data Digital

Penggunaan alat dan teknologi yang canggih dalam analisis data digital sangat penting untuk meningkatkan efisiensi dan akurasi audit TI. Beberapa alat yang umum digunakan dalam analisis data digital dalam audit TI meliputi:

1) Alat Forensik Digital

Alat forensik digital seperti EnCase dan FTK (*Forensic Tool Kit*) berperan penting dalam audit TI, terutama ketika auditor perlu memulihkan data yang hilang atau terhapus dari perangkat keras atau perangkat lunak. EnCase, misalnya, adalah salah satu alat yang sangat populer yang digunakan untuk forensik digital, karena kemampuannya dalam mengidentifikasi dan mengembalikan data yang hilang, serta menganalisis bukti digital yang mungkin tersembunyi atau rusak. Alat ini memungkinkan auditor untuk melakukan analisis mendalam terhadap perangkat penyimpanan seperti hard disk atau flash drive untuk menemukan informasi yang dapat menjadi kunci dalam investigasi insiden keamanan siber atau kegagalan sistem.

FTK adalah alat forensik digital lain yang sering digunakan dalam audit TI untuk mengidentifikasi jejak digital, memulihkan data yang terhapus, dan menganalisis bukti yang ada di dalam sistem. Salah satu fitur utama FTK adalah kemampuannya untuk memproses data dalam jumlah besar dengan cepat, memungkinkan auditor untuk menganalisis banyak file dan metadata dengan efisiensi tinggi. FTK juga mendukung pencarian yang lebih mendalam terhadap data yang terfragmentasi dan memberi auditor kemampuan untuk menilai dan mengkonfirmasi bukti secara lebih menyeluruh, yang sangat berguna dalam investigasi untuk menemukan kejahatan siber atau kecurangan.

2) Software Audit TI

Software audit TI seperti ACL Analytics dan IDEA menawarkan kemampuan untuk memproses dan

menganalisis data transaksi dalam jumlah besar secara efisien. ACL Analytics memungkinkan auditor untuk melakukan analisis data secara cepat dengan menggunakan teknik statistik dan algoritma yang dirancang khusus untuk mendeteksi pola yang mencurigakan atau tidak sesuai. Misalnya, perangkat lunak ini dapat mengidentifikasi transaksi yang tidak biasa atau perbedaan antara data yang tercatat dengan transaksi yang sebenarnya, sehingga memberikan wawasan yang lebih dalam tentang ketidaksesuaian atau potensi risiko dalam sistem TI (Cascarino, 2017).

IDEA, di sisi lain, juga merupakan alat yang sangat berguna untuk audit TI, terutama dalam memeriksa data dalam jumlah besar dan mengidentifikasi risiko atau penyimpangan. Dengan menggunakan teknik analitik yang canggih, IDEA memungkinkan auditor untuk mengidentifikasi ketidaksesuaian dalam transaksi, menganalisis tren, dan membuat laporan berbasis data yang lebih akurat. Fitur-fitur seperti pencarian pola, analisis waktu, dan pemeriksaan data duplikat memungkinkan auditor untuk menggali lebih dalam dan memberikan laporan yang lebih tepat dalam mendukung keputusan manajerial atau penyelidikan lebih lanjut.

3) Sistem Pemantauan dan Deteksi Intrusi (IDS)

Sistem Pemantauan dan Deteksi Intrusi (IDS) seperti Splunk dan Wireshark sangat penting dalam audit TI karena memungkinkan pemantauan aktif terhadap lalu lintas jaringan dan deteksi potensi ancaman keamanan. Splunk, misalnya, adalah alat yang dapat mengumpulkan dan menganalisis data log dari berbagai perangkat di jaringan. Dengan kemampuan untuk memvisualisasikan data dalam bentuk grafik dan laporan yang mudah dipahami, Splunk membantu auditor untuk mendeteksi anomali atau aktivitas yang mencurigakan yang bisa menandakan adanya potensi pelanggaran keamanan atau serangan siber.

Wireshark, di sisi lain, adalah alat pemantauan jaringan yang sangat kuat yang digunakan untuk menangkap dan menganalisis paket data yang dikirimkan melalui jaringan.

Wireshark memberikan wawasan mendalam tentang bagaimana data dipindahkan dalam jaringan dan memungkinkan auditor untuk mengidentifikasi lalu lintas yang tidak sah atau mencurigakan. Misalnya, auditor dapat mendeteksi serangan man-in-the-middle, di mana penyerang mencoba mengakses atau mengubah data yang dikirimkan antara dua pihak tanpa izin. Dengan kemampuannya untuk menampilkan data mentah dalam format yang mudah dianalisis, Wireshark menjadi alat yang efektif dalam proses deteksi intrusi dan pemantauan jaringan.

D. Teknik Pengujian Kontrol IT (*Penetration Testing, Vulnerability Assessment*)

Pada konteks audit IT keuangan, pengujian kontrol TI sangat penting untuk memastikan bahwa sistem dan infrastruktur IT yang mendukung transaksi dan data keuangan terlindungi dengan baik dari potensi ancaman yang bisa membahayakan keamanan dan integritas informasi. Salah satu cara yang digunakan untuk mengevaluasi kekuatan pengendalian TI adalah melalui *penetration testing* (pengujian penetrasi) dan *vulnerability assessment* (penilaian kerentanannya). Keduanya adalah teknik yang digunakan untuk mengidentifikasi dan mengatasi potensi kerentanannya dalam sistem, aplikasi, dan infrastruktur IT, yang dapat menyebabkan kegagalan sistem atau pelanggaran data yang dapat merugikan organisasi.

1. *Penetration Testing* dalam Audit TI Keuangan

Penetration testing, atau sering disebut sebagai "*pentesting*", adalah teknik yang digunakan untuk menguji kerentanannya dalam sistem TI dengan cara mensimulasikan serangan dunia maya yang mungkin terjadi. Tujuan dari pengujian ini adalah untuk menilai seberapa kuat sistem pertahanan TI organisasi terhadap potensi serangan eksternal atau internal, serta untuk mengidentifikasi celah keamanan yang perlu diperbaiki. Penetration testing dapat dibagi menjadi beberapa jenis berdasarkan tujuan dan lingkup pengujian:

a. *Black Box Testing*: Pada jenis pengujian ini, auditor tidak memiliki informasi sebelumnya tentang sistem atau aplikasi yang

diuji. Bertindak seperti penyerang eksternal yang tidak memiliki akses ke dalam sistem.

b. *White Box Testing*: Dalam pengujian ini, auditor diberikan informasi yang lengkap tentang sistem yang diuji, termasuk kode sumber dan konfigurasi jaringan. Ini memungkinkan pengujian yang lebih mendalam terhadap sistem.

c. *Gray Box Testing*: Pengujian ini menggabungkan elemen dari kedua pendekatan sebelumnya. Auditor diberikan sebagian informasi tentang sistem, tetapi tidak sepenuhnya mengetahui tentang kerentanannya.

Penetration testing melibatkan beberapa langkah kunci yang harus dilakukan secara sistematis untuk memastikan hasil yang akurat dan dapat diandalkan:

a. Perencanaan dan Persiapan

Pada tahap perencanaan dan persiapan dalam penetration testing untuk audit TI keuangan, auditor bekerja sama dengan klien untuk menentukan ruang lingkup dan tujuan pengujian. Ini mencakup diskusi mendalam tentang sistem atau aplikasi yang akan diuji serta potensi risiko yang terkait dengan pengujian tersebut. Auditor perlu memastikan bahwa memahami infrastruktur TI yang ada, termasuk aplikasi keuangan, basis data, dan sistem transaksi yang terhubung, untuk memastikan pengujian dilakukan secara menyeluruh dan efektif. Menetapkan ruang lingkup yang jelas adalah langkah krusial untuk memastikan bahwa pengujian dilakukan sesuai dengan kebijakan dan batasan yang disepakati antara auditor dan klien.

Pada perencanaan ini, auditor juga perlu menentukan jenis pengujian yang akan dilakukan, seperti pengujian sistem internal, eksternal, atau pengujian jaringan tanpa izin (*black-box testing*). Pengujian black-box menguji sistem tanpa pengetahuan sebelumnya, memungkinkan auditor untuk melihat sistem dari perspektif seorang penyerang yang tidak memiliki akses ke informasi internal. Ini memberikan gambaran yang lebih realistis tentang potensi kerentanannya dalam kondisi dunia nyata. Langkah ini juga mencakup diskusi tentang kerangka waktu yang diperlukan untuk menyelesaikan pengujian dan jenis laporan yang diinginkan oleh klien, baik itu laporan rinci atau laporan eksekutif yang lebih singkat.

b. Pengumpulan Informasi (*Reconnaissance*)

Pengumpulan informasi (*reconnaissance*) dalam penetration testing adalah tahap awal yang sangat penting untuk mengidentifikasi potensi titik lemah dalam sistem yang akan diuji. Pada tahap ini, auditor mengumpulkan sebanyak mungkin informasi tentang target, baik yang bersifat publik maupun yang dapat diakses melalui eksploitasi kelemahan sistem. Salah satu metode yang umum digunakan adalah pemetaan jaringan (*network mapping*), yang mencakup identifikasi alamat IP, subnet, dan sistem yang terhubung ke jaringan. Hal ini memungkinkan auditor untuk memahami struktur dan topologi jaringan yang ada, yang kemudian dapat digunakan untuk merencanakan pengujian lebih lanjut.

Auditor juga memeriksa port terbuka pada sistem yang diuji. Port yang terbuka dapat menunjukkan layanan atau aplikasi yang berjalan di sistem tersebut, yang berpotensi menjadi titik masuk bagi penyerang. Dengan menggunakan alat pemindai port seperti Nmap, auditor dapat mendeteksi layanan yang berjalan pada port tertentu dan menganalisis kerentanannya. Auditor juga perlu mengidentifikasi sistem operasi yang digunakan pada perangkat target. Mengetahui sistem operasi sangat penting, karena setiap sistem memiliki kerentanannya sendiri, dan mengetahui versi perangkat lunak serta patch yang diterapkan memungkinkan auditor untuk menemukan celah keamanan yang spesifik.

c. Identifikasi Kerentanannya (*Vulnerability Scanning*)

Identifikasi kerentanannya (*vulnerability scanning*) adalah salah satu langkah kunci dalam penetration testing, di mana auditor menggunakan berbagai alat untuk mendeteksi potensi celah keamanan dalam sistem yang dapat dimanfaatkan oleh pihak yang tidak berwenang. Pada tahap ini, auditor melakukan pemindaian untuk menemukan perangkat lunak yang belum terpatch, misconfigurations, atau celah lainnya dalam infrastruktur TI yang berpotensi mengekspos organisasi terhadap risiko. Alat pemindai kerentanannya seperti Nessus, OpenVAS, dan Qualys sering digunakan untuk mengidentifikasi kelemahan yang mungkin tidak terlihat dalam pemeriksaan manual. Pemindaian ini mencakup berbagai area, seperti sistem operasi, aplikasi, dan perangkat keras yang terhubung ke jaringan.

Pada pemeriksaan kerentanannya, auditor juga menilai konfigurasi sistem untuk memastikan bahwa tidak ada pengaturan yang tidak aman yang dapat membuka akses bagi penyerang. Misalnya, layanan yang tidak perlu bisa jadi tetap aktif pada sistem, atau port yang tidak terlindungi bisa memungkinkan akses yang tidak sah. Selain itu, auditor akan memverifikasi apakah ada perangkat lunak yang sudah tidak terupdate dan rentan terhadap eksploitasi, seperti versi lama dari aplikasi atau sistem operasi yang tidak mendapat patch keamanan terbaru. Hal ini sangat penting dalam audit TI keuangan, di mana setiap celah keamanan dapat berpotensi memengaruhi integritas data dan transaksi.

d. Eksploitasi

Eksploitasi dalam penetration testing merupakan tahap di mana auditor mencoba untuk memanfaatkan celah atau kerentanannya yang telah ditemukan selama proses identifikasi. Pada tahap ini, auditor akan berusaha untuk memperoleh akses lebih dalam ke sistem yang diuji, dengan tujuan untuk mengevaluasi sejauh mana kerentanannya dapat dimanfaatkan oleh penyerang untuk mendapatkan kontrol atau mengakses data yang sensitif. Proses eksploitasi ini bisa dilakukan dengan memanfaatkan alat dan teknik yang sama dengan yang digunakan oleh penyerang, seperti SQL injection, buffer overflow, atau serangan berbasis web lainnya. Hal ini memberikan gambaran nyata mengenai potensi dampak yang dapat terjadi apabila kerentanannya tidak ditangani dengan baik.

Eksploitasi juga membantu auditor untuk menguji apakah kontrol keamanan yang ada, seperti firewall, sistem deteksi intrusi, dan mekanisme autentikasi, mampu mengatasi ancaman tersebut. Jika auditor berhasil mendapatkan akses lebih dalam ke dalam sistem, akan menilai sejauh mana penyerang dapat bergerak bebas dalam lingkungan tersebut, mengakses data sensitif, atau bahkan merusak integritas sistem. Ini sangat penting dalam konteks audit TI keuangan, di mana informasi transaksi dan data pelanggan sangat rentan terhadap eksploitasi. Melalui eksploitasi, auditor bisa menilai sejauh mana kebijakan pengamanan yang diterapkan oleh organisasi dapat menahan serangan yang mungkin terjadi.

2. *Vulnerability Assessment* dalam Audit TI Keuangan

Vulnerability assessment adalah proses yang lebih luas dalam menilai kerentanannya dalam sistem TI. Berbeda dengan penetration testing yang berfokus pada simulasi serangan nyata, vulnerability assessment bertujuan untuk mengidentifikasi dan mengklasifikasikan potensi kerentanannya yang ada dalam sistem dan infrastruktur TI. Penilaian ini lebih kepada menemukan celah-celah yang bisa dieksploitasi dan memberikan gambaran mengenai keamanan sistem secara umum. *Vulnerability assessment* juga melibatkan beberapa tahapan yang perlu dilalui auditor untuk menghasilkan hasil yang berguna:

a. Pemetaan Sistem dan Infrastruktur

Pada tahap pertama dalam *vulnerability assessment*, auditor memetakan seluruh sistem dan infrastruktur yang digunakan oleh organisasi. Ini mencakup pemetaan aplikasi, jaringan, perangkat keras, serta perangkat lunak yang digunakan dalam operasional TI. Dengan pemetaan yang lengkap, auditor dapat memperoleh pemahaman menyeluruh tentang bagaimana sistem terhubung dan berinteraksi satu sama lain. Hal ini penting untuk memastikan bahwa setiap elemen yang terlibat dalam pengolahan data atau transaksi keuangan dapat diperiksa secara komprehensif. Pemetaan ini memungkinkan auditor untuk mengidentifikasi titik-titik yang rentan terhadap potensi ancaman dan kegagalan sistem.

Auditor akan mengevaluasi konfigurasi perangkat keras dan perangkat lunak yang digunakan. Ini mencakup pemeriksaan terhadap sistem operasi, aplikasi pihak ketiga, serta pengaturan firewall dan kontrol akses. Misalnya, perangkat lunak yang tidak terpatch atau pengaturan sistem yang tidak aman dapat menjadi pintu masuk bagi ancaman eksternal. Dalam konteks ini, pemetaan sistem membantu auditor menentukan apakah kontrol pengamanan yang diterapkan pada titik-titik tertentu sudah cukup untuk melindungi data sensitif, terutama dalam lingkungan yang sangat terhubung seperti sistem TI keuangan.

b. Pemindaian Kerentanannya (*Vulnerability Scanning*)

Pada tahap pemindaian kerentanannya, auditor menggunakan alat pemindai untuk menganalisis sistem dan aplikasi yang ada dalam organisasi guna menemukan potensi celah keamanan yang

diketahui. Alat ini bekerja dengan cara memindai seluruh infrastruktur TI, termasuk perangkat lunak, perangkat keras, dan jaringan, untuk mendeteksi kerentanannya seperti perangkat lunak yang tidak terupdate atau patch yang belum diterapkan. Misalnya, perangkat lunak yang tidak terupdate sering kali menjadi target utama serangan siber karena memiliki celah yang diketahui dan dapat dieksploitasi oleh pihak yang tidak bertanggung jawab. Dengan memindai dan mendeteksi kerentanannya, auditor dapat memberikan rekomendasi untuk memperbarui atau mengonfigurasi ulang sistem untuk memperkuat keamanannya.

Alat pemindaian kerentanannya juga mendeteksi port yang terbuka yang tidak aman, yang sering menjadi celah bagi ancaman eksternal. Port yang terbuka memungkinkan akses yang tidak sah jika tidak dikendalikan dengan baik, sehingga menjadi vektor bagi malware dan serangan peretasan. Alat seperti Nessus dan OpenVAS dapat digunakan untuk memindai port dan memberikan laporan terkait port terbuka yang rentan, yang harus segera ditutup atau diamankan dengan pengaturan yang lebih ketat. Pemeriksaan ini sangat penting dalam memastikan bahwa sistem jaringan aman dan hanya dapat diakses oleh pengguna yang berwenang.

c. Analisis dan Penilaian

Setelah pemindaian kerentanannya selesai, tahap selanjutnya dalam proses penilaian kerentanannya adalah analisis dan penilaian mendalam terhadap hasil yang telah dikumpulkan. Auditor akan memeriksa setiap temuan untuk menentukan apakah kerentanannya benar-benar berisiko tinggi bagi organisasi. Kerentanan yang ditemukan diklasifikasikan berdasarkan dua faktor utama: tingkat keparahannya dan kemungkinan dampaknya terhadap sistem dan operasi organisasi. Proses ini melibatkan evaluasi seberapa besar potensi eksploitasi yang dapat terjadi jika kerentanannya tidak segera ditangani. Sebagai contoh, jika sebuah kerentanannya melibatkan perangkat lunak yang tidak ter-update, namun perangkat lunak tersebut tidak digunakan dalam aplikasi kritis, maka dampaknya mungkin lebih rendah dibandingkan jika kerentanannya terjadi pada aplikasi yang sangat sensitif seperti sistem keuangan organisasi.

Setelah mengidentifikasi kerentanannya, auditor akan mengklasifikasikan temuan-temuan tersebut dalam beberapa kategori yang menggambarkan tingkat risiko. Misalnya, kerentanannya dapat dikategorikan sebagai rendah, menengah, atau tinggi, berdasarkan potensi kerusakan yang ditimbulkan jika eksploitasi terjadi. Kerentanan dengan tingkat keparahan tinggi, seperti kelemahan dalam enkripsi data atau kegagalan pengelolaan kredensial pengguna, akan diprioritaskan untuk diperbaiki segera, karena dapat menimbulkan dampak yang sangat besar pada kerahasiaan, integritas, dan ketersediaan data organisasi. Sebaliknya, kerentanan yang lebih rendah mungkin hanya memerlukan perhatian lebih lanjut di kemudian hari.

d. Laporan Temuan dan Rencana Perbaikan

Setelah tahap analisis dan penilaian kerentanannya, langkah selanjutnya dalam proses *vulnerability assessment* adalah menyusun laporan temuan dan rencana perbaikan. Laporan ini merupakan dokumentasi penting yang merangkum semua kerentanannya yang ditemukan selama pemindaian dan analisis. Dalam laporan ini, auditor akan memberikan rincian tentang jenis kerentanannya, potensi risikonya, dan dampaknya terhadap sistem atau data organisasi. Selain itu, laporan ini juga menyarankan langkah-langkah perbaikan yang perlu dilakukan untuk mengatasi kerentanannya yang ditemukan, baik itu memperbarui perangkat lunak, mengonfigurasi ulang sistem, atau memperkuat kebijakan keamanan yang ada.

Laporan temuan yang disusun oleh auditor harus jelas, terstruktur dengan baik, dan mudah dipahami oleh pihak yang akan menerima rekomendasi tersebut, seperti tim TI atau manajemen organisasi. Setiap kerentanannya akan dijelaskan dengan rinci, termasuk metode eksploitasi yang dapat digunakan oleh pihak yang tidak berwenang untuk mengeksploitasi celah tersebut. Rekomendasi yang diberikan dalam laporan ini bertujuan untuk mengurangi atau menghilangkan risiko yang ada, sehingga organisasi dapat menghindari potensi ancaman yang dapat merusak integritas data dan sistem. Laporan juga akan menyertakan penilaian tentang prioritas perbaikan, berdasarkan tingkat keparahan dan kemungkinan terjadinya serangan.

E. Pelaporan Hasil Audit IT

Pelaporan hasil audit IT adalah salah satu langkah krusial dalam proses audit teknologi informasi, terutama dalam sektor keuangan. Setelah auditor melakukan serangkaian evaluasi terhadap kontrol TI, pengujian sistem, dan identifikasi kerentanannya, hasil dari semua proses tersebut harus disajikan secara jelas dan terstruktur. Pelaporan yang baik akan memberikan wawasan yang mendalam mengenai temuan-temuan audit, memberikan rekomendasi perbaikan yang jelas, dan membantu manajemen serta stakeholder lainnya dalam mengambil tindakan yang tepat. Dalam sektor keuangan, di mana data sensitif dan keandalan sistem TI adalah hal yang sangat vital, pelaporan hasil audit IT menjadi elemen yang sangat menentukan dalam menjaga keamanan dan keberlanjutan operasional.

1. Tujuan Pelaporan Hasil Audit IT

Pelaporan hasil audit TI memiliki beberapa tujuan utama yang perlu diperhatikan oleh auditor, antara lain:

a. Menyampaikan Temuan Temuan yang Signifikan
   Pelaporan hasil audit harus mencakup temuan-temuan penting yang ditemukan selama audit. Temuan ini bisa berupa celah keamanan dalam sistem TI, ketidakpatuhan terhadap kebijakan dan prosedur internal, atau risiko yang dapat mempengaruhi kelangsungan operasional dan integritas data keuangan. Temuan ini harus disajikan dengan jelas dan dapat dipahami oleh audiens yang terdiri dari berbagai level manajerial dan profesional.

b. Memberikan Rekomendasi untuk Perbaikan
   Laporan audit TI juga harus mencakup rekomendasi yang jelas untuk perbaikan. Rekomendasi ini bersifat praktis dan ditujukan untuk mengatasi masalah yang ditemukan selama audit, misalnya dengan menyarankan penerapan kontrol yang lebih ketat, perbaikan sistem keamanan, atau perbaruan perangkat lunak yang lebih aman.

c. Membantu Manajemen dalam Pengambilan Keputusan
   Laporan audit TI memberikan dasar yang kuat bagi manajemen dalam mengambil keputusan mengenai langkah-langkah yang perlu diambil untuk memperbaiki infrastruktur TI, mengelola

risiko, dan memastikan bahwa sistem dan proses berjalan secara efisien dan aman.

d. Memenuhi Kewajiban Kepatuhan dan Regulasi
   Sektor keuangan sering kali diatur oleh berbagai regulasi dan standar yang mengharuskan pelaksanaan audit TI secara berkala. Laporan audit TI juga berfungsi untuk memenuhi kewajiban regulasi dan kepatuhan ini, serta untuk memberikan bukti yang diperlukan kepada otoritas pengawas atau regulator.

2. Struktur Laporan Audit IT

Laporan audit TI yang baik harus memiliki struktur yang jelas dan terorganisir, agar memudahkan pembaca dalam memahami temuan dan rekomendasi yang disajikan. Berikut adalah komponen utama yang harus ada dalam laporan audit TI:

a. Pendahuluan
   Pendahuluan harus memberikan gambaran umum mengenai ruang lingkup audit, tujuan audit, serta metodologi yang digunakan. Pada bagian ini, auditor harus menjelaskan latar belakang audit, termasuk alasan dilakukan audit TI (misalnya, audit tahunan, audit berdasarkan permintaan, atau audit berdasarkan risiko tertentu) dan area yang diuji (seperti keamanan jaringan, pengelolaan data keuangan, atau pengendalian akses).

b. Ringkasan Eksekutif
   Bagian ini memberikan gambaran umum mengenai temuan-temuan utama dari audit, serta dampaknya terhadap organisasi. Ringkasan eksekutif harus menyampaikan secara singkat isu-isu utama yang ditemukan, tingkat keparahannya, serta langkah-langkah yang direkomendasikan untuk perbaikan. Ini bertujuan agar manajemen dapat memahami secara cepat isu-isu yang ada, bahkan jika tidak membaca seluruh laporan secara rinci.

c. Temuan Audit
   Pada bagian ini, auditor harus merinci setiap temuan yang ditemukan selama proses audit. Setiap temuan harus disajikan dengan detail yang cukup, termasuk bukti pendukung (misalnya, log audit, hasil pengujian penetrasi, laporan pemindaian kerentanannya) dan dampaknya terhadap keamanan, integritas, atau kinerja sistem TI. Temuan ini harus diklasifikasikan

berdasarkan tingkat risiko yang ditimbulkan, dari yang paling tinggi hingga yang paling rendah.

d. Rekomendasi
   Setelah menyajikan temuan-temuan, auditor harus memberikan rekomendasi untuk mengatasi masalah yang teridentifikasi. Rekomendasi ini harus praktis, jelas, dan dapat dipahami oleh pihak yang berkepentingan. Setiap rekomendasi harus mencakup saran spesifik mengenai langkah-langkah yang harus diambil, seperti pembaruan perangkat lunak, implementasi kontrol yang lebih ketat, atau perbaikan dalam kebijakan dan prosedur pengelolaan data.
e. Penilaian Kepatuhan terhadap Kebijakan dan Regulasi
   Bagian ini menyajikan penilaian terhadap sejauh mana sistem TI yang diperiksa memenuhi standar kepatuhan yang berlaku, baik itu kebijakan internal perusahaan maupun regulasi eksternal yang relevan (misalnya, SOX, GDPR, PCI DSS). Jika terdapat ketidakpatuhan, auditor harus merinci area mana yang tidak sesuai dengan regulasi dan memberikan rekomendasi untuk memperbaikinya.
f. Evaluasi Risiko
   Setiap temuan dan rekomendasi dalam laporan audit harus disertai dengan penilaian risiko yang terkait. Ini berarti, auditor harus menjelaskan potensi dampak dari celah keamanan atau ketidakpatuhan yang ditemukan, serta kemungkinan skenario yang dapat terjadi jika masalah tersebut tidak segera diatasi. Evaluasi ini membantu manajemen untuk memprioritaskan langkah-langkah yang perlu diambil.
g. Tindak Lanjut
   Laporan audit TI harus mencakup bagian tindak lanjut, yang merinci rencana untuk mengawasi dan mengevaluasi implementasi rekomendasi yang telah diberikan. Auditor dapat memberikan saran untuk pemeriksaan lebih lanjut atau audit lanjutan untuk memastikan bahwa perbaikan telah dilaksanakan dengan tepat dan efektif.

3. Teknik Pelaporan yang Efektif dalam Audit IT

Pelaporan hasil audit TI bukan hanya tentang menyajikan informasi, tetapi juga tentang cara menyampaikan informasi tersebut

agar dapat dipahami dan diambil tindakan dengan tepat. Beberapa teknik pelaporan yang efektif dalam audit TI mencakup:

a. Penyajian Data yang Jelas dan Tersusun

Penyajian data yang jelas dan terstruktur adalah kunci dalam menyampaikan temuan audit TI dengan cara yang mudah dipahami oleh semua pihak terkait. Sebagai auditor, sangat penting untuk menyusun laporan dengan format yang terorganisir agar manajemen dan pihak lainnya dapat menilai hasil audit secara efektif. Penggunaan elemen visual seperti grafik, tabel, dan diagram membantu memperjelas informasi yang kompleks, memudahkan pembaca untuk menganalisis hasil temuan secara lebih cepat dan tepat. Sebagai contoh, grafik yang menunjukkan jumlah serangan atau insiden keamanan dalam periode waktu tertentu memberikan gambaran yang jelas tentang pola ancaman yang perlu diperhatikan oleh tim TI.

Grafik dan tabel juga dapat membantu dalam menunjukkan tren yang relevan dalam sistem TI, seperti peningkatan atau penurunan kerentanannya yang ditemukan. Sebuah tabel yang memuat temuan-temuan utama, bersama dengan tingkat keparahan masing-masing kerentanannya dan rekomendasi perbaikannya, akan memudahkan pembaca untuk memahami area mana yang membutuhkan perhatian lebih besar. Hal ini sangat penting bagi manajer yang harus membuat keputusan berbasis data untuk memperkuat kontrol TI dan mengalokasikan sumber daya dengan lebih tepat.

b. Penggunaan Bahasa yang Jelas dan Sederhana

Penggunaan bahasa yang jelas dan sederhana dalam laporan audit TI sangat penting untuk memastikan bahwa temuan-temuan audit dapat dipahami oleh semua pihak yang terlibat, baik yang memiliki latar belakang teknis maupun yang tidak. Banyak audiens laporan audit TI, seperti manajer keuangan atau eksekutif puncak, tidak memiliki pemahaman mendalam tentang istilah teknis atau prosedur audit TI. Oleh karena itu, auditor perlu menyusun laporan dengan bahasa yang mudah dimengerti dan menghindari penggunaan jargon teknis yang dapat membingungkan. Misalnya, alih-alih menggunakan istilah teknis yang rumit, auditor bisa memilih kata-kata yang lebih sederhana untuk menggambarkan masalah yang terjadi.

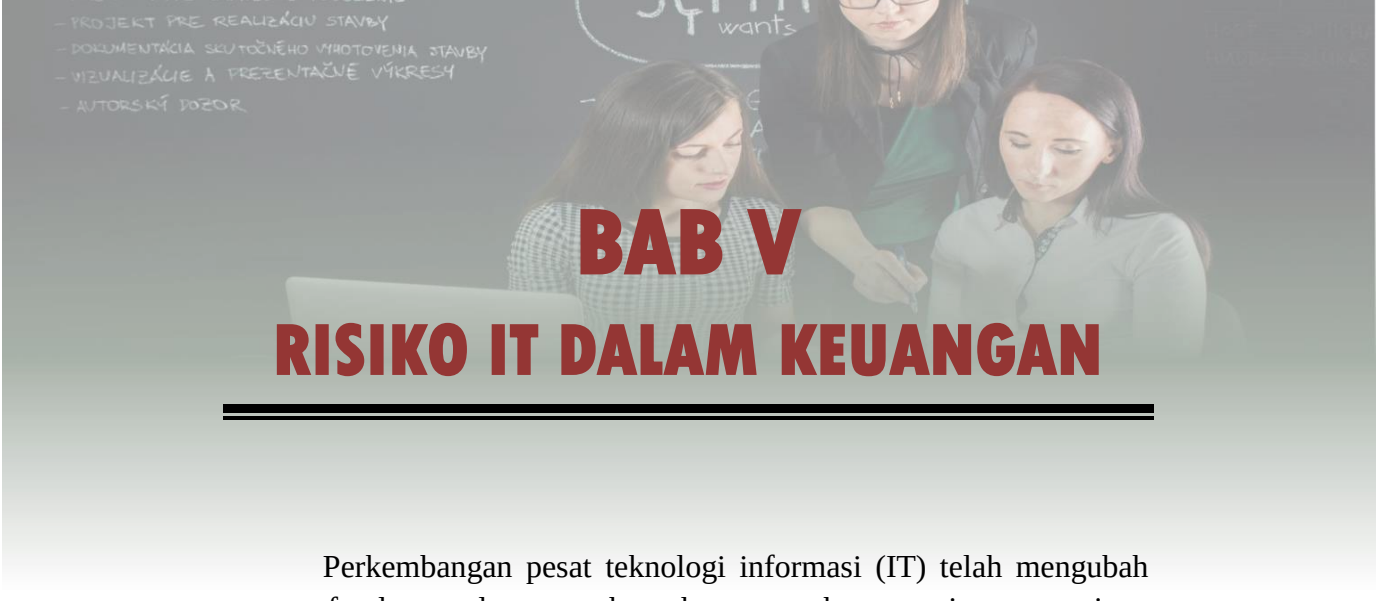
Penggunaan bahasa yang sederhana juga akan membantu mempercepat proses pengambilan keputusan. Ketika laporan dapat dipahami dengan mudah, manajemen lebih cepat dalam menilai situasi dan merespons temuan yang dilaporkan. Sebagai contoh, daripada menyampaikan temuan dalam kalimat yang penuh dengan terminologi teknis, auditor dapat menyampaikan hal tersebut dalam bentuk yang lebih naratif dan menjelaskan dampaknya dalam bahasa yang lebih familiar bagi pembaca non-teknis. Ini penting untuk menghindari kebingungannya pihak-pihak yang mungkin tidak terlibat langsung dalam kegiatan teknis, namun bertanggung jawab untuk membuat keputusan strategis.

c. Penyajian Rekomendasi dengan Prioritas

Pada laporan audit TI, penyajian rekomendasi yang terstruktur dengan baik dan diberi prioritas sangat penting untuk mendukung manajemen dalam mengambil keputusan yang tepat. Auditor harus mengklasifikasikan rekomendasi berdasarkan tingkat urgensi dan potensi dampaknya terhadap organisasi. Hal ini membantu manajemen untuk fokus pada masalah yang memiliki risiko terbesar dan memerlukan perhatian segera. Misalnya, masalah yang terkait dengan pengendalian akses yang lemah atau perlindungan data pribadi sering kali memiliki dampak yang signifikan, seperti pelanggaran data atau kebocoran informasi sensitif, sehingga harus ditangani segera. Sebaliknya, rekomendasi yang terkait dengan pembaruan perangkat lunak minor atau peningkatan kenyamanan pengguna dapat dianggap sebagai prioritas yang lebih rendah.

Proses klasifikasi ini melibatkan penilaian terhadap potensi kerugian finansial, reputasi, atau operasional yang dapat ditimbulkan jika masalah tersebut tidak segera ditangani. Auditor dapat menggunakan skala prioritas, seperti "tinggi", "sedang", atau "rendah", atau memberikan penilaian numerik untuk menilai tingkat urgensi dari masing-masing rekomendasi. Ini akan memberikan gambaran yang jelas kepada manajemen tentang langkah mana yang perlu diambil pertama kali untuk mengurangi risiko terbesar. Rekomendasi dengan prioritas tinggi biasanya mencakup langkah-langkah yang dapat mencegah pelanggaran

atau kehilangan data yang dapat merusak operasional dan reputasi organisasi secara signifikan.



BAB V
RISIKO IT DALAM KEUANGAN

Perkembangan pesat teknologi informasi (IT) telah mengubah secara fundamental cara sektor keuangan beroperasi, namun juga membawa berbagai risiko baru yang memerlukan perhatian khusus. Risiko IT dalam keuangan mencakup potensi ancaman terhadap integritas data, gangguan operasional, dan kerusakan reputasi yang bisa disebabkan oleh serangan siber, kegagalan sistem, atau penyalahgunaan akses. Peningkatan ketergantungan pada sistem berbasis digital untuk pengolahan transaksi keuangan, penyimpanan data, serta layanan pelanggan membuat industri keuangan lebih rentan terhadap risiko IT yang dapat mempengaruhi stabilitas ekonomi. Di antara jenis risiko IT yang paling signifikan dalam sektor keuangan adalah risiko keamanan siber, yang melibatkan ancaman terhadap data pribadi dan transaksi keuangan yang dapat diekspos oleh peretas atau penyalahgunaan oleh pihak internal. Selain itu, risiko teknologi yang berkaitan dengan kegagalan sistem atau aplikasi juga menjadi tantangan besar, karena kesalahan atau downtime dapat merugikan operasi dan menyebabkan kerugian finansial.

A. Jenis Risiko IT dalam Sistem Keuangan

Pada dunia keuangan, teknologi informasi (TI) berperan yang sangat penting dalam mendukung operasi dan layanan. Namun, semakin bergantung pada teknologi, semakin besar pula risiko yang terkait dengan penerapannya. Risiko IT dalam sistem keuangan dapat berupa ancaman terhadap data, integritas sistem, dan keberlanjutan operasional, yang semuanya dapat berdampak pada kelangsungan hidup perusahaan keuangan. Risiko ini dapat berupa gangguan sistem, pelanggaran keamanan data, dan ketidakpatuhan terhadap regulasi, serta dapat mengarah pada kerugian finansial yang signifikan. Risiko IT dalam

sistem keuangan dapat dikategorikan dalam beberapa jenis, masing-masing dengan karakteristik dan dampak yang berbeda. Kategori-kategori risiko tersebut meliputi:

1. Risiko Keamanan Cyber (*Cybersecurity Risk*)

Keamanan cyber adalah salah satu jenis risiko IT yang paling penting dalam sektor keuangan. Risiko ini terkait dengan potensi ancaman terhadap sistem TI yang dapat menyebabkan akses yang tidak sah, pencurian data, atau bahkan perusakan sistem. Di dunia keuangan, data pribadi dan transaksi keuangan sangat berharga, menjadikannya target utama bagi para peretas. Beberapa bentuk risiko keamanan cyber yang umum di sektor keuangan termasuk:

a. Serangan Malware dan Ransomware: Perangkat lunak berbahaya dapat merusak sistem TI atau mengenkripsi data, sehingga menghalangi akses ke informasi penting hingga tebusan dibayar.
b. Phishing: Teknik penipuan di mana penyerang mencoba untuk mendapatkan informasi pribadi dengan menyamar sebagai entitas yang sah, misalnya, melalui email atau situs web palsu.
c. Serangan DDoS (*Distributed Denial of Service*): Serangan ini dapat mengganggu akses layanan online dengan membanjiri server dengan lalu lintas yang berlebihan, mengakibatkan gangguan atau downtime.

2. Risiko Kepatuhan (*Compliance Risk*)

Di sektor keuangan, lembaga harus mematuhi berbagai peraturan dan standar yang terkait dengan pengelolaan data dan perlindungan konsumen, seperti *General Data Protection Regulation* (GDPR) di Uni Eropa dan *Sarbanes-Oxley Act* (SOX) di Amerika Serikat. Risiko kepatuhan berkaitan dengan potensi pelanggaran terhadap regulasi yang dapat mengakibatkan denda besar dan merusak reputasi lembaga keuangan. Beberapa contoh risiko kepatuhan meliputi:

a. Pelanggaran Terhadap Kebijakan Perlindungan Data: Tidak mematuhi standar perlindungan data yang diatur oleh undang-undang seperti GDPR dapat menyebabkan sanksi dan denda yang signifikan.
b. Kegagalan dalam Melaksanakan Audit atau Pelaporan Keuangan: Lembaga keuangan yang tidak dapat menyediakan

data yang akurat dan tepat waktu sesuai dengan peraturan yang berlaku dapat menghadapi risiko hukum.

3. Risiko Operasional (*Operational Risk*)

Risiko operasional dalam sistem TI keuangan berhubungan dengan kegagalan sistem yang dapat mempengaruhi kelancaran operasional sehari-hari. Ini termasuk gangguan yang disebabkan oleh kesalahan manusia, kegagalan perangkat keras atau perangkat lunak, serta masalah lainnya yang dapat menyebabkan gangguan layanan. Beberapa contoh risiko operasional meliputi:

a. Kegagalan Infrastruktur TI: Misalnya, server yang down atau aplikasi yang tidak dapat diakses dapat mengganggu transaksi keuangan dan mempengaruhi pengalaman pelanggan.
b. Kesalahan Pengguna: Proses manual yang melibatkan pengguna TI dapat menyebabkan kesalahan manusia yang dapat berakibat pada kesalahan transaksi atau kehilangan data.

- Kegagalan Sistem Cadangan: Sistem cadangan yang tidak berfungsi dengan baik dapat menyebabkan kehilangan data atau ketidakmampuan untuk memulihkan sistem dalam kasus kegagalan besar.

B. Risiko Keamanan Siber (Cybersecurity *Risks*)

Keamanan siber (*cybersecurity*) adalah salah satu risiko IT yang paling signifikan dalam sektor keuangan. Dalam beberapa tahun terakhir, lembaga keuangan telah menjadi target utama bagi para peretas dan pihak yang tidak bertanggung jawab, yang mencoba mengeksploitasi kerentanannya untuk mendapatkan akses yang tidak sah ke data sensitif atau merusak sistem operasional. Risiko keamanan siber tidak hanya berdampak pada keamanan data dan transaksi, tetapi juga pada reputasi lembaga keuangan, yang dapat mengakibatkan kerugian finansial yang besar dan penurunan kepercayaan dari nasabah. Sebagai respons terhadap ancaman ini, lembaga keuangan perlu mengembangkan kebijakan dan prosedur yang ketat untuk melindungi datanya dan sistem yang mendukung operasi keuangan.

Keamanan siber di sektor keuangan berkaitan dengan perlindungan terhadap informasi sensitif, integritas sistem IT, serta

kelangsungan operasional dari ancaman yang dapat merusak atau merusak aset digital. Dalam konteks lembaga keuangan, data sensitif seperti informasi akun nasabah, transaksi keuangan, dan catatan finansial harus dilindungi dari akses tidak sah, pencurian, dan penyalahgunaan. Ketidakamanan sistem dapat menyebabkan kerugian finansial, pelanggaran privasi, serta reputasi yang rusak.

1. Ancaman Keamanan Siber dalam Sektor Keuangan

Beberapa ancaman utama yang dihadapi sektor keuangan dalam hal keamanan siber meliputi:

a. Serangan Malware (*Malicious Software*)
   Serangan malware adalah salah satu bentuk ancaman yang paling umum dan berbahaya. Malware bisa datang dalam berbagai bentuk, termasuk virus, trojan, dan ransomware, yang dirancang untuk merusak atau mengakses sistem tanpa izin. Dalam sektor keuangan, malware dapat digunakan untuk mencuri informasi sensitif seperti nomor kartu kredit, kredensial akun bank, dan informasi pribadi lainnya. Salah satu contoh serangan malware yang terkenal adalah serangan ransomware, di mana data nasabah dienkripsi dan hanya dapat diakses kembali setelah korban membayar tebusan.
b. Phishing dan *Social Engineering*
   Phishing adalah bentuk serangan di mana pelaku mencoba untuk menipu korban agar memberikan informasi pribadi atau kredensial akses melalui email, pesan teks, atau situs web palsu. Dalam sektor keuangan, phishing sering digunakan untuk mendapatkan informasi login akun nasabah atau detail transaksi keuangan. Teknik *social engineering*, yang melibatkan manipulasi psikologis korban untuk mengeksploitasi kelemahan manusia, sering digunakan dalam serangan phishing. Pelaku seringkali menyamar sebagai pegawai bank atau lembaga keuangan untuk meyakinkan korban agar menyerahkan informasi penting.
c. Serangan *Denial of Service* (DDoS)
   Serangan *Denial of Service* (DDoS) bertujuan untuk mengganggu layanan daring lembaga keuangan dengan membanjiri server dengan trafik yang berlebihan, sehingga menyebabkan situs web atau aplikasi menjadi tidak dapat

diakses. Meskipun DDoS tidak selalu bertujuan untuk mencuri data atau merusak informasi, gangguan ini dapat mengakibatkan kerugian finansial dan kerusakan reputasi yang signifikan bagi lembaga yang diserang. Serangan DDoS pada lembaga keuangan sering kali terjadi selama periode sibuk seperti peluncuran produk baru atau perubahan kebijakan layanan.

d. Akses Tidak Sah dan Peretasan (*Hacking*)

Serangan peretasan adalah ancaman signifikan lainnya di sektor keuangan, di mana para peretas mencoba mendapatkan akses tidak sah ke sistem dengan tujuan untuk mencuri data, uang, atau merusak infrastruktur. Dalam kasus peretasan, para peretas dapat mengeksploitasi kelemahan dalam sistem atau aplikasi untuk mengakses data yang dilindungi atau untuk mengambil alih kontrol atas transaksi keuangan. Salah satu contoh paling terkenal adalah serangan terhadap Equifax pada 2017, di mana informasi pribadi lebih dari 140 juta orang dicuri, termasuk data keuangan yang sensitif.

2. Dampak Risiko Keamanan Siber terhadap Sektor Keuangan

Ancaman keamanan siber dapat mengakibatkan berbagai dampak negatif yang merugikan lembaga keuangan, baik dari segi finansial, reputasi, maupun hukum. Beberapa dampak utama termasuk:

a. Finansial

Serangan siber dapat memiliki dampak finansial yang sangat besar terhadap sektor keuangan. Salah satu dampaknya adalah pencurian dana nasabah, yang dapat terjadi melalui berbagai metode, seperti akses ilegal ke rekening atau data pribadi yang digunakan untuk transaksi tidak sah. Selain itu, lembaga keuangan yang menjadi korban serangan siber sering kali harus mengeluarkan biaya signifikan untuk memulihkan sistem dan memastikan bahwa data nasabah terlindungi setelah serangan. Misalnya, jika terjadi serangan ransomware, lembaga keuangan mungkin harus membayar tebusan yang besar untuk mendapatkan akses kembali ke data yang telah dienkripsi oleh penyerang. Biaya pemulihan ini, bersama dengan pengujian forensik dan pemulihan sistem, dapat menambah beban keuangan yang besar (Atkins & Lawson, 2021).

b. Kerusakan Reputasi

Kerusakan reputasi akibat serangan siber di sektor keuangan dapat memiliki dampak jangka panjang yang signifikan, karena kepercayaan nasabah adalah fondasi utama dalam industri ini. Ketika data sensitif, seperti informasi pribadi dan finansial nasabah, bocor atau terancam, hal ini mengurangi persepsi publik tentang kemampuan lembaga keuangan untuk melindungi aset. Serangan siber yang sukses, seperti pencurian data atau gangguan layanan, dapat memperburuk citra lembaga, mengurangi keyakinan nasabah terhadap keamanan layanan yang diberikan, dan berdampak pada loyalitas.

c. Sanksi Hukum dan Kepatuhan

Sanksi hukum dan kepatuhan menjadi dampak penting yang harus diperhatikan oleh lembaga keuangan dalam menghadapi ancaman serangan siber. Ketika lembaga keuangan gagal memenuhi standar perlindungan data yang ditetapkan oleh regulator, dapat menghadapi berbagai sanksi hukum yang serius, termasuk denda besar dan tindakan hukum. Regulator di banyak negara memiliki peraturan ketat terkait perlindungan data pribadi nasabah, dan pelanggaran terhadap peraturan ini tidak hanya merusak reputasi lembaga, tetapi juga mengakibatkan kerugian finansial yang signifikan. Misalnya, pelanggaran yang terkait dengan penyalahgunaan atau kebocoran data pribadi dapat mengarah pada denda yang menghancurkan.

C. Risiko Kepatuhan (*Compliance Risks*)

Risiko kepatuhan atau *compliance risks* adalah salah satu kategori risiko IT yang penting dalam sektor keuangan. Dalam konteks ini, risiko kepatuhan mengacu pada kemungkinan terjadinya kegagalan dalam mematuhi peraturan, undang-undang, dan standar yang relevan dengan operasi keuangan serta penggunaan teknologi informasi. Dalam dunia yang semakin digital, lembaga keuangan dihadapkan pada tantangan besar untuk memastikan bahwa sistem teknologi informasi sesuai dengan persyaratan kepatuhan yang terus berkembang, baik secara nasional maupun internasional. Dengan meningkatnya ketergantungan pada teknologi dalam transaksi dan pengelolaan data, risiko kepatuhan kini tidak hanya berkaitan dengan aspek hukum dan

regulasi, tetapi juga dengan perlindungan terhadap data pribadi dan transaksi elektronik. Kepatuhan terhadap regulasi tidak hanya mencakup hukum yang berlaku di negara tempat lembaga beroperasi, tetapi juga regulasi internasional yang dapat memengaruhi cara lembaga keuangan menjalankan bisnis, terutama yang berhubungan dengan data dan transaksi internasional. Kegagalan dalam memastikan kepatuhan dapat menyebabkan denda yang signifikan, kerugian finansial, dan kerusakan reputasi yang parah.

Sektor keuangan secara historis telah diatur oleh sejumlah peraturan yang bertujuan untuk melindungi kepentingan nasabah, menjamin stabilitas sistem keuangan, dan mencegah tindak pidana seperti pencucian uang, pendanaan terorisme, dan penipuan. Kepatuhan terhadap regulasi-regulasi ini tidak hanya melibatkan pengawasan langsung terhadap kegiatan bisnis tetapi juga penerapan teknologi yang digunakan untuk mengelola data dan transaksi. Teknologi yang digunakan oleh lembaga keuangan untuk menyimpan, mengelola, dan memproses data memerlukan pengawasan ketat untuk memastikan bahwa sistem tersebut mematuhi peraturan yang berlaku, terutama yang terkait dengan perlindungan data pribadi, transaksi keuangan, dan pelaporan keuangan.

1. Peraturan Penting dalam Kepatuhan Sektor Keuangan

Beberapa peraturan yang memengaruhi kepatuhan sektor keuangan terkait IT, antara lain:

a. *General Data Protection Regulation* (GDPR)
   GDPR adalah regulasi Uni Eropa yang menetapkan standar perlindungan data pribadi bagi individu di Eropa. Meskipun GDPR secara khusus mengatur data pribadi warga negara Uni Eropa, banyak lembaga keuangan global yang terlibat dalam transaksi internasional harus mematuhi regulasi ini. Kepatuhan terhadap GDPR melibatkan penerapan teknologi yang dapat mengamankan data pribadi nasabah dan memastikan bahwa data tersebut tidak digunakan atau dibagikan tanpa izin.

b. *Bank Secrecy Act* (BSA) dan *Anti-Money Laundering* (AML)
   BSA dan peraturan AML bertujuan untuk mencegah pencucian uang dan pendanaan terorisme. Lembaga keuangan wajib menggunakan sistem yang dapat mengidentifikasi dan melaporkan transaksi mencurigakan. Dalam hal ini, teknologi

informasi berperan penting dalam pemantauan transaksi keuangan secara *real-time* dan analisis data untuk mendeteksi pola yang mencurigakan. Sistem TI yang tidak memadai atau tidak sesuai dengan standar kepatuhan dapat membuka celah untuk pencucian uang dan pendanaan terorisme.

c. *Payment Card Industry Data Security Standard* (PCI DSS)
PCI DSS adalah standar keamanan yang ditetapkan oleh industri kartu pembayaran untuk melindungi data pemegang kartu kredit dan debit. Lembaga keuangan yang terlibat dalam pemrosesan pembayaran kartu harus memastikan bahwa sistem TI memenuhi persyaratan PCI DSS untuk melindungi data transaksi dari akses yang tidak sah.

d. *Sarbanes-Oxley Act* (SOX)
SOX adalah undang-undang yang mengatur laporan keuangan perusahaan publik di Amerika Serikat. Dalam konteks kepatuhan IT, SOX mengharuskan perusahaan untuk memiliki kontrol internal yang efektif untuk mengelola data dan transaksi keuangan. Penggunaan teknologi informasi yang tepat sangat penting dalam memastikan integritas data keuangan dan mencegah kecurangan atau manipulasi laporan keuangan.

2. Risiko Kepatuhan Terkait IT dalam Keuangan

Seiring dengan berkembangnya teknologi dan regulasi yang semakin kompleks, lembaga keuangan harus menghadapi sejumlah risiko kepatuhan yang berkaitan langsung dengan penggunaan IT. Risiko kepatuhan terkait IT dalam sektor keuangan meliputi:

a. Kegagalan dalam Perlindungan Data Pribadi

Kegagalan dalam perlindungan data pribadi nasabah merupakan risiko kepatuhan yang sangat signifikan dalam sektor keuangan, terutama dengan adanya regulasi seperti *General Data Protection Regulation* (GDPR) yang memberikan sanksi berat bagi pelanggaran. GDPR mewajibkan lembaga keuangan untuk melindungi data pribadi nasabah dengan standar keamanan yang ketat, dan kegagalan untuk memenuhi persyaratan ini dapat berakibat fatal. Peraturan ini tidak hanya menuntut perlindungan yang memadai terhadap data nasabah dari ancaman siber, tetapi juga transparansi dalam pengelolaan data, seperti bagaimana data dikumpulkan, digunakan, dan disimpan. Pelanggaran terhadap

perlindungan data dapat mengakibatkan denda yang sangat besar, yang dalam beberapa kasus mencapai hingga 4% dari total pendapatan tahunan lembaga keuangan.

b. Kegagalan dalam Pemantauan dan Pelaporan Transaksi Keuangan

Kegagalan dalam pemantauan dan pelaporan transaksi keuangan yang mencurigakan dapat menempatkan lembaga keuangan pada risiko hukum yang signifikan, terutama terkait dengan peraturan anti-pencucian uang (AML) dan pendanaan terorisme. Lembaga keuangan diwajibkan untuk memantau transaksi secara *real-time* untuk mendeteksi aktivitas yang mencurigakan, seperti transaksi besar yang tidak sesuai dengan profil nasabah atau pola transaksi yang tidak wajar. Sistem TI yang tidak memadai atau kurang efisien dalam memproses transaksi ini dapat menyebabkan kegagalan dalam mendeteksi dan melaporkan kegiatan ilegal yang seharusnya dilaporkan kepada pihak berwenang.

c. Kegagalan dalam Mematuhi Standar Keamanan Pembayaran

Kegagalan dalam mematuhi standar keamanan pembayaran seperti PCI DSS (*Payment Card Industry Data Security Standard*) dapat menyebabkan kerugian finansial yang signifikan bagi lembaga keuangan. PCI DSS adalah seperangkat aturan yang dirancang untuk melindungi data pembayaran nasabah, khususnya yang terkait dengan kartu kredit dan debit, serta mencegah akses tidak sah yang dapat menjerumuskan data sensitif ke tangan peretas. Lembaga keuangan yang tidak mematuhi standar ini berisiko menghadapi pencurian data kartu pembayaran, yang dapat merusak reputasi dan menambah beban keuangan akibat biaya pemulihan dan litigasi (Jartelius, 2020).

d. Kegagalan dalam Mengelola Pengawasan dan Audit Sistem TI

Kegagalan dalam mengelola pengawasan dan audit sistem TI di lembaga keuangan dapat menyebabkan dampak yang signifikan terhadap kepatuhan hukum dan integritas operasional perusahaan. Regulasi seperti *Sarbanes-Oxley Act* (SOX) di Amerika Serikat mewajibkan lembaga keuangan untuk memiliki pengawasan yang efektif terhadap sistem TI, terutama untuk memastikan bahwa laporan keuangan yang dihasilkan akurat dan tidak ada penyalahgunaan data. SOX bertujuan untuk mencegah

manipulasi atau penyalahgunaan laporan keuangan yang dapat merugikan investor dan stakeholder lainnya. Jika lembaga keuangan gagal dalam mengelola audit dan pengawasan terhadap sistem TI, berisiko menghadapi sanksi hukum yang berat, termasuk denda besar dan kerugian reputasi yang bisa mempengaruhi hubungan dengan klien dan mitra bisnis.

D. Risiko Operasional dan *Downtime* Sistem IT

Risiko operasional dan *downtime* sistem IT merupakan dua elemen kritis dalam manajemen risiko yang dihadapi oleh lembaga keuangan dalam era digital saat ini. Kegagalan sistem teknologi informasi yang digunakan oleh lembaga keuangan dapat berdampak signifikan pada operasional, layanan kepada pelanggan, dan stabilitas keuangan. Risiko operasional dalam konteks IT adalah potensi kerugian yang timbul akibat dari kegagalan sistem teknologi informasi yang digunakan oleh lembaga keuangan, kegagalan dalam proses-proses yang bergantung pada teknologi, atau kesalahan manusia dalam pengoperasian sistem tersebut. Dampak dari risiko operasional dan downtime sistem IT di sektor keuangan dapat sangat merugikan, baik dari segi finansial, operasional, maupun reputasi. Beberapa dampak utama yang dapat terjadi meliputi:

1. Kerugian Finansial

Kegagalan sistem IT dalam sektor keuangan dapat menyebabkan kerugian finansial yang signifikan, baik secara langsung maupun tidak langsung. Kerugian langsung sering kali berupa hilangnya transaksi atau pendapatan yang terlewatkan karena ketidaktersediaan sistem. Misalnya, jika sistem pembayaran atau platform transaksi online mengalami downtime, transaksi yang seharusnya dilakukan akan tertunda atau gagal, mengakibatkan kehilangan pendapatan bagi lembaga keuangan. Selain itu, pelanggan yang tidak dapat mengakses layanan keuangan juga dapat beralih ke kompetitor, yang berdampak pada pengurangan pangsa pasar. Kerugian tidak langsung muncul melalui biaya yang dikeluarkan untuk memulihkan sistem IT yang rusak. Biaya pemulihan ini meliputi perbaikan perangkat keras dan perangkat lunak, serta pekerjaan pemulihan data yang hilang atau rusak. Hal ini seringkali memerlukan waktu dan sumber daya yang cukup besar, yang tentunya meningkatkan

beban operasional lembaga keuangan. Selain itu, gangguan operasional juga dapat menghambat aktivitas bisnis sehari-hari, menyebabkan ketidakmampuan untuk menyediakan layanan penting bagi nasabah dan meningkatkan biaya operasional secara keseluruhan.

2. Gangguan Layanan Pelanggan

Gangguan layanan pelanggan dalam sektor keuangan dapat terjadi ketika sistem TI, seperti sistem pembayaran, aplikasi mobile banking, atau platform perbankan online, mengalami downtime. Ketika layanan ini tidak tersedia, nasabah yang bergantung pada teknologi untuk melakukan transaksi atau mengakses layanan keuangan akan merasa frustrasi. Hal ini dapat mengganggu aktivitas perbankan sehari-hari, seperti mentransfer dana, memeriksa saldo, atau membayar tagihan, yang pada gilirannya akan merusak pengalaman sebagai pelanggan. Ketika gangguan ini terjadi secara berulang, dampaknya terhadap kepuasan pelanggan dapat semakin besar. Gangguan layanan yang berkepanjangan dapat menimbulkan dampak yang lebih besar berupa kerusakan reputasi lembaga keuangan. Sebuah bank atau lembaga keuangan yang tidak dapat menjaga sistemnya tetap berfungsi dengan baik dapat dianggap tidak profesional atau tidak mampu melindungi aset nasabah. Reputasi ini sangat sulit untuk diperbaiki, dan sering kali mengarah pada penurunan jumlah pelanggan atau penurunan loyalitas pelanggan yang sudah ada.

3. Reputasi yang Rusak

Reputasi adalah salah satu aset paling berharga bagi lembaga keuangan, dan gangguan sistem atau risiko operasional yang terjadi berulang kali dapat merusak citra secara signifikan. *Downtime* yang berlangsung lama, terutama yang memengaruhi layanan inti seperti transaksi pembayaran atau akses akun nasabah, dapat menyebabkan hilangnya kepercayaan dari pelanggan. Nasabah yang terganggu oleh ketidaknyamanan ini mungkin merasa bahwa lembaga keuangan tidak dapat diandalkan, yang akhirnya merusak reputasi perusahaan di pasar (Aloqab *et al*., 2018). Di era digital yang sangat terkoneksi, dampak dari gangguan layanan dapat menyebar dengan cepat melalui media sosial dan platform online. Pelanggan yang merasa kecewa sering kali membagikan pengalaman buruk, memperburuk persepsi publik tentang lembaga keuangan tersebut. Komentar negatif yang menyebar luas dapat

merusak citra perusahaan dalam waktu singkat, lebih jauh lagi memperburuk kerugian finansial yang mungkin sudah ada akibat gangguan layanan.

4. Pelanggaran Kepatuhan dan Denda

Pelanggaran kepatuhan yang terjadi akibat downtime atau kegagalan sistem TI di lembaga keuangan dapat mengakibatkan denda yang signifikan dan tindakan hukum lainnya. Lembaga keuangan diharuskan untuk mematuhi berbagai regulasi yang mengatur perlindungan data pribadi nasabah, pelaporan transaksi keuangan, serta pencegahan pencucian uang. Ketika sistem TI gagal berfungsi dengan baik, misalnya dalam hal pemantauan transaksi mencurigakan atau pelaporan data yang akurat, hal ini dapat mengarah pada pelanggaran peraturan yang diberlakukan oleh otoritas pengawas.

Contoh nyata dari dampak ini adalah kasus di mana lembaga keuangan besar di AS dikenakan denda besar karena kegagalan dalam mematuhi peraturan yang mengatur perlindungan data pribadi atau pelaporan transaksi yang mencurigakan. Sebagai contoh, beberapa lembaga keuangan yang mengalami gangguan sistem yang serius tidak mampu melaporkan transaksi yang wajib dilaporkan menurut *Bank Secrecy Act* (BSA), yang mengatur kewajiban pemantauan transaksi mencurigakan, atau *General Data Protection Regulation* (GDPR), yang melindungi data pribadi pengguna. Kegagalan dalam memenuhi kewajiban ini dapat berujung pada sanksi finansial yang berat, yang semakin meningkatkan kerugian lembaga keuangan tersebut.

E. Mitigasi Risiko IT dalam Keuangan

Pada industri keuangan, teknologi informasi (IT) telah menjadi komponen yang sangat krusial dalam menjalankan operasi sehari-hari. Dengan ketergantungan yang tinggi pada sistem IT untuk proses transaksi, pengelolaan data nasabah, pelaporan keuangan, dan komunikasi antar pihak terkait, risiko yang terkait dengan teknologi informasi menjadi perhatian utama bagi lembaga keuangan. Risiko IT yang dihadapi oleh lembaga keuangan mencakup berbagai macam faktor seperti ancaman siber, pelanggaran privasi, kegagalan sistem, downtime, serta masalah kepatuhan dan operasional.

Mitigasi risiko IT adalah serangkaian tindakan yang dirancang untuk mengurangi atau menghilangkan potensi ancaman yang dapat merusak integritas, kerahasiaan, dan ketersediaan sistem informasi dalam lembaga keuangan. Mengingat pentingnya keberlanjutan operasional lembaga keuangan, mitigasi risiko IT harus dilakukan dengan hati-hati dan berdasarkan pendekatan yang komprehensif untuk meminimalisir dampak dari insiden yang tidak diinginkan. Mitigasi risiko IT di sektor keuangan melibatkan berbagai pendekatan dan strategi yang disesuaikan dengan kebutuhan spesifik lembaga keuangan serta ancaman yang dihadapi. Beberapa pendekatan utama dalam mitigasi risiko IT meliputi:

1. Penguatan Keamanan Siber

Keamanan siber adalah prioritas utama dalam mitigasi risiko IT dalam lembaga keuangan. Serangan siber yang berhasil dapat menyebabkan kerugian finansial yang besar, merusak reputasi perusahaan, dan melanggar peraturan perlindungan data. Oleh karena itu, lembaga keuangan perlu mengimplementasikan langkah-langkah pencegahan yang kuat untuk melindungi data dan sistem. Beberapa langkah yang dapat diambil dalam penguatan keamanan siber meliputi:

a. Firewall dan Antivirus: Menggunakan perangkat lunak keamanan seperti firewall dan antivirus untuk melindungi jaringan dari serangan luar.
b. Enkripsi Data: Data yang sensitif seperti informasi nasabah harus dienkripsi untuk mencegah kebocoran data jika terjadi peretasan atau serangan malware.
c. Autentikasi Multi-Faktor: Implementasi autentikasi multi-faktor (MFA) dapat meningkatkan tingkat keamanan akun, sehingga lebih sulit bagi pihak yang tidak sah untuk mengakses sistem keuangan.
d. Pemantauan Keamanan 24/7: Sistem pemantauan yang dapat mendeteksi aktivitas mencurigakan atau serangan yang sedang berlangsung perlu diterapkan secara kontinu.
e. Penetration Testing: Penetration testing atau uji penetrasi dilakukan untuk mengidentifikasi potensi kelemahan dalam sistem IT lembaga keuangan dan menilai seberapa kuat pertahanan terhadap serangan eksternal.

2. Kebijakan Pengelolaan Data yang Ketat

Kebijakan pengelolaan data yang ketat sangat penting dalam sektor keuangan untuk memastikan bahwa data nasabah dilindungi dengan baik dari ancaman siber dan pelanggaran privasi. Salah satu aspek yang krusial dalam kebijakan ini adalah pengelolaan akses. Lembaga keuangan harus mengontrol siapa saja yang memiliki akses ke data sensitif dan memastikan bahwa hanya individu yang berwenang, seperti petugas yang memiliki tanggung jawab khusus terhadap data tersebut, yang bisa mengaksesnya. Penggunaan sistem autentikasi multi-faktor dan pembatasan akses berdasarkan peran (*role-based access control*) menjadi langkah penting dalam mengurangi risiko kebocoran data akibat akses yang tidak sah.

Kebijakan penghapusan data juga harus dijalankan dengan sangat hati-hati. Lembaga keuangan harus memiliki prosedur yang jelas mengenai penghapusan data lama yang sudah tidak relevan lagi untuk memastikan bahwa data yang tidak diperlukan tidak akan jatuh ke tangan yang salah. Penghapusan data yang tidak tepat atau tidak terlaksana dengan baik dapat berisiko menyebabkan kebocoran data yang tidak disengaja, yang dapat berakibat pada kerugian finansial dan kerusakan reputasi. Oleh karena itu, lembaga harus memastikan bahwa kebijakan penghapusan data ini dilaksanakan secara konsisten dan sesuai dengan peraturan yang berlaku, seperti GDPR di Uni Eropa.

3. Pelatihan Karyawan dan Manajemen Risiko Internal

Pelatihan karyawan merupakan aspek yang sangat penting dalam mitigasi risiko IT di sektor keuangan. Karyawan yang tidak dilatih dengan baik mengenai kebijakan dan prosedur keamanan IT berisiko menjadi titik lemah dalam sistem pertahanan. Bisa saja secara tidak sengaja membuka pintu bagi ancaman siber seperti phishing atau malware. Oleh karena itu, lembaga keuangan harus mengadakan pelatihan keamanan secara berkala untuk semua karyawan, termasuk pelatihan tentang cara mengenali email phishing, protokol pengamanan kata sandi, dan penggunaan perangkat dengan aman. Pelatihan ini juga harus mencakup pemahaman mendalam tentang peraturan perlindungan data yang berlaku, seperti GDPR, untuk memastikan karyawan paham perannya dalam menjaga data nasabah tetap aman.

Keberhasilan mitigasi risiko IT juga bergantung pada adanya manajemen risiko internal yang proaktif. Tim ini bertanggung jawab

untuk mengidentifikasi dan mengelola potensi risiko IT yang bisa muncul dalam operasional sehari-hari, harus mampu menilai ancaman secara dini dan merancang langkah mitigasi yang tepat, yang melibatkan kolaborasi dengan departemen IT. Dalam hal ini, tim manajemen risiko harus memiliki pemahaman yang baik tentang lanskap ancaman siber dan perangkat teknologi terbaru yang digunakan lembaga keuangan, sehingga dapat mengantisipasi perubahan dan mengelola risiko dengan efektif.

4. Pemeliharaan dan Pemantauan Sistem yang Proaktif

Pemeliharaan dan pemantauan sistem TI secara proaktif merupakan komponen vital dalam menjaga kinerja dan keamanan sistem informasi lembaga keuangan. Pembaruan perangkat lunak secara berkala adalah langkah pertama untuk memastikan sistem tetap aman dari ancaman siber terbaru. Tanpa pembaruan rutin, perangkat lunak yang usang bisa menjadi celah bagi peretas untuk mengeksploitasi kerentanannya, yang dapat menyebabkan kerugian finansial dan kerusakan reputasi. Penggantian perangkat keras yang sudah usang juga penting karena perangkat keras yang lama dapat menyebabkan kegagalan sistem atau bahkan downtime yang merugikan, sehingga memengaruhi kelancaran operasional lembaga keuangan.

Pemantauan sistem yang kontinu sangat penting untuk mendeteksi potensi masalah sejak dini. Dengan pemantauan yang baik, lembaga keuangan dapat mengidentifikasi gangguan atau kerentanannya sebelum berkembang menjadi insiden besar. Teknologi pemantauan yang canggih memungkinkan untuk memeriksa status sistem dan mengidentifikasi masalah dalam waktu nyata. Hal ini sangat berguna dalam memastikan bahwa masalah dapat segera diatasi tanpa menunggu masalah menjadi lebih besar, yang berisiko merugikan nasabah atau bahkan melanggar regulasi yang ada.

5. Perencanaan Pemulihan Bencana dan Kelangsungan Bisnis

Perencanaan pemulihan bencana dan kelangsungan bisnis merupakan elemen krusial dalam memastikan bahwa lembaga keuangan dapat mengatasi gangguan yang disebabkan oleh insiden besar, seperti serangan siber, bencana alam, atau kegagalan teknologi. *Disaster Recovery Plan* (DRP) adalah salah satu komponen penting yang berfokus pada pemulihan infrastruktur TI yang rusak atau terganggu.

DRP mencakup langkah-langkah yang terperinci untuk mengembalikan sistem yang down, memulihkan data yang hilang, dan memastikan bahwa layanan TI dapat kembali beroperasi secepat mungkin. Tanpa DRP yang baik, lembaga keuangan berisiko kehilangan data vital dan menghadapi downtime yang lama, yang dapat berdampak besar pada operasional dan kepercayaan nasabah.

Business Continuity Plan (BCP) memiliki peran yang sangat penting dalam perencanaan kelangsungan bisnis. BCP berfokus pada keberlanjutan operasional secara keseluruhan, memastikan bahwa lembaga keuangan dapat terus menjalankan fungsinya meskipun terjadi gangguan besar. Ini mencakup rencana untuk menjaga keberlanjutan pelayanan kepada nasabah, pengelolaan keuangan, serta operasional internal. Sebagai contoh, dalam situasi darurat, BCP dapat mencakup pengalihan operasional ke lokasi alternatif atau pengaturan sistem cadangan untuk memastikan bahwa transaksi nasabah dapat terus diproses tanpa gangguan besar.

BAB VI
KEAMANAN DATA DAN PRIVASI DALAM AUDIT IT

Keamanan data dan privasi menjadi komponen krusial dalam audit IT, terutama dalam sektor keuangan, yang dihadapkan pada ancaman cyber yang terus berkembang. Data pelanggan, transaksi keuangan, dan informasi sensitif lainnya harus dilindungi dengan baik untuk memastikan integritas dan kerahasiaannya. Risiko kebocoran data atau akses yang tidak sah dapat merusak kepercayaan pelanggan, serta menyebabkan kerugian finansial dan hukum bagi lembaga keuangan. Pengelolaan privasi dalam audit IT juga melibatkan pemastian bahwa lembaga keuangan mengikuti standar dan kebijakan yang memastikan pengolahan data dilakukan secara sah dan transparan. Audit harus mencakup pemantauan penerapan kebijakan pengelolaan data pribadi yang efektif, termasuk enkripsi data, kontrol akses yang ketat, dan mekanisme pengawasan untuk mencegah pelanggaran privasi. Implementasi teknologi keamanan yang mutakhir, seperti *blockchain* atau teknologi identitas digital, juga semakin penting untuk meningkatkan lapisan perlindungan terhadap data sensitif.

A. Perlindungan Data Pelanggan dalam Sektor Keuangan

Di era digital yang semakin berkembang, sektor keuangan sangat bergantung pada teknologi informasi untuk memproses dan mengelola data pelanggan, termasuk transaksi keuangan, informasi pribadi, serta data sensitif lainnya. Oleh karena itu, perlindungan data pelanggan menjadi isu yang sangat penting, terutama mengingat meningkatnya ancaman terhadap keamanan data seperti serangan siber, pencurian identitas, dan penyalahgunaan informasi pribadi. Perlindungan data pelanggan dalam sektor keuangan tidak hanya mencakup upaya untuk

melindungi data tersebut dari ancaman eksternal, tetapi juga untuk memastikan bahwa data dikelola dengan cara yang sesuai dengan peraturan dan kebijakan yang berlaku, serta menjaga hak privasi individu. Lembaga keuangan dapat menerapkan berbagai langkah perlindungan data untuk mengurangi risiko terkait dengan pengelolaan data pelanggan. Beberapa langkah penting meliputi:

1. Enkripsi Data

Enkripsi data merupakan salah satu teknik fundamental dalam melindungi informasi sensitif dalam sektor keuangan. Prinsip dasarnya adalah mengubah data asli menjadi format yang tidak bisa dibaca tanpa kunci enkripsi yang tepat. Teknik ini sangat penting untuk melindungi data baik yang sedang ditransmisikan misalnya, informasi transaksi online maupun data yang disimpan, seperti informasi rekening dan identitas nasabah di server bank. Dalam dunia keuangan, di mana data pribadi dan keuangan sangat bernilai, enkripsi membantu mencegah akses yang tidak sah dan memastikan integritas data meskipun ada potensi kebocoran.

Penggunaan enkripsi yang kuat menjadi wajib untuk melindungi data pelanggan. Salah satu standar enkripsi yang diakui di industri adalah AES-256 (*Advanced Encryption Standard*), yang menawarkan tingkat keamanan tinggi dengan panjang kunci 256-bit. Standar ini banyak digunakan dalam berbagai aplikasi, termasuk komunikasi digital, penyimpanan data, dan transaksi online. AES-256 dianggap sangat aman karena meskipun teknologi pemrosesan komputer semakin kuat, enkripsi ini masih sulit untuk dipecahkan dengan serangan brute force, menjadikannya pilihan utama untuk melindungi data sensitif di sektor keuangan.

2. Pengelolaan Akses dan Pengawasan Sistem

Pengelolaan akses yang baik merupakan fondasi penting dalam menjaga keamanan data pelanggan di lembaga keuangan. Salah satu metode yang banyak digunakan adalah *role-based access control* (RBAC), di mana akses diberikan berdasarkan peran yang dimiliki individu dalam organisasi. Misalnya, hanya karyawan yang memiliki peran sebagai manajer yang bisa mengakses data sensitif, sementara pegawai dengan peran yang lebih rendah hanya diberikan akses terbatas. Selain itu, *attribute-based access control* (ABAC) memungkinkan

pengelolaan akses lebih fleksibel dengan mempertimbangkan atribut lain, seperti lokasi atau waktu akses, yang dapat membantu lebih lanjut dalam membatasi hak akses.

Sistem kontrol akses yang efektif tidak hanya membatasi siapa yang dapat mengakses data, tetapi juga menjamin bahwa akses tersebut dilakukan dengan cara yang aman. Oleh karena itu, penting bagi lembaga keuangan untuk menetapkan kebijakan yang jelas terkait otentikasi pengguna, seperti penggunaan kata sandi yang kuat, otentikasi dua faktor (2FA), dan mekanisme otorisasi lainnya yang dapat memverifikasi identitas pengguna sebelum memberikan akses. Kebijakan ini memastikan bahwa hanya individu yang berwenang yang dapat melihat atau memodifikasi data sensitif, sehingga mengurangi risiko penyalahgunaan akses.

3. Pencadangan Data dan Pemulihan Bencana

Pencadangan data yang rutin adalah langkah fundamental dalam menjaga integritas dan keamanan data pelanggan di lembaga keuangan. Dengan adanya cadangan data yang terorganisir, lembaga keuangan dapat mengatasi situasi darurat, seperti kerusakan perangkat keras, bencana alam, atau serangan siber yang dapat menyebabkan kehilangan data kritis. Cadangan data yang baik tidak hanya mencakup file dan data transaksi penting, tetapi juga memastikan bahwa informasi yang tersimpan dapat dipulihkan dengan cepat dan tanpa gangguan signifikan terhadap operasional. Hal ini juga mengurangi dampak negatif terhadap reputasi lembaga keuangan jika terjadi insiden yang mengancam data nasabah.

Pemulihan bencana atau *disaster recovery plan* (DRP) menjadi bagian integral dari strategi mitigasi risiko yang efektif. DRP menyusun langkah-langkah yang harus diambil oleh lembaga keuangan untuk memulihkan sistem dan data dalam waktu sesingkat mungkin setelah insiden besar. Rencana ini mencakup pengidentifikasian sumber daya yang diperlukan untuk pemulihan, pengaturan prioritas data mana yang harus dipulihkan terlebih dahulu, dan pengelolaan prosedur untuk menjaga kelangsungan operasional. Sebuah studi oleh *Gartner* (2020) menunjukkan bahwa lembaga keuangan yang memiliki rencana pemulihan bencana yang solid mampu mengurangi waktu pemulihan (*recovery time objective*/RTO) dan kerugian operasional secara signifikan setelah insiden.

4. Keamanan Jaringan dan Infrastruktur IT

Keamanan jaringan merupakan fondasi yang tak tergantikan dalam melindungi data pelanggan di lembaga keuangan. Dengan semakin berkembangnya ancaman dunia maya, seperti peretasan dan serangan malware, penting bagi lembaga keuangan untuk memastikan bahwa infrastruktur jaringannya aman. Salah satu metode dasar untuk melindungi jaringan adalah penggunaan firewall, yang berfungsi sebagai penghalang antara jaringan internal lembaga keuangan dengan jaringan eksternal yang tidak terjamin keamanannya. Firewall dapat menyaring lalu lintas data yang masuk dan keluar, memastikan hanya komunikasi yang sah yang dapat mencapai sistem internal. Penggunaan firewall yang efektif dapat meminimalkan potensi serangan dari luar yang dapat mengancam integritas data pelanggan.

Penerapan *Virtual Private Network* (VPN) juga menjadi langkah yang sangat penting dalam memperkuat keamanan jaringan. VPN memungkinkan akses jaringan yang aman, terutama bagi karyawan yang bekerja dari lokasi jauh. Dengan mengenkripsi koneksi internet, VPN menghalangi pihak yang tidak berwenang untuk mengakses data yang sedang dikirimkan melalui jaringan publik. Implementasi VPN yang baik memastikan bahwa informasi yang dikirim antar kantor atau antara karyawan dan sistem pusat lembaga keuangan tetap aman dari intersepsi oleh pihak ketiga. Sebagai tambahan, penggunaan VPN dapat melindungi lembaga keuangan dari ancaman serangan berbasis lokasi, yang mungkin berfokus pada perangkat atau infrastruktur di tempat tertentu.

5. Kepatuhan terhadap Standar Keamanan dan Regulasi

Kepatuhan terhadap standar keamanan dan regulasi perlindungan data adalah langkah yang sangat penting bagi lembaga keuangan untuk melindungi data pelanggan dan mengurangi risiko hukum. Salah satu standar internasional yang paling dikenal adalah ISO/IEC 27001, yang memberikan pedoman bagi organisasi dalam mengelola dan melindungi informasi sensitif. Standar ini menekankan pada penerapan sistem manajemen keamanan informasi yang komprehensif untuk memastikan bahwa data dikelola secara aman dan dapat diakses hanya oleh pihak yang berwenang. Dengan mengikuti ISO/IEC 27001, lembaga keuangan dapat meningkatkan kepercayaan pelanggan serta memenuhi kewajiban regulasi terkait perlindungan data pribadi.

Untuk lembaga yang berhubungan dengan transaksi pembayaran, kepatuhan terhadap standar PCI-DSS (*Payment Card Industry Data Security Standard*) juga menjadi sangat krusial. Standar ini berfokus pada perlindungan informasi kartu pembayaran dan mengharuskan lembaga keuangan untuk mengimplementasikan kebijakan dan prosedur yang ketat terkait dengan pengolahan, penyimpanan, dan transmisi data kartu pembayaran. Kepatuhan terhadap PCI-DSS tidak hanya memastikan perlindungan terhadap data nasabah, tetapi juga melindungi lembaga keuangan dari potensi kebocoran data yang bisa berujung pada kerugian finansial dan reputasi.

B. Regulasi Privasi Global (GDPR, CCPA)

Di dunia yang semakin terhubung dan terdigitalkan, privasi data pelanggan telah menjadi salah satu aspek yang paling kritikal dalam sektor bisnis, terutama dalam industri yang mengelola informasi sensitif, seperti sektor keuangan. Regulasi privasi data berperan yang sangat penting dalam memastikan bahwa data pribadi dikelola dengan cara yang aman, sah, dan transparan. Dua regulasi utama yang berfokus pada privasi data yang dapat dijadikan acuan global adalah *General Data Protection Regulation* (GDPR) yang berlaku di *Uni Eropa dan California Consumer Privacy Act* (CCPA) yang diberlakukan di negara bagian California, Amerika Serikat. Regulasi-regulasi ini tidak hanya memberikan perlindungan kepada individu, tetapi juga menantang perusahaan untuk memenuhi kewajiban baru dalam pengelolaan data pribadi. Melalui audit IT, lembaga keuangan dan organisasi lainnya dapat memastikan kepatuhan terhadap regulasi ini, mengidentifikasi potensi risiko pelanggaran, serta membangun sistem yang lebih aman untuk pengelolaan data pribadi.

1. *General Data Protection Regulation* (GDPR)

GDPR adalah regulasi yang diberlakukan oleh Uni Eropa sejak 25 Mei 2018. Tujuannya adalah untuk memberikan kontrol lebih besar kepada individu atas data pribadi dan untuk menyederhanakan peraturan perlindungan data untuk bisnis internasional dengan satu regulasi yang berlaku di seluruh Uni Eropa. GDPR berlaku bagi setiap perusahaan yang memproses data pribadi individu yang berada di Uni Eropa,

terlepas dari lokasi perusahaan tersebut. Beberapa poin penting yang perlu dipahami dalam konteks GDPR adalah sebagai berikut:

a. Hak Subjek Data: GDPR memberikan hak-hak penting kepada individu terkait data pribadi, termasuk hak untuk mengakses data, hak untuk mengoreksi data yang salah, hak untuk menghapus data, dan hak untuk menarik persetujuan.
b. Prinsip-prinsip Pemrosesan Data: GDPR menetapkan beberapa prinsip dasar yang harus diikuti dalam pemrosesan data pribadi, termasuk prinsip keadilan, transparansi, tujuan yang sah, dan pembatasan penyimpanan data.
c. Penyusunan Kebijakan Privasi yang Jelas dan Transparan: Organisasi diharuskan untuk memberi tahu individu secara jelas mengenai bagaimana data pribadi akan diproses, yang melibatkan penyusunan kebijakan privasi yang rinci dan mudah diakses.
d. Pemberitahuan Pelanggaran Data: GDPR mensyaratkan perusahaan untuk memberi pemberitahuan kepada otoritas perlindungan data dan individu yang terkena dampak dalam waktu 72 jam setelah mengetahui pelanggaran data yang dapat membahayakan privasi.
e. Penyimpanan dan Pemrosesan Data Sensitif: Pengumpulan dan pemrosesan data sensitif (seperti data kesehatan, data biometrik, atau data ras) diatur dengan ketat dan hanya diperbolehkan dalam keadaan tertentu.
f. Penunjukan DPO (*Data Protection Officer*): Organisasi yang terlibat dalam pemrosesan data pribadi dalam skala besar atau yang memiliki risiko tinggi terkait privasi data diwajibkan menunjuk seorang DPO untuk memantau dan melaporkan kepatuhan terhadap regulasi.

Pada audit IT, penting untuk memastikan bahwa organisasi mematuhi ketentuan GDPR, terutama terkait dengan pengelolaan dan pemrosesan data pribadi. Beberapa langkah yang harus dilakukan oleh auditor dalam konteks GDPR adalah:

a. Penilaian Dampak Perlindungan Data (DPIA)

   Penilaian Dampak Perlindungan Data (*Data Protection Impact Assessment*/DPIA) merupakan bagian integral dari kepatuhan terhadap *General Data Protection Regulation* (GDPR), terutama bagi organisasi yang memproses data pribadi

yang berisiko tinggi. DPIA bertujuan untuk menilai potensi risiko terhadap hak dan kebebasan individu yang dapat timbul akibat pemrosesan data. Dalam konteks audit IT, evaluasi terhadap pelaksanaan DPIA sangat penting untuk memastikan bahwa organisasi telah melakukan penilaian yang tepat sebelum memulai atau melanjutkan kegiatan pemrosesan data yang dapat berdampak signifikan terhadap privasi individu.

Audit IT harus memverifikasi apakah organisasi mengidentifikasi dan mengelola risiko terkait data pribadi dengan benar, termasuk langkah-langkah mitigasi yang diterapkan untuk mengurangi potensi dampak negatif. Hal ini mencakup penilaian terhadap kebijakan dan prosedur pemrosesan data yang ada, serta pemeriksaan apakah langkah-langkah pengamanan yang memadai diterapkan untuk melindungi data pribadi. Dengan melakukan DPIA yang tepat, organisasi tidak hanya memastikan kepatuhan terhadap GDPR, tetapi juga menunjukkan komitmen terhadap perlindungan data pribadi yang lebih kuat.

b. Evaluasi Keamanan Data

Evaluasi keamanan data merupakan langkah penting dalam audit kepatuhan terhadap *General Data Protection Regulation* (GDPR), yang bertujuan untuk melindungi data pribadi dari ancaman kebocoran atau pelanggaran. Salah satu aspek yang harus diverifikasi adalah apakah perusahaan telah mengimplementasikan langkah-langkah keamanan yang memadai, seperti enkripsi data. Enkripsi memastikan bahwa data yang sedang disimpan atau ditransmisikan tidak dapat diakses oleh pihak yang tidak berwenang, bahkan jika terjadi pelanggaran sistem. Teknik enkripsi seperti AES-256 adalah standar industri yang umum digunakan untuk melindungi data pribadi agar tetap aman selama proses pemrosesan atau pengarsipan.

Kontrol akses yang tepat juga menjadi elemen kunci dalam evaluasi keamanan data. Perusahaan harus memastikan bahwa hanya individu yang berwenang yang dapat mengakses data pribadi. Penerapan sistem kontrol akses berbasis peran (RBAC) atau kontrol akses berbasis atribut (ABAC) memungkinkan organisasi untuk membatasi akses sesuai dengan kebutuhan

setiap karyawan atau pihak eksternal. Hal ini membantu meminimalkan potensi penyalahgunaan akses oleh pihak yang tidak berhak.

c. Audit Kebijakan Privasi dan Prosedur

Audit kebijakan privasi dan prosedur adalah komponen vital dalam memastikan bahwa sebuah organisasi mematuhi prinsip-prinsip *General Data Protection Regulation* (GDPR). Salah satu prinsip utama yang harus dipatuhi adalah transparansi. Organisasi harus memiliki kebijakan privasi yang jelas dan mudah diakses oleh individu yang datanya dikumpulkan, yang menjelaskan bagaimana dan untuk tujuan apa data pribadi akan digunakan. Auditor harus mengevaluasi apakah kebijakan privasi tersebut cukup jelas dan transparan dalam menjelaskan hak-hak pengguna serta proses pengolahan data yang dilakukan oleh perusahaan.

Prinsip pembatasan tujuan juga harus diperiksa. GDPR mengharuskan data pribadi hanya diproses untuk tujuan yang spesifik dan sah, yang harus dijelaskan secara rinci dalam kebijakan privasi. Jika kebijakan privasi memungkinkan penggunaan data untuk tujuan yang tidak sesuai dengan tujuan awal pengumpulan data, auditor harus mengidentifikasi potensi pelanggaran. Prinsip ini membantu mencegah penyalahgunaan data dan melindungi hak privasi individu.

2. *California Consumer Privacy Act* (CCPA)

CCPA adalah undang-undang yang diberlakukan di negara bagian California, Amerika Serikat, yang memberikan hak kepada konsumen untuk mengontrol informasi pribadi yang dikumpulkan oleh bisnis. CCPA mulai berlaku pada 1 Januari 2020 dan memberikan konsumen hak untuk mengetahui data apa yang dikumpulkan tentangnya, hak untuk meminta penghapusan data tersebut, dan hak untuk menolak penjualan datanya. Beberapa elemen penting dari CCPA yang perlu dipahami adalah sebagai berikut:

a. Hak Akses dan Penghapusan Data: CCPA memberi konsumen hak untuk meminta perusahaan untuk mengungkapkan informasi pribadi yang telah dikumpulkan, serta meminta penghapusan informasi tersebut.

b. Penolakan Penjualan Data: Konsumen memiliki hak untuk menolak penjualan data pribadi kepada pihak ketiga. Perusahaan harus menyediakan mekanisme yang jelas bagi konsumen untuk mengekspresikan keinginan ini.
c. Pemberitahuan tentang Pengumpulan Data: Perusahaan harus memberitahukan konsumen secara jelas mengenai data apa yang dikumpulkan dan tujuan penggunaannya sebelum data tersebut dikumpulkan.
d. Keamanan Data: CCPA mengharuskan perusahaan untuk mengambil langkah-langkah yang wajar untuk melindungi data pribadi dari pelanggaran dan kebocoran.

Audit IT dalam konteks CCPA bertujuan untuk memastikan bahwa organisasi mematuhi ketentuan dalam mengelola data pribadi konsumen. Beberapa langkah audit yang penting dalam kepatuhan terhadap CCPA adalah:

a. Verifikasi Kebijakan Privasi

Verifikasi kebijakan privasi dalam konteks *California Consumer Privacy Act* (CCPA) adalah salah satu aspek krusial yang perlu diaudit untuk memastikan bahwa perusahaan mematuhi ketentuan perlindungan data yang berlaku di California. CCPA memberikan hak yang signifikan kepada konsumen, seperti hak untuk mengakses data pribadi yang dimiliki perusahaan, hak untuk menghapus data tersebut, serta hak untuk menolak penjualan data pribadi. Auditor harus mengevaluasi apakah kebijakan privasi perusahaan secara jelas menjelaskan hak-hak ini dan apakah prosedur yang diperlukan untuk mengakses, menghapus, atau menolak penjualan data telah ditetapkan dengan baik.

Auditor juga perlu memastikan bahwa kebijakan privasi tersebut menginformasikan konsumen dengan cara yang mudah dipahami, sesuai dengan prinsip transparansi yang diatur dalam CCPA. Hal ini meliputi kewajiban perusahaan untuk memberikan informasi yang jelas mengenai kategori data pribadi yang dikumpulkan, tujuan penggunaan data, dan dengan siapa data tersebut dibagikan. Evaluasi ini bertujuan untuk memastikan bahwa kebijakan privasi tidak hanya mematuhi persyaratan hukum, tetapi juga memberikan konsumen kontrol yang nyata atas data pribadi.

b. Penerapan Prosedur Penghapusan Data

Penerapan prosedur penghapusan data dalam kerangka *California Consumer Privacy Act* (CCPA) sangat penting untuk memastikan bahwa perusahaan tidak menyimpan data pribadi lebih lama dari yang diperlukan dan bahwa konsumen dapat menghapus data ketika diminta. Auditor perlu memastikan bahwa perusahaan memiliki proses yang terstruktur dan terdokumentasi dengan baik untuk menangani permintaan penghapusan data. Hal ini mencakup identifikasi data pribadi yang diminta untuk dihapus, serta pengecekan apakah data tersebut disimpan sesuai dengan kebijakan penyimpanan yang wajar.

Auditor harus mengevaluasi apakah perusahaan memiliki mekanisme yang efisien untuk memverifikasi identitas konsumen yang mengajukan permintaan penghapusan data, guna memastikan bahwa permintaan tersebut tidak dilakukan oleh pihak yang tidak berwenang. Prosedur yang jelas dan dapat diakses oleh konsumen harus tersedia untuk memudahkan pengajuan permintaan penghapusan data, misalnya melalui formulir daring atau pusat panggilan. Selain itu, perusahaan harus memastikan bahwa penghapusan data dilakukan dalam waktu yang tepat, sesuai dengan ketentuan CCPA yang memberikan batas waktu 45 hari untuk merespons permintaan.

c. Evaluasi Kontrol Akses

Evaluasi kontrol akses merupakan aspek krusial dalam memastikan bahwa data pribadi konsumen dilindungi dengan baik sesuai dengan ketentuan *California Consumer Privacy Act* (CCPA). Auditor harus menilai apakah perusahaan telah menerapkan kebijakan yang ketat untuk membatasi akses ke data pribadi hanya kepada individu yang memiliki otorisasi yang sah. Hal ini mencakup penerapan mekanisme kontrol akses berbasis peran (*role-based access control*, RBAC), di mana hak akses diberikan berdasarkan fungsi dan tanggung jawab pengguna dalam organisasi. Auditor harus memastikan bahwa hanya karyawan atau pihak yang benar-benar membutuhkan akses untuk menjalankan tugas yang diberikan izin untuk mengakses data pribadi konsumen.

Auditor perlu mengevaluasi penerapan autentikasi yang kuat, seperti penggunaan otentikasi multi-faktor (MFA), untuk memperkuat proses verifikasi pengguna yang mengakses data sensitif. MFA membantu mencegah akses yang tidak sah meskipun kredensial pengguna bocor atau dicuri. Audit harus memeriksa apakah perusahaan melakukan audit log secara teratur untuk mendeteksi aktivitas akses yang tidak sah atau mencurigakan dan apakah ada kebijakan untuk meninjau dan memperbarui akses secara periodik. Hal ini membantu memastikan bahwa akses ke data pribadi konsumen hanya dilakukan oleh pihak yang berwenang dan untuk tujuan yang sah.

C. Teknik Enkripsi dan Proteksi Data

Enkripsi adalah proses mengubah data asli menjadi format yang tidak dapat dibaca tanpa kunci dekripsi yang sesuai. Data yang telah dienkripsi hanya dapat dibaca oleh pihak yang memiliki kunci atau akses yang sah. Proteksi data, di sisi lain, mencakup berbagai metode yang digunakan untuk melindungi data dari ancaman yang dapat merusak, merusak, atau mengakses data tersebut tanpa izin. Proteksi data ini termasuk enkripsi, kontrol akses, penggunaan firewall, dan sistem deteksi intrusi. Tujuan utama dari enkripsi adalah untuk melindungi data saat disimpan (*data at rest*), dalam perjalanan (*data in transit*), atau saat sedang diproses (*data in use*). Penggunaan enkripsi juga memberikan perlindungan terhadap kebocoran data yang tidak disengaja maupun pencurian data oleh pihak yang tidak berwenang.

1. Jenis-jenis Teknik Enkripsi

Enkripsi dapat dibagi menjadi dua kategori utama: enkripsi simetris dan enkripsi asimetris. Masing-masing teknik ini memiliki karakteristik dan penerapan yang berbeda, yang bergantung pada kebutuhan organisasi dan data yang sedang diproses.

a. Enkripsi Simetris (*Symmetric Encryption*)

Enkripsi simetris menggunakan kunci yang sama untuk enkripsi dan dekripsi data. Ini adalah teknik yang lebih cepat dan efisien, terutama ketika mengelola sejumlah besar data. Namun, kelemahan utama dari enkripsi simetris adalah tantangan dalam mengelola dan membagikan kunci secara aman. Jika kunci

tersebut jatuh ke tangan yang salah, maka seluruh data yang dienkripsi dengan kunci tersebut dapat diakses oleh pihak yang tidak berwenang.

b. Enkripsi Asimetris (*Asymmetric Encryption*)

Berbeda dengan enkripsi simetris, enkripsi asimetris menggunakan dua kunci yang berbeda: kunci publik dan kunci privat. Kunci publik digunakan untuk mengenkripsi data, sementara kunci privat digunakan untuk mendekripsinya. Enkripsi asimetris lebih aman dibandingkan enkripsi simetris karena kunci privat tidak perlu dibagikan, tetapi lebih lambat dalam pemrosesannya.

c. Teknik Enkripsi Lainnya

Terdapat beberapa teknik enkripsi lainnya yang digunakan dalam berbagai aplikasi dan skenario, di antaranya:

1) *Homomorphic Encryption*: Jenis enkripsi ini memungkinkan perhitungan dilakukan pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu. Ini sangat berguna dalam konteks *cloud computing*, di mana data harus diproses tanpa mengungkapkan informasi sensitif kepada penyedia layanan.
2) *Quantum Cryptography*: Teknik enkripsi ini didasarkan pada prinsip fisika kuantum dan menjanjikan tingkat keamanan yang sangat tinggi, meskipun teknologi ini masih dalam tahap penelitian dan pengembangan.

2. Strategi Proteksi Data dalam Audit IT

Terdapat berbagai strategi proteksi data yang digunakan untuk memastikan bahwa data yang sensitif terlindungi dengan baik. Beberapa strategi proteksi data yang relevan dalam konteks audit IT adalah sebagai berikut:

a. Kontrol Akses

Kontrol akses merupakan langkah penting dalam melindungi data sensitif, karena hanya individu yang berwenang yang dapat mengakses informasi tersebut. Salah satu metode kontrol akses yang umum digunakan adalah Kontrol Akses Berbasis Peran (RBAC). Dalam sistem RBAC, hak akses diberikan kepada pengguna berdasarkan perannya dalam organisasi, bukan berdasarkan identitas individu. Pendekatan ini memungkinkan perusahaan untuk mengelola hak akses dengan lebih efisien dan

memastikan bahwa hanya pengguna yang memiliki peran tertentu yang dapat mengakses data yang relevan dengan tugas.

b. Firewall dan Sistem Deteksi Intrusi

Firewall dan sistem deteksi intrusi (IDS) adalah dua komponen utama dalam melindungi jaringan dan sistem informasi dari ancaman keamanan. Firewall bertindak sebagai penghalang antara jaringan internal yang aman dan jaringan eksternal yang tidak terpercaya, seperti internet. Firewall memfilter lalu lintas data yang masuk dan keluar, memastikan hanya data yang sah yang dapat melewati batasan ini. Tipe firewall yang paling umum adalah firewall berbasis aturan, yang memblokir atau mengizinkan akses berdasarkan serangkaian aturan yang telah ditentukan sebelumnya, seperti alamat IP, port, atau protokol yang digunakan. Firewall dapat ditempatkan di tingkat jaringan atau aplikasi untuk memberikan proteksi yang lebih mendalam.

Sistem Deteksi Intrusi (IDS) memiliki peran yang sangat penting dalam mendeteksi potensi ancaman dalam jaringan. IDS memantau lalu lintas data secara *real-time* dan menganalisis pola untuk mendeteksi aktivitas yang mencurigakan, seperti upaya penyusupan atau peretasan. Terdapat dua jenis utama IDS: IDS berbasis jaringan dan IDS berbasis host. IDS berbasis jaringan memantau lalu lintas yang melewati jaringan, sementara IDS berbasis host memantau aktivitas yang terjadi pada sistem atau perangkat tertentu. IDS dapat memberikan peringatan dini kepada administrator jaringan mengenai potensi ancaman yang dapat merusak integritas sistem.

c. Backup dan Pemulihan Data

Backup dan pemulihan data adalah langkah penting dalam strategi proteksi data yang harus diterapkan dalam organisasi untuk melindungi data dari potensi kehilangan yang disebabkan oleh serangan ransomware, bencana alam, atau kesalahan manusia. Backup data yang teratur dan terorganisir dengan baik memastikan bahwa salinan data penting disimpan di lokasi yang aman, baik itu secara lokal maupun di *cloud*. Backup yang baik harus mencakup seluruh data vital, termasuk konfigurasi sistem, file aplikasi, dan data pelanggan, untuk memastikan pemulihan yang efektif setelah terjadinya insiden. Penjadwalan backup

secara otomatis dan menggunakan teknik backup incremental dapat meminimalkan gangguan terhadap operasional sambil memastikan data tetap aman.

Backup data saja tidak cukup jika tidak dilengkapi dengan prosedur pemulihan data yang baik. Prosedur ini memastikan bahwa data yang telah dicadangkan dapat dipulihkan dengan cepat dan akurat dalam situasi darurat. Uji coba pemulihan data secara rutin sangat penting untuk memvalidasi bahwa sistem backup bekerja sesuai rencana dan dapat diandalkan saat dibutuhkan. Pemulihan data yang cepat sangat penting, terutama bagi perusahaan yang bergantung pada data untuk operasional harian. Jika data tidak dapat dipulihkan dengan cepat, bisnis dapat mengalami kerugian yang signifikan, baik dalam hal pendapatan maupun reputasi.

D. Penanganan Insiden Keamanan Data

Penanganan insiden keamanan data merupakan salah satu aspek penting dalam mengelola keamanan informasi dalam organisasi. Keamanan data yang efektif tidak hanya bergantung pada langkah pencegahan seperti enkripsi, kontrol akses, dan firewall, tetapi juga pada kemampuan organisasi untuk merespons dan menangani insiden ketika terjadi kebocoran atau pelanggaran data. Hal ini sangat relevan dalam konteks audit IT, di mana organisasi diharuskan untuk menunjukkan bahwa ia telah memiliki rencana yang matang dan sistem yang sesuai untuk mendeteksi, merespons, dan memitigasi insiden keamanan data.

Insiden keamanan data mencakup berbagai kejadian yang dapat merusak integritas, kerahasiaan, atau ketersediaan data dalam sistem. Ini termasuk serangan dunia maya seperti ransomware, phishing, pencurian identitas, serta kebocoran data yang disebabkan oleh kesalahan manusia atau kegagalan sistem. Insiden ini bisa berdampak signifikan terhadap reputasi perusahaan, kepercayaan pelanggan, serta dapat menyebabkan kerugian finansial yang substansial akibat denda, biaya pemulihan, atau kehilangan data sensitif. Keberhasilan penanganan insiden keamanan data sangat bergantung pada seberapa cepat dan efektif organisasi dapat merespons dan mengendalikan insiden tersebut.

1. Rencana Respons Insiden (*Incident Response Plan*)

Rencana respons insiden adalah serangkaian prosedur yang dirancang untuk membantu organisasi merespons insiden keamanan secara efektif dan cepat. Rencana ini harus disusun dengan melibatkan berbagai pihak dalam organisasi, termasuk tim keamanan siber, manajer IT, serta tim hukum dan komunikasi. Rencana respons insiden yang baik melibatkan beberapa tahap yang perlu dilakukan secara terstruktur:

a. Pengenalan dan Deteksi Insiden

Pengenalan dan deteksi insiden adalah langkah pertama yang krusial dalam rencana respons insiden (*Incident Response Plan*, IRP) untuk menjaga keamanan data. Deteksi dini terhadap ancaman atau pelanggaran dapat mencegah kerusakan lebih lanjut yang dapat memengaruhi integritas data dan reputasi organisasi. Salah satu alat utama dalam deteksi insiden adalah *Intrusion Detection Systems* (IDS). Sistem ini dirancang untuk memantau lalu lintas jaringan secara *real-time* dan mendeteksi perilaku yang tidak biasa atau tanda-tanda potensi serangan seperti upaya intrusi atau manipulasi data. IDS memberikan peringatan secara otomatis saat terdeteksi adanya ancaman yang mungkin belum diketahui sebelumnya.

Security Information and Event Management (SIEM) adalah alat penting lainnya yang digunakan untuk meningkatkan deteksi insiden. SIEM mengumpulkan dan menganalisis data dari berbagai sumber, termasuk perangkat jaringan, server, aplikasi, dan perangkat keamanan lainnya. Dengan menganalisis data secara terpusat, SIEM memungkinkan identifikasi insiden yang terjadi dalam waktu yang lebih singkat, bahkan sebelum ancaman tersebut berkembang menjadi pelanggaran besar. SIEM juga berfungsi untuk menghubungkan peristiwa yang tersebar dan memberikan gambaran lebih jelas tentang serangan yang sedang berlangsung, serta memberikan peringatan kepada tim keamanan agar dapat segera melakukan respons.

b. Penanggulangan dan Isolasi Insiden

Setelah insiden terdeteksi dalam sistem keamanan informasi, langkah berikutnya adalah melakukan penanggulangan dan isolasi untuk meminimalkan dampak yang ditimbulkan oleh ancaman tersebut. Salah satu tindakan pertama yang harus diambil adalah pemutusan koneksi jaringan dari sistem yang

terinfeksi. Dengan memutuskan koneksi ini, ancaman yang sedang terjadi, seperti serangan malware atau ransomware, dapat dibatasi pada sistem yang terinfeksi tanpa menyebar ke perangkat lain dalam jaringan. Hal ini mengurangi potensi kerusakan lebih lanjut pada infrastruktur yang lebih luas, serta melindungi data sensitif yang mungkin sedang terancam.

Langkah selanjutnya yang krusial adalah isolasi sistem yang terinfeksi. Mengisolasi sistem ini bisa berarti mematikan server atau menonaktifkan perangkat yang terinfeksi agar tidak dapat berkomunikasi lebih lanjut dengan komponen lain dalam jaringan. Dengan cara ini, risiko penyebaran serangan atau infeksi ke sistem lainnya dapat diminimalkan. Tindakan isolasi ini memastikan bahwa serangan tidak berkembang lebih jauh dan membantu tim respons untuk lebih fokus dalam menangani insiden tanpa gangguan dari elemen eksternal.

c. Penyelidikan dan Analisis Insiden

Setelah insiden terdeteksi dan sistem yang terinfeksi diisolasi, langkah selanjutnya dalam Rencana Respons Insiden (*Incident Response Plan*) adalah penyelidikan dan analisis insiden. Proses ini bertujuan untuk mengidentifikasi penyebab insiden dan dampaknya. Penyelidikan ini melibatkan pengumpulan dan pemeriksaan bukti-bukti digital, log, serta data yang terkait dengan kejadian tersebut. Proses ini sangat penting untuk memahami bagaimana serangan terjadi dan untuk menilai tingkat kerusakan yang ditimbulkan. Tanpa analisis yang tepat, organisasi tidak akan bisa mengidentifikasi apakah serangan telah merusak data penting atau apakah ancaman masih aktif dalam sistem.

Salah satu teknik utama yang digunakan dalam penyelidikan adalah forensik digital, yang melibatkan analisis perangkat keras, perangkat lunak, dan data yang ada untuk menemukan bukti yang menunjukkan sumber serta metodologi serangan. Forensik digital tidak hanya digunakan untuk melacak aktivitas serangan, tetapi juga untuk memulihkan data yang hilang atau rusak, serta mengidentifikasi vektor serangan yang mungkin tidak terlihat pada awalnya. Teknik ini memungkinkan organisasi untuk mengungkapkan bagaimana serangan dimulai, bagaimana menyebar, dan apakah ada data sensitif yang terkompromikan.

d. Pemulihan dan Perbaikan Sistem

Setelah menganalisis dan memahami insiden, langkah berikutnya dalam Rencana Respons Insiden (*Incident Response Plan*) adalah pemulihan dan perbaikan sistem. Tahap ini sangat penting untuk memastikan bahwa organisasi dapat kembali beroperasi setelah insiden tanpa adanya kerusakan yang berkelanjutan. Pemulihan data merupakan langkah pertama yang harus dilakukan setelah insiden. Data yang hilang atau rusak akibat serangan harus dipulihkan dengan menggunakan cadangan yang telah dibuat sebelumnya. Proses pemulihan harus dilakukan dengan hati-hati untuk memastikan bahwa tidak ada data yang terlewat, serta untuk mencegah kerusakan lebih lanjut yang bisa terjadi jika pemulihan dilakukan sembarangan.

Pembaruan perangkat lunak dan patch keamanan merupakan langkah penting untuk memastikan bahwa perangkat lunak dan sistem yang terinfeksi telah diperbaiki dan diperbarui dengan patch keamanan terbaru. Serangan sering kali mengeksploitasi celah yang ada pada sistem, dan jika celah tersebut tidak ditutup dengan pembaruan yang tepat, sistem akan tetap rentan terhadap serangan serupa di masa depan. Pembaruan ini termasuk pembaruan untuk sistem operasi, aplikasi, dan perangkat keras yang digunakan oleh organisasi. Pengabaian terhadap pembaruan keamanan dapat menyebabkan potensi serangan yang berkelanjutan atau bahkan memperburuk dampak dari insiden tersebut.

e. Pelaporan dan Dokumentasi

Pelaporan dan dokumentasi adalah komponen yang sangat penting dalam penanganan insiden keamanan. Setiap langkah yang diambil selama respons insiden harus didokumentasikan dengan rinci, mulai dari deteksi awal hingga pemulihan akhir. Dokumentasi ini tidak hanya berfungsi untuk mencatat apa yang telah dilakukan, tetapi juga sebagai dasar untuk evaluasi insiden. Evaluasi ini sangat penting untuk memahami bagaimana insiden ditangani, mengidentifikasi kekuatan dan kelemahan dalam respons, serta memberi wawasan tentang perbaikan yang dapat diterapkan di masa depan. Tanpa dokumentasi yang baik, organisasi akan kesulitan untuk belajar dari insiden yang terjadi,

sehingga mengurangi efektivitas rencana respons di masa mendatang.

Dokumentasi yang tepat juga mendukung pelaporan kepada otoritas yang relevan. Dalam beberapa kasus, seperti pelanggaran data pribadi yang melibatkan informasi sensitif, organisasi wajib melaporkan insiden tersebut kepada badan pengatur seperti Regulator Perlindungan Data atau Badan Regulasi Keuangan. Pelaporan yang tepat waktu dan lengkap memungkinkan otoritas untuk mengambil langkah-langkah yang diperlukan, seperti pemberitahuan kepada individu yang terdampak atau tindakan korektif yang lebih lanjut. Kegagalan dalam pelaporan ini dapat mengakibatkan sanksi hukum dan denda yang signifikan, serta merusak reputasi organisasi.

2. Komunikasi Selama Insiden

Komunikasi yang jelas dan tepat sangat penting selama penanganan insiden keamanan. Komunikasi internal harus dilakukan secara teratur untuk menyampaikan informasi yang relevan kepada semua pemangku kepentingan dalam organisasi, termasuk tim teknis, manajemen, dan tim hukum. Tim teknis membutuhkan informasi terbaru tentang perkembangan insiden untuk dapat merespons secara cepat, sedangkan manajemen dan tim hukum perlu memahami status insiden untuk membuat keputusan yang tepat dan mematuhi kewajiban hukum. Komunikasi yang tidak efektif atau terlambat dapat memperburuk situasi dan memperpanjang waktu yang dibutuhkan untuk memitigasi dampak insiden.

Komunikasi eksternal juga krusial. Organisasi harus memastikan bahwa informasi yang dibutuhkan disampaikan dengan jelas kepada pelanggan dan pihak lain yang terkena dampak, seperti mitra bisnis atau pihak ketiga yang terkait. Transparansi tentang apa yang terjadi dan langkah-langkah yang diambil untuk memperbaiki keadaan akan memberikan rasa aman kepada pihak yang terkena dampak dan menjaga kepercayaan. Selain itu, perusahaan perlu mematuhi regulasi yang mengharuskan pemberitahuan kepada pihak berwenang dan pelanggan terkait pelanggaran data pribadi atau informasi sensitif lainnya.

3. Evaluasi dan Peningkatan Rencana Respons Insiden

Setelah insiden selesai ditangani, evaluasi keefektifan respons merupakan langkah penting untuk menilai seberapa cepat dan efisien tim dalam mengatasi ancaman yang ada. Kecepatan dalam merespons sangat penting untuk meminimalkan kerusakan lebih lanjut. Evaluasi ini melibatkan penilaian terhadap waktu yang dibutuhkan untuk mendeteksi insiden, mengisolasi ancaman, dan memulihkan sistem. Dalam hal ini, kecepatan respons dapat dipengaruhi oleh sejauh mana tim siap dan terlatih, serta bagaimana alat yang digunakan dalam deteksi dan pemulihan berfungsi dalam situasi nyata. Penelitian menunjukkan bahwa kesiapan tim dan sistem yang optimal dapat mengurangi waktu yang diperlukan untuk mengatasi insiden secara signifikan.

Identifikasi kelemahan dalam rencana respons sangat penting untuk meningkatkan kesiapsiagaan di masa depan. Setiap insiden memberikan wawasan baru tentang potensi celah dalam kebijakan atau prosedur yang ada. Misalnya, kelemahan mungkin ditemukan dalam sistem deteksi yang tidak cukup cepat mendeteksi ancaman, atau dalam komunikasi yang tidak lancar antar tim. Proses evaluasi ini akan mencakup analisis mendalam tentang aspek mana dari deteksi, analisis, dan pemulihan yang perlu diperbaiki. Pembelajaran dari insiden ini membantu organisasi mengidentifikasi titik-titik lemah yang sebelumnya tidak terdeteksi, serta memvalidasi efektivitas respons yang diterapkan.

E. Studi Kasus: Pelanggaran Keamanan Data di Lembaga Keuangan

Keamanan data dan privasi menjadi aspek yang sangat penting dalam audit TI, terutama di sektor lembaga keuangan yang mengelola informasi pribadi dan keuangan sensitif. Pelanggaran terhadap data ini dapat menimbulkan kerugian finansial yang signifikan, merusak reputasi, dan menurunkan kepercayaan nasabah.

1. Capital One (2019)

Pada tahun 2019, Capital One menghadapi salah satu insiden keamanan data terbesar yang pernah terjadi di sektor keuangan. Peretasan ini berhasil mengeksploitasi kelemahan konfigurasi firewall

yang tidak memadai dalam pengelolaan infrastruktur berbasis *cloud*. Akibatnya, lebih dari 100 juta data nasabah, termasuk informasi pribadi seperti nomor jaminan sosial, data rekening bank, dan informasi kartu kredit, bocor ke tangan pelaku kejahatan siber. Meskipun tidak semua data bersifat keuangan yang langsung, insiden ini meningkatkan risiko penipuan dan pencurian identitas secara signifikan. Insiden ini diakibatkan oleh kurangnya perhatian terhadap keamanan pada lingkungan *cloud*. Meskipun *cloud* sering dipromosikan sebagai solusi aman untuk penyimpanan data, konfigurasi yang tidak tepat dapat menjadi celah bagi serangan siber. Dalam kasus ini, seorang mantan karyawan *Amazon Web Services* (AWS) memanfaatkan kerentanan firewall untuk mendapatkan akses tidak sah ke data nasabah. Hal ini menunjukkan pentingnya penerapan kontrol keamanan yang ketat, bahkan ketika menggunakan teknologi canggih seperti *cloud computing*.

Pelanggaran ini memicu keprihatinan global terhadap pengelolaan data dalam sektor keuangan. Capital One menerima banyak kritik karena gagal melindungi informasi sensitif pelanggan, yang dianggap sebagai salah satu kewajiban utama lembaga keuangan. Regulator, seperti *Office of the Comptroller of the Currency* (OCC) di Amerika Serikat, menjatuhkan denda besar kepada Capital One karena pelanggaran ini. Perusahaan harus membayar lebih dari $80 juta dalam denda dan menghadapi tuntutan hukum dari nasabah yang merasa dirugikan. Dampaknya terhadap nasabah tidak hanya berupa risiko pencurian identitas tetapi juga hilangnya kepercayaan terhadap Capital One sebagai penyedia layanan keuangan. Banyak pelanggan mengkhawatirkan potensi penggunaan data untuk tujuan ilegal, termasuk pembukaan akun palsu dan pengajuan pinjaman atas namanya. Meskipun Capital One berupaya memberikan layanan monitoring identitas gratis kepada korban, tindakan ini dianggap tidak cukup untuk mengembalikan kepercayaan penuh dari publik.

Dari sisi organisasi, insiden ini mendorong Capital One untuk mengevaluasi ulang kebijakan keamanan. Perusahaan memperkenalkan langkah-langkah baru untuk meningkatkan keamanan *cloud*, termasuk penggunaan kontrol akses yang lebih ketat, pemantauan keamanan *real-time*, dan pelatihan untuk tim IT, juga mengadopsi kerangka kerja keamanan seperti NIST *Cybersecurity Framework* untuk mengidentifikasi, melindungi, mendeteksi, dan merespons ancaman lebih proaktif di masa depan. Insiden ini menjadi pelajaran penting bagi

industri keuangan lainnya. Banyak bank dan lembaga keuangan mulai meningkatkan fokus pada keamanan siber, terutama untuk memastikan bahwa lingkungan *cloud* aman dari ancaman. Investasi dalam teknologi seperti *artificial intelligence* (AI) untuk deteksi ancaman otomatis dan enkripsi data menjadi prioritas utama setelah insiden Capital One.

2. T-Mobile US (2023)

Pada awal tahun 2023, T-Mobile US mengalami pelanggaran data besar yang memengaruhi sekitar 37 juta pelanggan. Insiden ini terjadi akibat eksploitasi pada *Application Programming Interface* (API) layanan pelanggan. API, yang dirancang untuk mempermudah akses informasi, menjadi celah yang dimanfaatkan pelaku untuk mendapatkan data pribadi pelanggan tanpa terdeteksi. Data yang bocor meliputi nama, alamat, tanggal lahir, dan rincian akun, meskipun data keuangan seperti nomor kartu kredit atau rekening bank tidak terungkap. Eksploitasi ini menggarisbawahi kerentanan pada infrastruktur teknologi informasi modern, terutama API yang sering menjadi target serangan karena fungsinya yang vital dalam integrasi sistem. Dalam kasus ini, T-Mobile menyatakan bahwa pelanggaran tersebut mulai terjadi pada akhir November 2022, tetapi baru terdeteksi pada Januari 2023. Keterlambatan dalam deteksi ini menimbulkan kekhawatiran terkait efektivitas sistem keamanan, terutama pada pemantauan aktivitas API secara *real-time*.

Meskipun data keuangan tidak terungkap, paparan data pribadi tetap memiliki risiko besar, terutama dalam serangan phishing dan penipuan identitas. Informasi seperti nama lengkap, alamat, dan tanggal lahir dapat digunakan untuk membangun kepercayaan dalam upaya phishing yang ditargetkan. Serangan ini dapat mengelabui korban untuk memberikan data yang lebih sensitif, seperti informasi login atau data keuangan, yang dapat menyebabkan kerugian lebih lanjut. T-Mobile telah menghadapi beberapa pelanggaran data serupa dalam beberapa tahun terakhir, menjadikan insiden ini sebagai tambahan pada rekam jejak yang kurang baik terkait keamanan informasi. Pada tahun 2021, perusahaan juga mengalami pelanggaran yang memengaruhi lebih dari 50 juta pengguna. Insiden berulang ini membahas perlunya peningkatan sistem keamanan yang signifikan untuk melindungi pelanggan.

Sebagai tanggapan terhadap insiden 2023, T-Mobile menyatakan telah melakukan langkah mitigasi untuk menutup celah keamanan pada API yang dieksploitasi. Selain itu, perusahaan berupaya memperkuat

sistem pemantauan dan audit keamanan untuk mencegah kejadian serupa. Namun, tanggapan ini tidak sepenuhnya menghapus kekhawatiran pelanggan dan regulator terhadap kemampuan perusahaan dalam mengelola risiko keamanan siber. Insiden ini juga menarik perhatian regulator, termasuk Komisi Komunikasi Federal (FCC), yang telah membuka penyelidikan terkait pelanggaran tersebut. Pengawasan ketat ini menunjukkan bahwa regulator semakin serius dalam menangani masalah keamanan data, terutama di sektor telekomunikasi yang menyimpan data pribadi dalam jumlah besar. Hal ini juga mendorong perusahaan seperti T-Mobile untuk memprioritaskan investasi dalam teknologi keamanan canggih, seperti deteksi anomali berbasis kecerdasan buatan (AI).

BAB VII
TEKNOLOGI PENDUKUNG AUDIT IT

Teknologi Pendukung Audit IT berfokus pada alat dan teknologi yang memperkuat efisiensi dan efektivitas proses audit dalam sektor keuangan. Dalam era digital yang semakin maju, teknologi berperan penting dalam mempermudah auditor untuk mengidentifikasi risiko, menganalisis data, dan memastikan kepatuhan terhadap regulasi. Teknologi ini mencakup berbagai perangkat lunak dan sistem yang memungkinkan auditor untuk melakukan analisis data secara lebih mendalam, mendeteksi anomali, serta melakukan audit secara lebih cepat dan tepat. Dengan adanya kemajuan teknologi seperti big data, *machine learning*, dan *artificial intelligence* (AI), auditor dapat membahas sejumlah besar data untuk menemukan potensi kesalahan atau pelanggaran yang sebelumnya sulit terdeteksi.

Seiring dengan perkembangan teknologi, auditor IT juga memanfaatkan perangkat khusus untuk mendukung audit yang lebih komprehensif dan akurat. Teknologi seperti analisis data otomatis dan pemrograman berbasis risiko semakin diterapkan dalam audit untuk meminimalkan kesalahan manusia dan mempercepat proses evaluasi. Penggunaan alat seperti *Continuous Auditing*, yang memungkinkan pemantauan berkelanjutan terhadap sistem IT perusahaan, memberikan auditor gambaran yang lebih jelas dan waktu yang lebih efektif dalam mengidentifikasi potensi risiko atau kerentanannya. Ini sejalan dengan meningkatnya penggunaan tools untuk penilaian keamanan siber, yang berperan penting dalam menjaga keutuhan data dan sistem keuangan.

A. Pemanfaatan Big Data dalam Audit IT

Big data merujuk pada kumpulan data yang sangat besar dan kompleks yang tidak dapat diproses menggunakan perangkat lunak pengelolaan data tradisional. Big data memiliki lima karakteristik utama yang dikenal sebagai 5Vs, yaitu *Volume, Velocity, Variety, Veracity,* dan *Value*. Dalam konteks audit IT, big data dapat mencakup data transaksi yang melibatkan jutaan atau bahkan miliaran baris data, serta berbagai jenis data yang berasal dari berbagai sumber dan sistem yang beragam. Pemanfaatan big data dalam audit IT memberi kemampuan untuk melakukan analisis yang lebih mendalam dan lebih cepat, mengidentifikasi pola, serta mendeteksi potensi masalah atau ketidakpatuhan secara lebih efisien.

1. Peran Big Data dalam Audit IT

a. Meningkatkan Efektivitas Analisis Risiko

Big data berperan yang semakin penting dalam meningkatkan efektivitas analisis risiko dalam audit IT. Dengan kemampuan untuk mengumpulkan dan memproses data dalam jumlah besar dari berbagai sumber secara *real-time*, auditor dapat memperoleh gambaran yang lebih jelas dan komprehensif tentang status keamanan dan operasional sebuah organisasi. Data yang lebih kaya memungkinkan auditor untuk mengidentifikasi pola dan anomali yang mungkin terlewat dalam audit tradisional yang mengandalkan sampel atau teknik inspeksi terbatas. Misalnya, menggunakan algoritma pembelajaran mesin untuk menganalisis transaksi, auditor dapat dengan cepat mendeteksi pola yang mencurigakan, seperti jumlah transaksi yang tidak biasa atau aliran dana yang tidak sesuai dengan kebiasaan normal, yang mungkin menandakan adanya aktivitas kecurangan atau kesalahan sistem (Davenport & Patil, 2022).

Kemampuan untuk menganalisis data dalam volume besar dan kecepatan tinggi memungkinkan identifikasi risiko yang lebih dini, memberikan auditor kesempatan untuk merespons lebih cepat. Misalnya, analisis big data memungkinkan deteksi lebih cepat terhadap anomali dalam aliran transaksi atau pola penggunaan sistem yang tidak sesuai dengan kebiasaan, yang mungkin menunjukkan adanya pelanggaran atau kesalahan

operasional. Dengan menggunakan model prediktif berbasis big data, auditor dapat memitigasi risiko yang mungkin timbul dengan lebih efektif, mengurangi dampak negatif terhadap organisasi.

b. Mempercepat Proses Audit

Big data berperan besar dalam mempercepat proses audit dengan memungkinkan auditor untuk memproses dan menganalisis volume data yang sangat besar dalam waktu yang lebih singkat. Dalam konteks perusahaan besar dengan transaksi yang berjumlah jutaan atau bahkan miliaran, seperti lembaga keuangan atau bank, pengolahan data secara manual melalui metode audit tradisional akan sangat memakan waktu dan rentan terhadap ketidakakuratan. Teknologi big data memungkinkan auditor untuk mengakses seluruh kumpulan data dan menggunakan algoritma untuk menyaring informasi yang relevan secara otomatis. Hal ini tidak hanya menghemat waktu, tetapi juga meningkatkan akurasi dalam menemukan anomali atau ketidaksesuaian dalam data.

Dengan big data, auditor dapat melakukan analisis data secara *real-time*, yang memungkinkan identifikasi masalah jauh lebih cepat daripada dengan audit tradisional. Teknologi ini memungkinkan pemrosesan data yang lebih efisien, mengurangi waktu yang dibutuhkan untuk memverifikasi informasi dan mencari potensi kesalahan atau pelanggaran dalam transaksi. Misalnya, dengan menggunakan alat berbasis big data, auditor dapat dengan cepat meninjau pola transaksi yang mencurigakan atau tidak sesuai dengan kebiasaan normal perusahaan, memungkinkan respons yang lebih cepat terhadap potensi masalah. Hal ini sangat penting dalam sektor-sektor yang bergantung pada data dalam jumlah besar, seperti perbankan, di mana kecepatan dan akurasi sangat menentukan.

c. Menjamin Kepatuhan terhadap Regulasi

Big data berperan penting dalam memastikan kepatuhan terhadap regulasi di sektor keuangan dengan memungkinkan auditor untuk secara efektif memantau dan menganalisis data dalam jumlah besar. Dalam konteks regulasi yang ketat seperti *General Data Protection Regulation* (GDPR) atau *Sarbanes-Oxley Act* (SOX), auditor dapat menggunakan teknologi big data

untuk memverifikasi apakah transaksi dan prosedur yang dilakukan oleh organisasi mematuhi standar yang ditetapkan. Misalnya, dengan menganalisis data transaksi secara otomatis, auditor dapat memastikan bahwa informasi pelanggan diperlakukan sesuai dengan prinsip privasi yang ditetapkan oleh GDPR, serta memeriksa apakah laporan keuangan memenuhi persyaratan yang diatur dalam SOX.

Big data memungkinkan auditor untuk mengidentifikasi ketidakpatuhan secara *real-time*. Dengan alat analisis berbasis big data, auditor dapat dengan cepat mendeteksi pola transaksi yang tidak sesuai dengan regulasi atau kebijakan internal. Misalnya, jika ada transaksi yang mencurigakan yang melibatkan data pribadi pelanggan atau laporan keuangan yang tidak sesuai dengan standar, teknologi big data dapat segera mengidentifikasi dan mengingatkan auditor. Ini sangat penting dalam sektor yang sangat teregulasi seperti perbankan dan asuransi, di mana ketidakpatuhan dapat menimbulkan sanksi besar atau merusak reputasi organisasi.

2. Teknik dan Alat yang Digunakan dalam Big Data untuk Audit IT

a. *Machine Learning* (Pembelajaran Mesin)

Machine learning (ML) berperan krusial dalam analisis data untuk audit IT, karena kemampuannya untuk secara otomatis mengidentifikasi pola dan anomali dalam data yang dapat menunjukkan adanya risiko atau pelanggaran. Dalam konteks audit, algoritma ML dapat dilatih untuk mengenali pola yang tidak biasa atau perilaku mencurigakan yang mungkin tidak terlihat dengan analisis manual. Sebagai contoh, dalam audit transaksi finansial, sistem berbasis ML dapat mendeteksi pola penipuan seperti transaksi yang dilakukan dalam waktu singkat atau oleh akun yang tidak terverifikasi. Algoritma ini dapat terus belajar dari data yang ada, memperbaiki kemampuan deteksi seiring berjalannya waktu.

Penerapan *machine learning* dalam audit IT tidak hanya terbatas pada deteksi penipuan, tetapi juga meluas ke identifikasi ketidakberesan lainnya dalam sistem. Dengan menggunakan teknik seperti *supervised learning* dan *unsupervised learning*,

sistem dapat menganalisis data historis untuk memprediksi dan mengidentifikasi anomali yang mungkin terjadi di masa depan. Misalnya, teknik unsupervised *learning* dapat digunakan untuk menemukan pola dalam data yang tidak teridentifikasi sebelumnya, sementara supervised *learning* dapat diterapkan untuk memverifikasi dan memvalidasi data berdasarkan kriteria yang telah ditentukan sebelumnya. Penggunaan teknik-teknik ini memungkinkan auditor untuk mempercepat proses deteksi dan mengurangi risiko kesalahan.

b. Analisis Sentimen dan Teks

Analisis sentimen dan teks merupakan alat yang sangat berguna dalam audit IT untuk menilai data tidak terstruktur, seperti email, laporan, dan komunikasi lainnya. Teknologi ini memungkinkan auditor untuk mengevaluasi nada, konteks, dan makna yang terkandung dalam teks, yang dapat memberikan wawasan lebih dalam mengenai perilaku individu atau kelompok yang mungkin mencurigakan. Misalnya, analisis sentimen dapat digunakan untuk mendeteksi sikap negatif atau ketidakpuasan yang mungkin menandakan adanya risiko pelanggaran atau ketidaksesuaian dengan kebijakan perusahaan. Selain itu, ini juga dapat membantu mengidentifikasi adanya kecurangan atau penyimpangan dalam komunikasi internal atau eksternal perusahaan yang tidak dapat dilihat melalui data numerik.

Pada konteks audit IT, penggunaan analisis teks juga dapat membantu mengidentifikasi pola-pola tersembunyi dalam komunikasi yang mungkin menunjukkan pelanggaran kebijakan atau perilaku yang tidak sah. Dengan memanfaatkan algoritma pemrosesan bahasa alami (NLP), auditor dapat menganalisis ribuan dokumen atau pesan yang sebelumnya sulit untuk diproses secara manual. Teknik ini memungkinkan pengumpulan dan pemahaman informasi yang tersembunyi dalam berbagai jenis data, mulai dari email, laporan keuangan, hingga catatan percakapan antara karyawan dan pihak eksternal. Oleh karena itu, analisis teks berperan penting dalam memberikan gambaran yang lebih jelas tentang keadaan dan potensi risiko yang tidak terdeteksi dengan audit tradisional.

c. *Data Visualization* (Visualisasi Data)

Data visualization adalah salah satu alat yang sangat efektif dalam memanfaatkan big data untuk audit IT. Dengan visualisasi data, auditor dapat mengubah data yang besar dan kompleks menjadi representasi grafis yang mudah dimengerti, seperti grafik, peta panas, dan dashboard interaktif. Penggunaan visualisasi memungkinkan auditor untuk segera mengidentifikasi pola atau anomali dalam data yang mungkin tidak terlihat melalui angka atau tabel tradisional. Sebagai contoh, dashboard interaktif dapat menunjukkan transaksi mencurigakan yang menonjol atau aktivitas yang tidak biasa dalam sistem, sehingga mempercepat proses identifikasi dan analisis masalah. Visualisasi ini sangat penting dalam situasi di mana auditor harus menangani volume data yang sangat besar dalam waktu terbatas.

Visualisasi data juga membantu auditor dalam mengkomunikasikan temuannya dengan lebih efektif kepada pihak-pihak yang mungkin tidak memiliki latar belakang teknis, seperti manajer atau eksekutif perusahaan. Dengan menampilkan data dalam bentuk visual, auditor dapat mengungkapkan temuan secara lebih jelas, sehingga keputusan manajerial dapat diambil dengan lebih cepat dan tepat. Sebagai contoh, penggunaan grafik garis atau diagram batang untuk menggambarkan tren dari data yang dimiliki dapat mempermudah pemangku kepentingan untuk memahami situasi yang sedang terjadi, seperti potensi pelanggaran atau kegagalan dalam sistem keamanan IT.

B. *Blockchain* dan Transparansi dalam Sistem Keuangan

Blockchain adalah sebuah sistem buku besar terdesentralisasi yang memungkinkan pencatatan transaksi secara aman, transparan, dan tidak dapat diubah (*immutable*). Setiap transaksi yang terjadi dicatat dalam sebuah blok, yang kemudian dihubungkan ke blok sebelumnya dalam sebuah rantai (*chain*). Proses ini memastikan bahwa semua data yang tercatat dalam *blockchain* bersifat permanen dan tidak dapat dimodifikasi setelah dicatat. Hal ini tercapai melalui penggunaan teknologi kriptografi yang canggih, yang melindungi data dari manipulasi. Salah satu keunggulan utama *blockchain* adalah transparansi. Setiap transaksi yang tercatat dapat dilihat oleh semua pihak yang memiliki akses ke jaringan *blockchain* tersebut. Ini

memberikan kepercayaan tambahan bagi pihak-pihak yang terlibat dalam transaksi, termasuk auditor, regulator, dan peserta transaksi lainnya.

1. *Blockchain* dalam Konteks Sistem Keuangan

Sistem keuangan global, terutama di sektor perbankan dan pembayaran, bergantung pada keamanan dan keandalan data transaksi. *Blockchain* menawarkan solusi untuk memperbaiki beberapa masalah yang sering terjadi dalam sistem keuangan tradisional, seperti biaya transaksi yang tinggi, keterlambatan dalam penyelesaian transaksi, dan risiko kecurangan.

a. Mengurangi Risiko Kecurangan dan Penyalahgunaan

Blockchain memiliki peran yang sangat penting dalam mengurangi risiko kecurangan dan penyalahgunaan dalam sistem keuangan. Salah satu aspek utama dari teknologi *blockchain* adalah prinsip desentralisasi, di mana setiap transaksi dicatat dalam sebuah buku besar yang terdistribusi dan tidak dapat dimanipulasi. Transaksi yang tercatat dalam *blockchain* menggunakan teknologi kriptografi yang kuat, sehingga setiap perubahan atau upaya manipulasi pada data yang telah tercatat akan terlihat jelas. Ini membuat *blockchain* sangat efektif dalam memitigasi risiko kecurangan yang sering terjadi dalam transaksi finansial tradisional, seperti pemalsuan dokumen atau penggelapan dana (Lewis, 2021).

Setiap transaksi yang dilakukan dalam *blockchain* memerlukan persetujuan dari jaringan pengguna yang terdistribusi, yang dikenal sebagai konsensus. Sistem konsensus ini memastikan bahwa hanya transaksi yang sah dan valid yang dapat diterima dalam jaringan, yang membuatnya hampir tidak mungkin untuk memanipulasi atau menambah transaksi palsu. Proses verifikasi yang transparan dan dapat dilacak ini memberikan lapisan keamanan tambahan yang membatasi potensi risiko yang mungkin timbul dari tindakan individu yang tidak bertanggung jawab atau pihak ketiga yang berusaha mengakses data secara ilegal.

b. Meningkatkan Efisiensi Transaksi

Blockchain dapat secara signifikan meningkatkan efisiensi transaksi dalam sistem keuangan dengan mengurangi

ketergantungan pada perantara atau pihak ketiga. Dalam sistem konvensional, transaksi keuangan, terutama transaksi internasional, sering kali melibatkan sejumlah pihak seperti bank, agen pembayaran, dan lembaga keuangan lainnya untuk memverifikasi dan memproses pembayaran. Proses ini tidak hanya memakan waktu, tetapi juga melibatkan biaya tambahan yang dapat mengurangi profitabilitas dan meningkatkan kompleksitas operasional. Dengan menggunakan *blockchain*, proses verifikasi dan penyelesaian transaksi dapat dilakukan langsung antar pihak yang terlibat tanpa perlu melalui banyak perantara, mengurangi waktu dan biaya yang terlibat secara signifikan (Lewis, 2021).

Pada konteks transaksi internasional, *blockchain* memungkinkan penyelesaian yang lebih cepat. Misalnya, dalam transaksi pengiriman uang antar negara, *blockchain* dapat mengurangi waktu yang dibutuhkan untuk memverifikasi dan menyelesaikan transaksi dari beberapa hari menjadi hanya beberapa menit. Hal ini disebabkan oleh kemampuan *blockchain* untuk menyediakan salinan transaksi yang terdesentralisasi dan dapat diverifikasi secara *real-time* oleh seluruh jaringan, sehingga menghilangkan kebutuhan akan otorisasi atau verifikasi pihak ketiga yang memakan waktu. Dengan cara ini, *blockchain* tidak hanya mempercepat proses transaksi, tetapi juga meningkatkan efisiensi alur kerja secara keseluruhan.

c. Pengurangan Biaya Operasional

Blockchain teknologi dapat secara signifikan mengurangi biaya operasional dalam sektor keuangan dengan menggantikan sistem tradisional yang memerlukan infrastruktur dan proses yang kompleks. Salah satu cara utama *blockchain* mengurangi biaya adalah dengan menghilangkan kebutuhan untuk infrastruktur fisik yang mahal, seperti server pusat data dan ruang penyimpanan yang diperlukan untuk memproses dan menyimpan transaksi. Sebaliknya, *blockchain* menggunakan jaringan desentralisasi yang didistribusikan di seluruh dunia, yang memungkinkan setiap node (atau pengguna jaringan) untuk menyimpan dan memvalidasi transaksi, mengurangi kebutuhan akan infrastruktur pusat yang mahal.

Blockchain juga mengurangi biaya terkait dengan proses verifikasi dan audit yang rumit. Dalam sistem keuangan tradisional, verifikasi transaksi sering kali memerlukan pihak ketiga yang terlibat, seperti bank atau lembaga keuangan lainnya, yang dapat memperlambat proses dan meningkatkan biaya operasional. Dengan *blockchain*, transaksi dapat diverifikasi secara otomatis oleh seluruh jaringan tanpa perlu melibatkan perantara. Teknologi seperti smart contracts dapat mengeksekusi transaksi secara otomatis ketika kondisi tertentu dipenuhi, mengurangi intervensi manual dan meningkatkan efisiensi operasional.

2. *Blockchain* dan Transparansi dalam Audit IT

Audit dalam sektor keuangan membutuhkan tingkat transparansi dan integritas data yang sangat tinggi. *Blockchain* memberikan solusi yang ideal untuk masalah ini, karena setiap transaksi yang tercatat dalam *blockchain* dapat dilacak dan diverifikasi oleh pihak yang memiliki akses ke jaringan. Ini menciptakan sistem yang sangat transparan dan mudah diaudit.

a. Pencatatan dan Verifikasi Transaksi

Blockchain teknologi membawa perubahan signifikan dalam proses audit dengan menyediakan pencatatan dan verifikasi transaksi yang lebih transparan dan aman. Setiap transaksi yang dilakukan dalam sistem *blockchain* tercatat dalam bentuk blok yang terhubung secara berurutan dan tersebar di seluruh jaringan. Setiap blok berisi informasi transaksi yang tidak dapat diubah setelah tercatat, menjamin integritas data tersebut. Dalam konteks audit, hal ini memberikan keuntungan besar, karena auditor dapat mengakses dan memverifikasi data transaksi secara *real-time*. Dengan cara ini, *blockchain* memungkinkan auditor untuk memantau transaksi secara langsung tanpa harus menunggu proses verifikasi atau rekonsiliasi manual yang biasanya memakan waktu lama (Badev & Chen, 2014).

Blockchain memberikan transparansi yang lebih tinggi dibandingkan dengan sistem konvensional. Setiap transaksi yang tercatat dalam *blockchain* dapat diakses oleh pihak yang berwenang, seperti auditor, tanpa perlu melibatkan perantara. Ini meminimalisir kemungkinan adanya manipulasi atau

pengubahan data, karena *blockchain* bersifat immutable (tidak dapat diubah). Fitur ini sangat penting dalam menjaga keakuratan dan keabsahan data yang digunakan dalam audit. Sebagai hasilnya, auditor dapat mengandalkan *blockchain* untuk memastikan bahwa transaksi yang tercatat memang sesuai dengan catatan keuangan yang ada, sesuai dengan standar akuntansi dan regulasi yang berlaku.

b. Pemantauan *Real-time*

Pemantauan *real-time* adalah salah satu manfaat utama yang ditawarkan oleh *blockchain* dalam konteks audit IT. Dalam sistem audit tradisional, auditor sering kali menghadapi keterlambatan dalam memperoleh data untuk memverifikasi transaksi, yang dapat menyebabkan waktu audit yang lebih lama dan meningkatkan risiko ketidakakuratan. Dengan *blockchain*, setiap transaksi yang dilakukan langsung tercatat dalam jaringan yang dapat diakses secara *real-time* oleh auditor. Hal ini memungkinkan auditor untuk langsung melihat dan memverifikasi transaksi yang terjadi tanpa harus menunggu laporan atau rekonsiliasi manual, sehingga meningkatkan efisiensi dan kecepatan proses audit (Buterin, 2014).

Keuntungan lainnya adalah kemampuan *blockchain* untuk memberikan visibilitas penuh terhadap seluruh transaksi yang terjadi, yang dapat langsung dipantau oleh auditor. Ini mengurangi ketergantungan pada pihak ketiga atau pengumpulan data historis yang biasanya memerlukan waktu. Dengan informasi yang lebih cepat dan akurat, auditor dapat segera mengidentifikasi masalah atau anomali dalam transaksi yang mungkin menunjukkan adanya kecurangan atau kesalahan. Pemantauan transaksi secara *real-time* ini memungkinkan auditor untuk melakukan tindakan preventif lebih awal, yang dapat mengurangi potensi kerugian dan melindungi integritas sistem keuangan.

c. Pengurangan Risiko Human Error

Pengurangan risiko human error adalah salah satu keuntungan utama yang ditawarkan oleh teknologi *blockchain* dalam audit IT. Dalam sistem audit tradisional, banyak pihak yang terlibat dalam verifikasi transaksi, seperti akuntan, auditor, dan manajer, yang semuanya mengandalkan input manual untuk

memeriksa dan mencocokkan data. Proses ini memerlukan ketelitian tinggi, dan setiap langkah manual berpotensi meningkatkan kemungkinan kesalahan manusia. Namun, dengan *blockchain*, sebagian besar proses manual ini dapat diotomatisasi. Setiap transaksi yang dicatat dalam *blockchain* dilakukan oleh algoritma yang terverifikasi, mengurangi ketergantungan pada intervensi manusia dalam pencatatan dan verifikasi transaksi, sehingga meminimalkan kemungkinan kesalahan yang dapat memengaruhi hasil audit.

Blockchain memastikan bahwa data yang tercatat bersifat immutable (tidak dapat diubah) dan transparan. Setiap transaksi yang terverifikasi dicatat secara permanen dalam blok dan tidak dapat dimanipulasi atau diubah tanpa persetujuan seluruh jaringan. Ini mengurangi risiko bahwa data yang diperoleh auditor dapat terkontaminasi atau dimanipulasi oleh kesalahan manusia yang tidak disengaja. Dengan begitu, auditor dapat merasa lebih yakin bahwa data yang dianalisis adalah akurat dan terpercaya, karena tahu bahwa setiap transaksi telah tercatat dengan benar sejak awal.

C. *Artificial Intelligence* dan *Machine Learning* untuk Audit

Pada era digital yang terus berkembang, teknologi seperti *Artificial Intelligence* (AI) dan *Machine Learning* (ML) semakin banyak diterapkan dalam berbagai bidang, termasuk di dalam proses audit IT. Kedua teknologi ini memungkinkan auditor untuk memperoleh wawasan yang lebih mendalam dan akurat dengan cara yang lebih efisien dan efektif dibandingkan dengan metode audit tradisional. *Artificial Intelligence* (AI) mengacu pada kemampuan mesin untuk melakukan tugas-tugas yang biasanya memerlukan kecerdasan manusia, seperti pengambilan keputusan, analisis data, dan pemecahan masalah. Dalam konteks audit IT, AI berperan dalam menganalisis data besar, menemukan pola-pola tertentu, dan memberikan rekomendasi berbasis data yang lebih akurat untuk auditor. *Machine Learning* adalah cabang dari AI yang memungkinkan sistem untuk "belajar" dari data tanpa diprogram secara eksplisit. ML menggunakan algoritma untuk mengenali pola dalam data dan kemudian menggunakan pola tersebut untuk membuat prediksi atau keputusan. Dalam audit IT, ML dapat

digunakan untuk menganalisis riwayat data audit, mendeteksi anomali, dan memprediksi potensi risiko.

1. Aplikasi AI dan ML dalam Audit IT

a. Automasi Proses Audit

Automasi proses audit dengan menggunakan AI dan ML membawa efisiensi yang signifikan dalam dunia audit IT. AI dapat digunakan untuk mengotomatiskan tugas-tugas repetitif yang memakan waktu, seperti pembuatan skrip untuk pengujian data atau pemeriksaan transaksi. Hal ini mengurangi beban kerja manual auditor, yang memungkinkan untuk fokus pada analisis yang lebih kompleks dan berfokus pada deteksi anomali atau pola yang lebih rumit dalam data. Sebagai contoh, AI dapat digunakan untuk menilai laporan keuangan dengan lebih cepat dan akurat, yang sebelumnya membutuhkan waktu yang lama jika dilakukan secara manual (Earley, 2015).

Machine learning (ML) dapat memberikan nilai tambah dalam memantau dan mengidentifikasi pola pengeluaran yang tidak biasa. Algoritma ML dapat dilatih untuk mengenali pola yang mencurigakan dalam pengeluaran organisasi, yang bisa menunjukkan adanya masalah atau potensi penipuan. Dengan terus mengumpulkan data dan menganalisisnya, sistem ini semakin cerdas dalam mendeteksi anomali yang mungkin terlewat oleh auditor manusia. Ini tidak hanya mempercepat proses audit, tetapi juga meningkatkan ketepatan temuan yang diperoleh.

b. Analisis Data Besar (*Big Data*)

Pada konteks audit IT, analisis data besar (*big data*) menjadi tantangan utama karena banyaknya volume data yang perlu dianalisis. Data ini sering kali berasal dari berbagai sumber, seperti transaksi keuangan atau data pelanggan, yang bisa mencapai terabyte atau lebih. Mengelola dan menganalisis data sebesar itu secara manual tidak hanya memakan waktu tetapi juga berisiko mengabaikan informasi penting yang dapat berpotensi mencurigakan. Dengan memanfaatkan kecerdasan buatan (AI) dan *machine learning* (ML), auditor dapat menganalisis data besar secara otomatis untuk mengidentifikasi pola-pola yang relevan dan membantu mempercepat proses audit secara

keseluruhan. AI dan ML mampu menyaring data yang tidak berguna dan memfokuskan perhatian pada area yang membutuhkan perhatian khusus, seperti transaksi yang tidak biasa atau aktivitas yang mencurigakan.

AI juga dapat meningkatkan kualitas data yang digunakan dalam proses audit dengan mendeteksi kesalahan atau inkonsistensi dalam data yang besar. Kesalahan dalam data, seperti data duplikat atau informasi yang tidak valid, sering kali menjadi hambatan dalam analisis. AI dapat mengidentifikasi kesalahan-kesalahan ini dan melakukan koreksi secara otomatis, sehingga data yang digunakan dalam audit lebih akurat dan dapat dipercaya.

c. Deteksi Penipuan dan Anomali

Pada konteks audit IT, deteksi penipuan dan anomali menggunakan kecerdasan buatan (AI) dan *machine learning* (ML) semakin menjadi alat yang esensial. Salah satu cara kerja teknologi ini adalah dengan mengidentifikasi pola perilaku yang biasa dalam data transaksi atau aktivitas pengguna. Algoritma ML dilatih untuk mengenali transaksi yang sesuai dengan pola ini, dan setiap penyimpangan yang terdeteksi dapat menandakan adanya anomali yang perlu diselidiki lebih lanjut. Misalnya, dalam audit transaksi keuangan, ML dapat mendeteksi transaksi yang lebih besar dari yang biasanya terjadi atau yang dilakukan pada waktu yang tidak wajar, serta transaksi yang dilakukan oleh akun yang tidak biasa, yang mungkin menunjukkan adanya penipuan atau kesalahan.

AI dapat meningkatkan efektivitas deteksi penipuan melalui analisis prediktif. Dengan kemampuan untuk menganalisis data dalam jumlah besar, AI dapat mengidentifikasi potensi risiko sebelum berkembang menjadi masalah yang lebih besar. Dengan cara ini, auditor tidak hanya dapat merespons kejadian yang telah terjadi, tetapi juga dapat mengambil tindakan pencegahan lebih awal, seperti memblokir transaksi mencurigakan atau memperkuat prosedur verifikasi.

2. Manfaat Penggunaan AI dan ML dalam Audit IT

a. Efisiensi dan Pengurangan Waktu

Salah satu manfaat utama penerapan AI dan ML dalam audit IT adalah peningkatan efisiensi yang signifikan. Dengan kemampuan AI untuk mengotomatiskan tugas-tugas repetitif seperti verifikasi transaksi atau pemrograman skrip pengujian, auditor dapat menghemat waktu yang sebelumnya digunakan untuk tugas manual. Misalnya, proses pemeriksaan data yang besar atau laporan transaksi yang sangat rinci, yang membutuhkan waktu lama jika dilakukan secara manual, dapat diselesaikan dalam hitungan jam dengan menggunakan teknologi ini. Dengan demikian, waktu yang dibutuhkan untuk menyelesaikan audit dapat dikurangi secara signifikan, memungkinkan auditor untuk menangani lebih banyak tugas dalam waktu yang lebih singkat.

Penggunaan *machine learning* dalam audit IT mempercepat proses analisis data besar. Dalam audit tradisional, auditor sering kali terhambat oleh volume data yang harus diperiksa, yang bisa menjadi sangat memakan waktu. ML dapat mengidentifikasi pola, anomali, atau kesalahan dengan cepat dalam kumpulan data yang besar, memberikan hasil yang lebih akurat tanpa keterlambatan. Teknologi ini memungkinkan auditor untuk menghemat waktu dalam menganalisis data dan langsung fokus pada area yang membutuhkan perhatian lebih, seperti identifikasi risiko yang lebih mendalam atau evaluasi kebijakan organisasi.

b. Peningkatan Keakuratan dan Deteksi Risiko

Penggunaan AI dan *machine learning* (ML) dalam audit IT dapat meningkatkan keakuratan audit dengan secara otomatis mengidentifikasi anomali yang mungkin terlewatkan dalam audit manual. Dalam audit tradisional, auditor manusia sering kali kesulitan untuk menangani volume data yang sangat besar, dan kesalahan atau perilaku yang tidak biasa bisa luput dari perhatian. Dengan ML, sistem dapat mempelajari pola data yang ada dan mendeteksi pola yang tidak biasa, yang mungkin menandakan adanya kesalahan atau risiko yang perlu dievaluasi lebih lanjut. Misalnya, dalam audit transaksi keuangan, ML dapat mengidentifikasi transaksi yang tidak sesuai dengan pola normal,

yang mungkin menunjukkan adanya kecurangan atau kesalahan pencatatan.

ML dapat mendeteksi anomali dalam sistem dengan cara yang lebih canggih daripada metode manual. Algoritma ML dapat mengidentifikasi hubungan yang tidak terlihat antara data, seperti transaksi yang melibatkan jumlah uang yang tidak biasa atau aktivitas yang tidak konsisten dengan profil pengguna. Ini memungkinkan auditor untuk menemukan potensi risiko lebih cepat, yang pada akhirnya meningkatkan akurasi hasil audit dan memberikan wawasan yang lebih dalam mengenai kondisi sistem yang sedang diaudit. Dengan deteksi otomatis ini, auditor dapat fokus pada area yang membutuhkan penanganan lebih lanjut, seperti investigasi terhadap potensi fraud atau kesalahan sistem.

c. Skalabilitas

Pada konteks audit IT, skalabilitas adalah salah satu keuntungan utama yang ditawarkan oleh penerapan kecerdasan buatan (AI) dan *machine learning* (ML). Organisasi besar, terutama yang memiliki banyak cabang atau operasi internasional, sering kali menghadapi tantangan besar dalam melaksanakan audit secara menyeluruh. Dengan volume data yang terus berkembang, auditor tradisional akan kesulitan mengelola dan memproses informasi tersebut dalam waktu yang wajar. Namun, AI dan ML memungkinkan auditor untuk menangani data dalam jumlah besar secara efisien. Teknologi ini dapat memproses dan menganalisis data dalam skala besar, mengurangi kebutuhan untuk menambah sumber daya manusia atau memperpanjang waktu audit.

Keunggulan skalabilitas ini sangat penting, terutama dalam audit yang melibatkan sistem atau cabang yang tersebar di berbagai lokasi. AI dan ML dapat digunakan untuk mengotomatisasi proses audit yang sebelumnya memerlukan tenaga kerja manual yang lebih banyak. Misalnya, dengan kemampuan analisis data secara *real-time*, auditor dapat segera mengidentifikasi masalah atau ketidaksesuaian di berbagai titik tanpa harus melakukan audit terpisah untuk setiap lokasi. Sistem yang dibangun dengan AI dan ML mampu memproses data dengan kecepatan dan ketepatan yang jauh melebihi kapasitas manusia, memfasilitasi audit yang lebih efisien pada skala besar.

D. Alat dan Platform Audit IT (CAATs, ACL, IDEA)

Pada dunia audit teknologi informasi (TI), penggunaan alat dan platform yang tepat sangat penting untuk meningkatkan efisiensi, akurasi, dan keandalan proses audit. Alat Audit Berbantuan Komputer (*Computer-Assisted Audit Tools*, CAATs) merupakan salah satu teknologi yang banyak digunakan oleh auditor untuk melakukan analisis data yang lebih mendalam dan mengidentifikasi risiko atau ketidaksesuaian dalam sistem informasi. CAATs mencakup berbagai perangkat lunak dan teknik yang memungkinkan auditor untuk mengakses, menganalisis, dan memverifikasi data secara lebih efektif daripada metode audit manual. Di antara berbagai alat CAATs yang tersedia, dua platform yang sangat populer adalah ACL (*Audit Command Language*) dan IDEA (*Interactive Data Extraction and Analysis*). Kedua platform ini digunakan oleh banyak auditor di seluruh dunia untuk melakukan audit data yang lebih efisien dan terperinci.

1. CAATs dalam Audit TI

Computer-Assisted Audit Tools (CAATs) merujuk pada perangkat atau aplikasi berbasis komputer yang digunakan oleh auditor untuk mendukung dan meningkatkan proses audit. CAATs memanfaatkan teknologi informasi untuk memproses data secara otomatis, memungkinkan auditor untuk melakukan analisis yang lebih cepat dan lebih akurat daripada metode audit manual. CAATs dapat digunakan dalam berbagai bentuk, termasuk perangkat lunak analisis data, aplikasi pemrograman, dan alat verifikasi transaksi.

a. Pengumpulan dan Ekstraksi Data

   Computer-Assisted Audit Techniques (CAATs) memungkinkan auditor untuk mengakses dan mengumpulkan data dari berbagai sistem informasi yang digunakan dalam suatu organisasi, baik yang terstruktur maupun tidak terstruktur. Dalam audit TI, data terstruktur biasanya berupa informasi yang tersimpan dalam basis data relasional, sementara data tidak terstruktur mencakup dokumen, email, atau file multimedia. Dengan menggunakan CAATs, auditor dapat memperoleh akses langsung ke berbagai jenis data yang mungkin sebelumnya sulit atau memakan waktu untuk diperoleh secara manual.

Proses pengumpulan dan ekstraksi data menggunakan CAATs sangat efisien karena alat ini memungkinkan auditor untuk mengambil data dalam jumlah besar dari sistem secara otomatis. CAATs mengintegrasikan berbagai metode pengumpulan data, seperti ekstraksi dari database, pemindai log transaksi, atau bahkan mengumpulkan informasi dari sistem yang lebih terisolasi. Ini mempermudah auditor untuk mengakses data yang diperlukan tanpa harus mengandalkan prosedur manual yang berisiko mempengaruhi kecepatan dan akurasi pengumpulan data. Setelah data dikumpulkan, tahap ekstraksi memungkinkan auditor untuk mengolah dan mengonversi data ke dalam format yang lebih mudah dianalisis. CAATs dapat membersihkan data dari inkonsistensi, menggabungkan informasi yang relevan, dan mengubah data yang tersebar dalam format yang berbeda menjadi satu kesatuan yang lebih terorganisir.

b. Analisis Data

Computer-Assisted Audit Techniques (CAATs) memungkinkan auditor untuk melakukan analisis data dalam jumlah besar dengan lebih efisien dan akurat. Teknologi ini dapat memproses data dari berbagai sistem dan menyajikannya dalam format yang mudah dianalisis, memungkinkan auditor untuk memeriksa konsistensi, kecocokan, dan kesalahan yang mungkin tidak terdeteksi dalam audit tradisional. Misalnya, CAATs dapat digunakan untuk menganalisis transaksi keuangan dalam sistem akuntansi dan mendeteksi pola yang tidak sesuai dengan kebijakan perusahaan atau regulasi yang berlaku. Hal ini memungkinkan auditor untuk fokus pada area yang berisiko tinggi atau rawan penipuan.

CAATs memiliki kemampuan untuk mengidentifikasi anomali dalam data, yang dapat menjadi petunjuk adanya kesalahan atau kecurangan. Dengan menggunakan teknik seperti data mining dan algoritma deteksi pola, CAATs dapat mendeteksi transaksi yang tidak biasa, transaksi ganda, atau perubahan dalam pola transaksi yang mungkin tidak terlihat dalam analisis manual. Anomali ini dapat memicu penyelidikan lebih lanjut, memberikan auditor wawasan yang lebih dalam tentang area yang membutuhkan perhatian khusus. Oleh karena

itu, CAATs meningkatkan kualitas audit dengan memastikan bahwa setiap transaksi dianalisis secara menyeluruh.

c. Verifikasi dan Validasi

Computer-Assisted Audit Techniques (CAATs) berperan penting dalam memastikan keakuratan dan kelengkapan data yang telah diproses dalam sistem informasi perusahaan. Salah satu fungsi utama CAATs adalah untuk memverifikasi apakah data yang dihasilkan dan disajikan oleh sistem sesuai dengan standar yang telah ditentukan. Auditor dapat memanfaatkan CAATs untuk membandingkan data yang ada dengan sumber referensi atau kebijakan yang berlaku untuk memastikan bahwa informasi yang diproses telah melalui langkah verifikasi yang tepat. Dengan menggunakan alat ini, auditor dapat menelusuri data dari awal hingga akhir dalam sistem untuk mengidentifikasi potensi kesalahan atau inkonsistensi yang mungkin terlewatkan dalam proses audit manual.

Pada konteks verifikasi, CAATs juga membantu dalam memastikan bahwa data yang disajikan tidak hanya akurat tetapi juga lengkap. Dengan menggunakan algoritma canggih, auditor dapat mengevaluasi apakah semua transaksi atau entri data yang relevan telah dimasukkan ke dalam sistem dengan benar. Hal ini penting karena kesalahan atau kelalaian dalam memasukkan data dapat mengarah pada kesalahan laporan keuangan yang berisiko menyesatkan keputusan manajerial atau melanggar regulasi yang berlaku. Selain itu, CAATs memungkinkan auditor untuk secara otomatis melakukan pencocokan data untuk memastikan bahwa informasi yang disajikan sesuai dengan sumber yang terpercaya, mengurangi potensi kesalahan manusia dalam proses audit.

d. Penyusunan Laporan

Computer-Assisted Audit Techniques (CAATs) dapat meningkatkan efisiensi dalam penyusunan laporan audit dengan menyediakan data yang lebih akurat dan dapat dipertanggungjawabkan. Hasil audit yang dihasilkan oleh CAATs mempermudah auditor dalam menyusun laporan karena data yang diperoleh sudah terstruktur dan terverifikasi dengan baik. Proses otomatisasi yang dilakukan oleh CAATs memungkinkan auditor untuk menghemat waktu dan sumber daya dalam menyusun laporan yang mencakup hasil temuan,

rekomendasi, dan kesimpulan yang lebih tepat. Laporan audit ini kemudian dapat digunakan sebagai dasar untuk pengambilan keputusan oleh manajer atau pihak lain yang berkepentingan.

CAATs membantu dalam memastikan bahwa laporan audit mencerminkan dengan tepat hasil analisis data yang telah dilakukan. Dengan kemampuan untuk memproses dan menganalisis data dalam jumlah besar, CAATs memudahkan auditor untuk menyajikan informasi yang relevan dan terperinci dalam laporan. Hal ini juga memastikan bahwa laporan audit mencakup semua informasi yang diperlukan tanpa adanya data yang terlewat atau tidak tercatat, yang sering kali terjadi dalam audit tradisional. CAATs memungkinkan auditor untuk menyajikan temuan dalam format yang lebih terstruktur dan lebih mudah dipahami oleh pembaca laporan.

2. ACL (*Audit Command Language*)

ACL adalah salah satu alat audit berbantuan komputer yang paling populer dan digunakan secara luas di seluruh dunia. Platform ini dirancang untuk membantu auditor mengakses, memproses, dan menganalisis data keuangan serta operasional perusahaan. ACL memungkinkan auditor untuk melakukan analisis data secara menyeluruh, termasuk pemrograman kueri yang kompleks dan analisis statistika.

a. Ekstraksi dan Pengolahan Data

Audit Command Language (ACL) adalah alat yang sangat efektif dalam ekstraksi dan pengolahan data dalam audit TI. Dengan ACL, auditor dapat menarik data dari berbagai sistem sumber, termasuk *Enterprise Resource Planning* (ERP) sistem, database relasional, dan file spreadsheet. Kemampuannya untuk mengakses data dari berbagai sumber yang berbeda memberikan auditor fleksibilitas dalam menyesuaikan pendekatan audit. ACL memungkinkan auditor untuk mengekstrak data dalam format yang mudah dianalisis, mengurangi ketergantungan pada pengumpulan data manual yang memakan waktu dan rawan kesalahan (Otero, 2020).

Setelah data diekstrak, ACL dapat digunakan untuk membersihkan dan memproses informasi tersebut untuk analisis lebih lanjut. Proses ini mencakup penghapusan duplikasi,

konversi format data, serta penggabungan dan pencocokan informasi dari berbagai sumber. Dengan menggunakan ACL, auditor dapat secara otomatis mengidentifikasi pola, kesalahan, atau anomali dalam data, yang membuatnya lebih mudah untuk mengevaluasi kepatuhan dan integritas informasi. Pengolahan data ini tidak hanya meningkatkan efisiensi tetapi juga mengurangi risiko kesalahan manusia yang terjadi dalam proses audit tradisional.

b. Pemrograman Audit

Audit Command Language (ACL) menawarkan fitur pemrograman yang sangat berguna bagi auditor untuk mengotomatisasi berbagai tugas audit yang berulang. Dengan kemampuan pemrograman, auditor dapat merancang dan menjalankan query otomatis untuk mencari anomali atau pola yang mencurigakan dalam data. Misalnya, auditor dapat membuat skrip untuk memeriksa apakah transaksi melebihi batas tertentu atau apakah ada transaksi yang tidak sesuai dengan kebijakan perusahaan. Kemampuan ini sangat penting untuk meningkatkan efisiensi audit, karena dapat mengurangi beban kerja manual dan mempercepat proses audit secara keseluruhan.

Pemrograman dalam ACL memungkinkan auditor untuk menyesuaikan analisis sesuai dengan kebutuhan spesifik dari audit yang sedang dilakukan. Dengan menulis query khusus, auditor dapat menggali lebih dalam ke dalam data untuk mencari indikasi penipuan, kesalahan, atau ketidaksesuaian dengan standar yang ditetapkan. Contohnya, auditor dapat membuat kode untuk secara otomatis mencari transaksi dengan pola tertentu atau untuk memverifikasi kesesuaian data antara berbagai sistem atau sumber informasi.

c. Visualisasi Data

Audit Command Language (ACL) menyediakan alat visualisasi yang memungkinkan auditor untuk menyajikan data yang telah dianalisis dalam bentuk grafik atau diagram. Visualisasi ini sangat berguna untuk memudahkan pemahaman hasil audit, terutama ketika berhadapan dengan data yang besar dan kompleks. Dengan menggunakan diagram batang, grafik garis, atau diagram lingkaran, auditor dapat dengan cepat mengidentifikasi tren, pola, atau anomali dalam data yang

mungkin tidak terlihat jelas dalam laporan teks biasa. Hal ini memungkinkan auditor untuk menyampaikan temuan audit dengan cara yang lebih intuitif dan mudah dipahami oleh berbagai pemangku kepentingan, termasuk manajemen atau klien.

Visualisasi dalam ACL mendukung auditor dalam membahas data secara interaktif. Auditor dapat memilih berbagai jenis grafik atau menyesuaikan tampilan data untuk menggali lebih dalam pada area tertentu yang memerlukan perhatian lebih. Sebagai contoh, dengan menggunakan diagram korelasi, auditor dapat melihat hubungan antara berbagai variabel dalam data, seperti antara transaksi yang tidak biasa dan waktu atau jenis akun yang digunakan. Hal ini memberikan wawasan yang lebih mendalam dan membantu auditor untuk membuat keputusan yang lebih baik dalam merumuskan temuan dan rekomendasi audit.

d. Keamanan dan Kepatuhan

Audit Command Language (ACL) memiliki berbagai fitur keamanan yang dirancang untuk memastikan bahwa data yang dianalisis tetap terlindungi dari akses yang tidak sah. Dalam lingkungan audit yang sering kali melibatkan data sensitif, ACL menyediakan kontrol akses berbasis peran yang memungkinkan organisasi untuk menetapkan siapa yang dapat mengakses data dan menjalankan analisis. Fitur ini mengurangi risiko kebocoran data dan memastikan bahwa hanya pihak yang berwenang yang dapat mengakses informasi yang relevan untuk audit. ACL juga menyediakan enkripsi untuk memastikan data tetap aman baik saat disimpan maupun saat dipindahkan, memberikan perlindungan ekstra terhadap ancaman eksternal yang mungkin terjadi selama proses audit.

ACL memastikan bahwa audit dilakukan sesuai dengan standar dan regulasi yang berlaku. Dengan fungsionalitas yang memungkinkan auditor untuk memverifikasi kepatuhan terhadap berbagai regulasi, ACL mendukung auditor dalam mengidentifikasi dan mendokumentasikan kepatuhan terhadap kebijakan internal perusahaan maupun peraturan eksternal seperti yang ditetapkan oleh otoritas regulasi. Fitur audit trail dalam ACL memastikan bahwa setiap langkah yang diambil

selama audit tercatat secara rinci, yang tidak hanya penting untuk transparansi tetapi juga untuk keperluan pelaporan dan review oleh pihak yang berwenang. Hal ini meningkatkan tingkat kepercayaan dalam hasil audit yang dilaksanakan dan membantu dalam mematuhi persyaratan hukum dan etika yang ketat.

3. IDEA (*Interactive Data Extraction and Analysis*)

IDEA adalah platform lain yang digunakan dalam audit TI yang menawarkan fungsionalitas serupa dengan ACL, tetapi dengan fitur tambahan yang lebih mendalam untuk analisis data. IDEA dirancang untuk menganalisis data dalam jumlah besar secara interaktif dan mendalam, memungkinkan auditor untuk menggali lebih dalam untuk menemukan ketidaksesuaian atau potensi penipuan dalam data.

a. Ekstraksi dan Pemrosesan Data

IDEA (*Interactive Data Extraction and Analysis*) adalah alat yang sangat berguna dalam dunia audit karena kemampuannya untuk mengekstraksi data dari berbagai sumber yang berbeda, termasuk database tradisional, sistem transaksi yang berbasis aplikasi, dan platform berbasis *cloud*. Dalam audit, data biasanya tersebar di berbagai sistem yang menggunakan format berbeda-beda. IDEA memungkinkan auditor untuk mengakses data ini secara efisien, mengimpor berbagai jenis data dalam format yang sesuai, dan menyatukannya untuk analisis lebih lanjut. Ini menghemat waktu dan tenaga, serta meningkatkan akurasi dalam proses audit.

Proses ekstraksi data dalam IDEA didukung oleh berbagai metode yang dapat disesuaikan, seperti filter dinamis, pemrograman otomatis, dan integrasi dengan berbagai database dan sumber daya yang ada. Auditor dapat memilih data yang relevan dengan cepat, baik itu data yang sudah ada dalam sistem ERP, aplikasi berbasis *cloud*, maupun sistem transaksi lain yang tidak terstruktur. Hal ini memungkinkan auditor untuk mendapatkan gambaran menyeluruh mengenai keadaan data dalam organisasi tanpa memerlukan banyak waktu untuk pengolahan manual. Dengan kemampuan untuk menangani berbagai jenis sumber data, IDEA memfasilitasi auditor untuk bekerja dengan lebih efektif dan efisien.

b. Analisis Statistik dan Pencarian Pola

IDEA (*Interactive Data Extraction and Analysis*) memberikan auditor berbagai alat analisis statistik yang sangat berguna untuk menggali informasi tersembunyi dalam data dan mengidentifikasi pola yang tidak biasa. Dengan menggunakan teknik statistik, auditor dapat melakukan analisis distribusi, korelasi, dan regresi untuk memahami hubungan antar variabel dalam data yang diperiksa. Alat ini memungkinkan auditor untuk membahas data lebih dalam dan menemukan informasi yang tidak bisa terlihat hanya dengan melihat data mentah secara manual. Analisis statistik ini meningkatkan ketajaman audit dengan membahas potensi masalah yang memerlukan perhatian lebih lanjut.

IDEA dilengkapi dengan teknik pencarian pola yang membantu auditor mengidentifikasi tren yang tidak biasa atau anomali dalam data yang besar dan kompleks. Teknik ini dapat mendeteksi pola transaksi yang mencurigakan, seperti pengeluaran yang tidak konsisten dengan pola sebelumnya, atau pola perilaku yang menunjukkan adanya potensi penipuan. Pencarian pola ini sangat berharga dalam audit karena dapat mengungkapkan masalah yang tidak terdeteksi dalam pemeriksaan biasa, serta memberi wawasan yang lebih mendalam mengenai potensi risiko yang dihadapi perusahaan. Dengan demikian, auditor bisa melakukan pemeriksaan yang lebih cermat terhadap transaksi atau data yang mencurigakan.

c. Pemrograman Audit yang Kuat

IDEA (*Interactive Data Extraction and Analysis*) menyediakan kemampuan pemrograman audit yang sangat kuat, memungkinkan auditor untuk menulis skrip audit yang lebih kompleks dan disesuaikan dengan kebutuhan spesifik audit. Dengan fitur pemrograman ini, auditor dapat membuat query atau skrip untuk mengekstraksi, memfilter, dan menganalisis data dalam jumlah besar sesuai dengan parameter yang ditentukan. Ini memungkinkan auditor untuk memeriksa data secara lebih rinci dan mendalam daripada jika hanya bergantung pada fungsi dasar perangkat lunak. Dengan kemampuan ini, IDEA menawarkan fleksibilitas lebih tinggi dalam menangani berbagai jenis audit, baik itu audit keuangan, operasional, maupun kepatuhan.

Skrip audit yang ditulis dalam IDEA memungkinkan auditor untuk menangani data yang lebih kompleks dan variabel dengan cara yang lebih efisien. Misalnya, auditor dapat menulis skrip untuk mencari pola tertentu dalam transaksi, mengidentifikasi ketidaksesuaian atau anomali dalam data, dan mendeteksi potensi penipuan. Hal ini mengurangi ketergantungan pada proses manual yang memakan waktu dan meningkatkan akurasi analisis. Dengan memberikan auditor kontrol lebih besar atas proses audit, pemrograman dalam IDEA juga memungkinkan personalisasi audit yang lebih tinggi, berdasarkan kebutuhan klien atau tujuan spesifik audit yang dilakukan.

d. Laporan dan Visualisasi

IDEA (*Interactive Data Extraction and Analysis*) memfasilitasi pembuatan laporan audit yang lebih efisien dan visualisasi data yang mudah dipahami. Fitur ini memungkinkan auditor untuk menyajikan hasil audit dalam format yang jelas dan terstruktur, mempercepat proses pengambilan keputusan oleh pemangku kepentingan. Dengan kemampuan untuk membuat laporan terperinci, IDEA memungkinkan auditor untuk menggambarkan temuan-temuannya dengan cara yang lebih terorganisir, mempermudah manajemen atau pihak terkait lainnya dalam menilai temuan dan meresponsnya dengan cepat. Laporan yang dihasilkan mencakup semua data relevan, kesimpulan, serta rekomendasi untuk perbaikan, yang membuat proses audit lebih transparan dan akuntabel.

IDEA juga menyediakan alat visualisasi data yang powerful, seperti grafik, diagram, dan peta panas (*heat maps*), yang memungkinkan auditor untuk mempresentasikan data dengan cara yang lebih intuitif. Visualisasi ini sangat berguna untuk menunjukkan pola atau anomali yang mungkin sulit dilihat dalam laporan teks tradisional. Penggunaan grafik atau diagram yang jelas memungkinkan pemangku kepentingan untuk cepat mengidentifikasi area yang membutuhkan perhatian lebih lanjut, tanpa harus menganalisis angka-angka mentah secara langsung.

E. *Cloud Computing* dalam Sistem Keuangan dan Audit

Cloud computing adalah model penyediaan layanan IT yang memungkinkan pengguna untuk mengakses aplikasi, server, penyimpanan, dan berbagai layanan lainnya melalui internet. Dalam konteks audit TI, *cloud computing* memungkinkan auditor untuk mengakses data secara *real-time* dan menganalisisnya dengan cepat, serta mengurangi kebutuhan akan infrastruktur IT yang mahal di perusahaan.

1. *Cloud Computing* dalam Sistem Keuangan

Pada sektor keuangan, *cloud computing* memungkinkan perusahaan untuk mengoptimalkan proses-proses keuangan, seperti pengelolaan data transaksi, perhitungan pajak, dan pelaporan keuangan. Layanan *cloud* memungkinkan organisasi untuk mengelola volume besar data finansial dengan lebih efisien, dengan biaya yang lebih rendah, serta kemampuan untuk memproses data dalam waktu nyata. Beberapa contoh penerapan *cloud computing* dalam sistem keuangan adalah sebagai berikut:

a. Sistem ERP Berbasis *Cloud*

Sistem *Enterprise Resource Planning* (ERP) berbasis *cloud* telah menjadi solusi yang sangat populer bagi perusahaan yang ingin mengelola berbagai fungsi bisnis secara terintegrasi, termasuk keuangan, inventaris, penggajian, dan pelaporan keuangan. Dengan menggunakan sistem ERP berbasis *cloud*, perusahaan dapat mengakses data secara *real-time* dari mana saja, selama ada koneksi internet, yang memberikan fleksibilitas dan efisiensi yang lebih besar dibandingkan dengan sistem tradisional yang berbasis server lokal. Hal ini juga memungkinkan perusahaan untuk lebih cepat merespons perubahan yang terjadi di pasar atau dalam operasional internal (Manvi & Shyam, 2021).

Salah satu keuntungan utama dari sistem ERP berbasis *cloud* adalah pengurangan biaya yang signifikan terkait dengan pengelolaan perangkat keras dan infrastruktur TI. Perusahaan tidak lagi perlu menginvestasikan dana yang besar untuk membeli, memelihara, dan memperbarui perangkat keras atau perangkat lunak di dalam ruangan. Sebaliknya, dapat

berlangganan layanan *cloud* yang dikelola oleh penyedia layanan yang memiliki keahlian dalam pengelolaan sistem besar. Hal ini tidak hanya mengurangi biaya awal, tetapi juga mengurangi biaya operasional dalam jangka panjang.

b. Penyimpanan Data Keuangan

Cloud computing menawarkan solusi penyimpanan data keuangan yang lebih aman, efisien, dan terpusat. Dengan memanfaatkan teknologi ini, perusahaan dapat menyimpan data transaksi keuangan, termasuk informasi sensitif seperti laporan keuangan dan catatan audit, di server *cloud* yang dikelola oleh penyedia layanan terkemuka. Data yang disimpan di *cloud* ini dilindungi oleh sistem keamanan tingkat tinggi, termasuk enkripsi dan kontrol akses yang ketat.

Penyimpanan data keuangan di *cloud* juga mempermudah proses audit. Karena data terpusat di satu tempat, auditor dapat mengakses dan meninjau informasi dengan lebih mudah, tanpa perlu mengumpulkan data dari berbagai sistem atau departemen yang terpisah. Akses yang lebih cepat dan mudah ini mempercepat proses audit dan memungkinkan identifikasi masalah lebih cepat. Selain itu, dengan catatan digital yang tersimpan dengan rapi dan terorganisir, auditor dapat melacak jejak transaksi dengan lebih efisien, yang meningkatkan transparansi dan akurasi laporan keuangan.

c. Layanan Akuntansi Berbasis *Cloud*

Layanan akuntansi berbasis *cloud*, seperti QuickBooks Online atau Xero, telah merubah cara perusahaan kecil dan menengah mengelola pembukuan. Dengan memanfaatkan *cloud computing*, perusahaan dapat mengakses data keuangan dari mana saja dan kapan saja, tanpa memerlukan perangkat keras khusus atau infrastruktur IT yang mahal. Layanan ini memungkinkan pengguna untuk mencatat transaksi, mengelola buku besar, dan menghasilkan laporan keuangan secara otomatis, yang meningkatkan efisiensi operasional dan mengurangi kemungkinan kesalahan manusia.

Salah satu keunggulan utama dari layanan akuntansi berbasis *cloud* adalah kemampuannya untuk memudahkan kolaborasi antar tim atau dengan konsultan eksternal. Pengguna dapat memberikan akses *real-time* kepada akuntan atau manajer

keuangan tanpa harus mengirim file atau mengelola versi dokumen yang berbeda. Selain itu, pembaruan perangkat lunak otomatis dari penyedia layanan *cloud* memastikan bahwa perusahaan selalu menggunakan versi terbaru dengan fitur dan pembaruan keamanan yang terjamin.

2. Manfaat *Cloud Computing* dalam Audit

Penerapan *cloud computing* dalam audit TI memberikan sejumlah manfaat penting bagi auditor dan organisasi yang diaudit, antara lain:

a. Aksesibilitas dan Kolaborasi yang Lebih Baik

Cloud computing telah membawa revolusi dalam proses audit, terutama dengan meningkatkan aksesibilitas dan kolaborasi. Auditor kini dapat mengakses data keuangan dan operasional secara remote tanpa terikat pada lokasi geografis tertentu. Hal ini memungkinkan audit berlangsung lebih fleksibel dan efisien, terutama dalam situasi di mana auditor perlu bekerja dari jarak jauh atau ketika perusahaan memiliki beberapa cabang di berbagai lokasi. Dengan akses berbasis *cloud*, data dapat diperoleh secara *real-time*, mempercepat proses audit dan memungkinkan auditor untuk fokus pada analisis kritis dan pengambilan keputusan strategis (Moghadasi *et al*., 2018).

Kemampuan *cloud* untuk mendukung kolaborasi lintas tim juga menjadi manfaat utama. Dengan platform berbasis *cloud*, auditor dari berbagai lokasi dapat bekerja pada dataset yang sama secara bersamaan, tanpa perlu khawatir tentang pengelolaan versi dokumen atau keterlambatan pengiriman file. Fitur kolaborasi ini memungkinkan komunikasi yang lebih baik antara auditor internal, eksternal, dan pihak manajemen, sehingga memastikan bahwa hasil audit lebih transparan dan dapat dipertanggungjawabkan. Tools *cloud* juga sering kali menyediakan fitur catatan dan pelacakan perubahan, memudahkan koordinasi di antara tim audit.

b. Efisiensi Biaya dan Waktu

Cloud computing menawarkan efisiensi biaya dan waktu yang signifikan dalam proses audit, terutama dengan menghilangkan kebutuhan infrastruktur fisik yang mahal. Dengan data dan aplikasi yang disimpan di *cloud*, perusahaan

tidak perlu lagi menginvestasikan dana besar untuk membeli, memelihara, dan memperbarui server atau perangkat keras khusus. Sebagai gantinya, biaya dialihkan ke model langganan berbasis kebutuhan, yang fleksibel dan dapat disesuaikan dengan skala organisasi.

Penggunaan *cloud* juga mempercepat proses audit dengan menyediakan akses *real-time* ke data dan alat analisis yang dibutuhkan auditor. Dalam sistem tradisional, proses audit seringkali terhambat oleh waktu yang diperlukan untuk mengumpulkan data dari berbagai lokasi atau mengintegrasikan informasi dari berbagai sumber. Dengan *cloud*, data terpusat dalam satu platform yang dapat diakses kapan saja dan dari mana saja, memungkinkan auditor untuk memulai dan menyelesaikan audit dengan lebih cepat. Waktu yang dihemat ini dapat dialokasikan untuk aktivitas strategis seperti pengembangan rekomendasi perbaikan.

c. Pengolahan Data yang Cepat dan *Real-time*

Cloud computing memfasilitasi pengolahan data keuangan secara cepat dan *real-time*, yang memberikan keunggulan signifikan dalam proses audit. Dengan teknologi ini, data dapat diproses langsung di server *cloud* tanpa memerlukan transfer manual atau pengunduhan. Auditor dapat mengakses dan menganalisis transaksi yang sedang berlangsung secara instan, mengurangi waktu tunggu yang biasanya diperlukan dalam sistem tradisional. Kecepatan ini memungkinkan auditor untuk mengidentifikasi masalah lebih awal dan memberikan rekomendasi yang relevan dengan situasi terkini.

Kemampuan *real-time* juga memungkinkan auditor untuk memonitor perubahan data atau aktivitas keuangan secara langsung. Dalam audit konvensional, ada jeda waktu antara pengumpulan data dan pelaporan hasil analisis, yang dapat mengurangi efektivitas audit, terutama dalam situasi dinamis. Dengan *cloud computing*, data yang diperbarui segera tersedia, memungkinkan auditor untuk beradaptasi dengan perubahan dan memberikan respons cepat terhadap risiko atau anomali yang terdeteksi.

BAB VIII
PRAKTIK TERBAIK DALAM AUDIT IT KEUANGAN

Pada audit IT keuangan, praktik terbaik sangat penting untuk memastikan bahwa sistem informasi dan teknologi yang mendukung fungsi keuangan perusahaan dapat memberikan hasil yang akurat, terpercaya, dan sesuai dengan regulasi yang berlaku. Praktik terbaik ini mencakup pemilihan kerangka kerja audit yang tepat, seperti COBIT, ISO 27001, dan NIST, yang membantu auditor untuk mengevaluasi kontrol IT secara komprehensif dan sistematis. Selain itu, teknologi terkini seperti big data, kecerdasan buatan (AI), dan *blockchain* semakin berperan penting dalam meningkatkan efektivitas audit IT, dengan memberikan wawasan yang lebih dalam serta kemampuan analisis yang lebih canggih.

Praktik terbaik dalam audit IT juga mencakup pendekatan berbasis risiko yang lebih adaptif, yang memungkinkan auditor untuk menilai dan memitigasi ancaman terkait data dan sistem IT yang digunakan dalam keuangan. Ini termasuk identifikasi dan pengendalian risiko terkait dengan keamanan siber, kepatuhan terhadap regulasi, serta potensi kerusakan operasional yang dapat memengaruhi integritas data keuangan. Auditor yang memiliki pemahaman yang baik mengenai risiko yang timbul dari sistem teknologi dan cara terbaik untuk mengelola tantangan ini akan lebih efektif dalam memberikan jaminan atas keandalan dan keberlanjutan operasional.

A. Audit Berbasis Risiko (*Risk-Based Audit*)

Audit berbasis risiko adalah pendekatan yang berfokus pada identifikasi, penilaian, dan pengelolaan risiko yang terkait dengan laporan keuangan dan sistem informasi perusahaan. Dalam pendekatan

ini, auditor tidak hanya berfokus pada jumlah sampel atau area yang luas, tetapi lebih pada potensi risiko yang ada pada area tertentu. Hal ini memungkinkan auditor untuk melakukan pemeriksaan yang lebih mendalam pada area yang dianggap paling berisiko, baik dari segi finansial maupun operasional. Pendekatan ini mengharuskan auditor untuk mengevaluasi dan mengidentifikasi risiko dalam beberapa kategori, termasuk risiko keuangan, operasional, reputasi, dan kepatuhan. Proses ini dimulai dengan melakukan penilaian risiko yang menyeluruh terhadap perusahaan dan sistem yang ada. Setelah itu, auditor memfokuskan upaya pada area yang memiliki tingkat risiko tertinggi, sehingga audit yang dilakukan lebih efektif dan efisien. Dalam konteks audit TI, audit berbasis risiko berperan penting dalam mengevaluasi integritas sistem informasi yang digunakan oleh perusahaan untuk mengelola data keuangan. Beberapa langkah utama dalam penerapan audit berbasis risiko dalam audit TI adalah sebagai berikut:

1. Penilaian Risiko Teknologi

Penilaian risiko teknologi dalam audit TI menjadi langkah penting dalam memastikan integritas dan keandalan sistem informasi perusahaan, terutama yang berkaitan dengan data keuangan. Sistem TI sering kali menjadi target ancaman, baik dari serangan siber maupun kesalahan operasional internal. Oleh karena itu, auditor perlu mengevaluasi risiko terkait keamanan, seperti potensi akses tidak sah atau pencurian data. Penilaian ini mencakup pemeriksaan sistem autentikasi, enkripsi, dan kebijakan keamanan lainnya untuk memastikan hanya pihak yang berwenang yang dapat mengakses informasi sensitive (Griffiths, 2016).

Ketersediaan sistem menjadi fokus utama dalam penilaian risiko. Sistem TI yang mengalami downtime atau kegagalan dapat mengganggu operasi bisnis dan mengakibatkan kerugian finansial. Auditor perlu mengevaluasi rencana pemulihan bencana dan strategi cadangan data untuk memastikan bahwa perusahaan memiliki kemampuan untuk memulihkan data dan melanjutkan operasionalnya dalam situasi darurat. Penilaian ini juga mencakup pengujian terhadap infrastruktur TI untuk menilai seberapa cepat sistem dapat kembali berfungsi setelah gangguan.

2. Analisis Risiko Keamanan Data

Analisis risiko keamanan data adalah bagian esensial dari audit berbasis risiko, terutama ketika data keuangan menjadi fokus. Sebagai informasi yang sangat sensitif, data keuangan rentan terhadap ancaman seperti peretasan, kebocoran, atau akses yang tidak sah. Oleh karena itu, auditor perlu mengevaluasi apakah perusahaan memiliki kontrol yang memadai untuk melindungi data ini. Penggunaan teknologi keamanan siber, seperti firewall, sistem deteksi intrusi, dan antivirus, menjadi langkah awal untuk mengurangi risiko ini.

Enkripsi data adalah aspek penting lain dalam menjaga kerahasiaan dan integritas data keuangan. Auditor harus memastikan bahwa perusahaan menggunakan algoritma enkripsi yang kuat untuk melindungi data yang sedang disimpan atau dikirim melalui jaringan. Enkripsi yang baik tidak hanya melindungi data dari pencurian, tetapi juga memberikan ketenangan bahwa data yang hilang atau dicuri tidak dapat dengan mudah diakses oleh pihak yang tidak berwenang. Evaluasi terhadap implementasi enkripsi termasuk melihat kebijakan pengelolaan kunci enkripsi.

3. Evaluasi Pengendalian Internal

Evaluasi pengendalian internal adalah langkah penting dalam audit untuk memastikan keandalan laporan keuangan dan efektivitas operasi perusahaan. Pengendalian internal mencakup kebijakan, prosedur, dan mekanisme yang dirancang untuk melindungi aset perusahaan, mencegah kesalahan atau kecurangan, dan memastikan bahwa data keuangan yang dihasilkan adalah akurat dan dapat dipercaya. Auditor mengevaluasi keberadaan dan penerapan kontrol ini untuk menilai apakah cukup memadai dalam mengurangi risiko signifikan (Messier Jr *et al*., 2017).

Salah satu aspek utama yang dinilai adalah prosedur untuk memastikan bahwa laporan keuangan akurat dan lengkap. Auditor mengevaluasi proses pencatatan transaksi, konsistensi dalam penerapan kebijakan akuntansi, dan mekanisme verifikasi data. Tujuannya adalah untuk memastikan bahwa informasi yang disajikan dalam laporan keuangan tidak mengandung kesalahan material yang dapat memengaruhi pengambilan keputusan pengguna laporan.

4. Penilaian Kepatuhan terhadap Regulasi

Penilaian kepatuhan terhadap regulasi adalah bagian esensial dari audit berbasis risiko, terutama di sektor keuangan yang sangat diatur. Auditor harus memastikan bahwa perusahaan telah memenuhi standar dan peraturan yang berlaku untuk mengelola, menyimpan, dan melaporkan data keuangan. Regulasi seperti *Sarbanes-Oxley Act* (SOX) di Amerika Serikat mewajibkan perusahaan publik untuk memiliki kontrol internal yang kuat, sementara peraturan seperti *General Data Protection Regulation* (GDPR) di Uni Eropa menekankan perlindungan data pribadi, termasuk data keuangan pelanggan.

Auditor mengevaluasi apakah kebijakan dan prosedur perusahaan telah dirancang untuk memenuhi regulasi tersebut. Misalnya, akan memeriksa apakah perusahaan memiliki mekanisme kontrol internal yang memadai sesuai dengan SOX atau apakah memiliki langkah-langkah untuk melindungi data pribadi sesuai GDPR. Selain itu, auditor juga menilai tingkat implementasi kebijakan ini dalam operasi sehari-hari, termasuk bagaimana perusahaan mengelola pelanggaran atau insiden yang terkait dengan regulasi.

B. Pendekatan Berkelanjutan dalam Audit IT

Pendekatan berkelanjutan dalam audit TI (*IT Sustainability Auditing*) adalah metode yang berfokus pada upaya untuk memastikan bahwa teknologi informasi dalam organisasi tidak hanya mendukung pencapaian tujuan jangka pendek, tetapi juga berkontribusi pada keberlanjutan jangka panjang dari aspek lingkungan, sosial, dan tata kelola. Konsep keberlanjutan ini sejalan dengan prinsip-prinsip bisnis berkelanjutan yang menuntut perusahaan untuk mempertimbangkan dampak sosial dan lingkungan dari keputusan, selain dari faktor finansial. Dalam audit TI, pendekatan berkelanjutan mengarah pada penerapan kebijakan, teknologi, dan praktik yang mendukung kinerja jangka panjang, sambil mempertahankan nilai-nilai etika dan mendorong efisiensi sumber daya. Oleh karena itu, audit TI yang berkelanjutan tidak hanya berfokus pada pengelolaan risiko teknologi dan informasi tetapi juga berupaya mengevaluasi dampak lingkungan dan sosial dari infrastruktur TI yang digunakan oleh organisasi.

1. Konsep dan Prinsip Pendekatan Berkelanjutan dalam Audit IT

Pendekatan berkelanjutan dalam audit TI melibatkan penilaian terhadap praktik TI yang ada dalam organisasi dari perspektif keberlanjutan. Berikut adalah beberapa prinsip dasar yang harus diperhatikan dalam audit TI berkelanjutan:

a. Kinerja Jangka Panjang dan Inovasi Berkelanjutan

Pendekatan berkelanjutan dalam audit teknologi informasi (IT) berfokus pada memastikan bahwa teknologi yang digunakan tidak hanya mendukung tujuan bisnis saat ini tetapi juga memberikan manfaat dalam jangka panjang. Salah satu prinsip kunci dalam pendekatan ini adalah mendorong kinerja jangka panjang dengan inovasi TI yang relevan. Teknologi yang diadopsi harus fleksibel dan dapat berkembang sesuai dengan perubahan kebutuhan organisasi, baik dari segi operasional maupun strategis. Dengan demikian, perusahaan dapat terus meningkatkan efisiensi dan produktivitas tanpa harus mengganti sistem secara menyeluruh (Dastbaz *et al*., 2015).

Inovasi berkelanjutan dalam TI juga mencakup penerapan teknologi ramah lingkungan dan etis. Hal ini melibatkan pengurangan konsumsi energi melalui solusi hemat daya seperti komputasi awan atau perangkat keras dengan desain berkelanjutan. Selain itu, perhatian terhadap dampak sosial, seperti memastikan perlindungan data pengguna dan kepatuhan terhadap regulasi privasi, menjadi bagian penting dari penerapan inovasi yang berkelanjutan. Dengan fokus ini, organisasi dapat menjaga keseimbangan antara kebutuhan bisnis dan tanggung jawab sosial.

b. Efisiensi Energi dan Pengelolaan Sumber Daya

Efisiensi energi dan pengelolaan sumber daya adalah pilar utama dalam pendekatan berkelanjutan pada audit teknologi informasi (TI). Audit ini bertujuan memastikan bahwa infrastruktur TI, seperti server, pusat data, dan perangkat keras lainnya, memanfaatkan energi secara efisien. Efisiensi energi dapat dicapai dengan mengadopsi teknologi hemat daya, seperti virtualisasi server dan komputasi awan, yang mengurangi jumlah perangkat fisik yang diperlukan. Auditor mengevaluasi apakah perusahaan telah menggunakan teknologi ini untuk

meminimalkan konsumsi energi yang tidak perlu, yang pada akhirnya menekan biaya operasional dan dampak lingkungan.

Pengelolaan sumber daya dalam audit TI juga mencakup analisis terhadap siklus hidup perangkat keras. Ini melibatkan penilaian terhadap proses pembelian, pemeliharaan, dan pembuangan perangkat TI untuk memastikan bahwa seluruh siklus dilakukan dengan cara yang ramah lingkungan. Misalnya, auditor menilai apakah perangkat keras yang usang telah didaur ulang dengan benar atau digantikan oleh perangkat yang lebih hemat energi. Penggunaan perangkat dengan efisiensi daya yang tinggi tidak hanya mengurangi jejak karbon organisasi tetapi juga membantu meningkatkan keberlanjutan operasional.

c. Keamanan dan Perlindungan Data

Keamanan dan perlindungan data merupakan aspek krusial dalam audit TI berkelanjutan, terutama karena meningkatnya jumlah data yang dikelola oleh organisasi. Dalam pendekatan berkelanjutan, audit ini berfokus pada perlindungan informasi sensitif yang disimpan dan diproses oleh sistem TI, dengan memastikan bahwa langkah-langkah keamanan yang tepat diimplementasikan untuk mencegah kebocoran atau peretasan data. Aspek ini mencakup penggunaan enkripsi data, pengendalian akses, serta sistem pemantauan yang dapat mendeteksi dan merespons ancaman dengan cepat. Keamanan data tidak hanya melibatkan perlindungan dari ancaman eksternal, tetapi juga memastikan bahwa hanya individu yang berwenang yang dapat mengakses informasi tertentu.

Pada audit TI berkelanjutan, penting untuk mematuhi peraturan perlindungan data yang berlaku, seperti *General Data Protection Regulation* (GDPR) di Eropa atau peraturan serupa di wilayah lain. Audit ini mengidentifikasi apakah organisasi telah mengimplementasikan kebijakan dan prosedur untuk memastikan kepatuhan terhadap regulasi tersebut. Kepatuhan terhadap GDPR, misalnya, mencakup prinsip-prinsip dasar seperti hak akses data, hak untuk dilupakan, serta transparansi dalam pengumpulan dan penggunaan data pribadi. Jika perusahaan gagal memenuhi persyaratan regulasi ini, dapat menimbulkan risiko hukum yang signifikan serta merusak reputasi perusahaan.

2. Penerapan Pendekatan Berkelanjutan dalam Audit TI

Penerapan pendekatan berkelanjutan dalam audit TI memerlukan penerapan prinsip-prinsip keberlanjutan dalam semua fase audit. Beberapa penerapan utama dalam konteks audit TI adalah sebagai berikut:

a. Evaluasi Dampak Lingkungan Teknologi

Evaluasi dampak lingkungan teknologi dalam audit TI berkelanjutan merupakan aspek yang sangat penting untuk memastikan bahwa organisasi tidak hanya fokus pada keuntungan finansial tetapi juga mempertimbangkan dampak ekologis dari penggunaan teknologi. Salah satu hal utama yang dievaluasi adalah bagaimana organisasi mengelola sumber daya alam dalam operasional TI. Misalnya, pengelolaan energi dalam pusat data (*data center*) menjadi perhatian utama, karena pusat data sering kali mengkonsumsi energi yang sangat besar. Menggunakan teknologi yang lebih efisien energi, seperti *cloud computing*, dapat membantu mengurangi penggunaan energi fosil dan mengurangi jejak karbon perusahaan (Bravi *et al*., 2020).

Auditor harus menilai pengurangan emisi karbon dari aktivitas TI. Dengan beralih ke solusi berbasis *cloud*, perusahaan dapat mengurangi kebutuhan untuk pusat data fisik yang besar, yang biasanya beroperasi dengan intensif energi. *Cloud computing* juga memungkinkan pengelolaan sumber daya yang lebih terpusat dan lebih efisien, mengurangi beban energi yang diperlukan untuk menjalankan server dan perangkat keras lainnya. Implementasi teknologi ramah lingkungan seperti virtualisasi server juga membantu mengurangi emisi karbon dan mendukung keberlanjutan operasional.

b. Penggunaan Teknologi Hijau dan Ramah Lingkungan

Penggunaan teknologi hijau (*green IT*) adalah bagian integral dari pendekatan berkelanjutan dalam audit TI, karena teknologi ini berfokus pada efisiensi energi dan pengurangan dampak lingkungan dari infrastruktur teknologi. Auditor perlu menilai apakah perusahaan telah mengadopsi perangkat keras dan perangkat lunak yang dirancang untuk mengurangi konsumsi energi dan emisi karbon. Contoh teknologi hijau yang umum digunakan adalah server dengan rating efisiensi energi tinggi,

yang mengurangi konsumsi listrik dan dampak lingkungan yang ditimbulkan dari operasi data center.

Perangkat keras yang ramah lingkungan juga mencakup penggunaan perangkat yang lebih efisien dan dapat didaur ulang. Sebagai contoh, banyak perusahaan yang kini beralih menggunakan server dan perangkat penyimpanan berbasis *solid-state drives* (SSD) karena lebih hemat energi dibandingkan dengan perangkat penyimpanan tradisional yang menggunakan *hard disk drives* (HDD). Selain itu, perangkat-perangkat ini memiliki umur pakai yang lebih panjang, sehingga mengurangi frekuensi penggantian perangkat keras dan jumlah limbah elektronik yang dihasilkan.

c. Keberlanjutan dalam Pemrograman dan Pengembangan Sistem

Keberlanjutan dalam pengembangan perangkat lunak semakin menjadi fokus utama dalam praktik audit TI yang berkelanjutan. Salah satu pendekatan yang diadopsi adalah pengembangan perangkat lunak yang efisien dalam penggunaan sumber daya sepanjang siklus hidupnya. Penggunaan sumber daya yang lebih sedikit selama tahap pengembangan dan operasi sistem tidak hanya mengurangi biaya, tetapi juga berdampak positif terhadap keberlanjutan lingkungan. Hal ini bisa mencakup pengoptimalan kode untuk mengurangi penggunaan daya dan meminimalkan jejak karbon yang dihasilkan dari operasional perangkat lunak tersebut.

Interoperabilitas antar sistem juga menjadi faktor penting dalam pengembangan perangkat lunak berkelanjutan. Dengan memastikan sistem yang dibangun dapat bekerja secara lancar dengan sistem lain, organisasi dapat menghindari duplikasi fungsi dan pemborosan sumber daya. Sebagai contoh, pengembangan aplikasi yang mudah terintegrasi dengan perangkat lunak lain mengurangi kebutuhan untuk membangun solusi yang redundan, yang pada gilirannya dapat mengurangi beban sistem dan penggunaan energi. Interoperabilitas yang baik juga mendukung penghematan waktu dan biaya, serta memperpanjang usia pakai sistem yang ada.

C. Kolaborasi antara Auditor IT dan Auditor Keuangan

Pada dunia bisnis yang semakin bergantung pada teknologi informasi (TI), audit IT dan audit keuangan menjadi dua bidang yang saling terkait dan penting dalam memastikan integritas serta transparansi laporan keuangan organisasi. Seiring dengan meningkatnya kompleksitas sistem TI, terdapat kebutuhan yang semakin besar untuk kolaborasi yang lebih erat antara auditor IT dan auditor keuangan. Kolaborasi ini tidak hanya akan meningkatkan efektivitas audit, tetapi juga membantu mengidentifikasi potensi risiko yang lebih baik serta meningkatkan kualitas pelaporan keuangan. Kolaborasi yang efektif antara auditor IT dan auditor keuangan menggabungkan keahlian dari kedua disiplin ilmu untuk memeriksa bagaimana sistem TI mendukung atau mempengaruhi laporan keuangan perusahaan. Hal ini melibatkan audit teknologi yang memadai untuk memastikan bahwa kontrol TI berfungsi dengan baik, dan pada saat yang sama, memastikan bahwa laporan keuangan yang dihasilkan tidak hanya akurat tetapi juga dapat dipercaya.

1. Model Kolaborasi Terpadu

Model Kolaborasi Terpadu dalam audit TI melibatkan kerja sama yang erat antara auditor TI dan auditor keuangan sepanjang seluruh proses audit. Dalam model ini, kedua auditor bekerja bersama-sama sejak tahap perencanaan hingga pelaporan akhir, memastikan bahwa setiap temuan dan evaluasi yang dilakukan saling terintegrasi. Kolaborasi ini memungkinkan kedua pihak untuk mendapatkan gambaran yang lebih komprehensif tentang sistem TI yang digunakan dalam perusahaan serta dampaknya terhadap laporan keuangan. Hal ini sangat penting mengingat semakin berkembangnya ketergantungan perusahaan pada teknologi untuk memproses data keuangan.

Auditor TI dalam model ini berfokus pada penilaian terhadap sistem TI yang mendukung proses bisnis dan laporan keuangan. Mengevaluasi kontrol TI, mengidentifikasi potensi risiko dalam pengelolaan data, serta menilai kecukupan perlindungan terhadap informasi sensitif. Auditor TI juga bertugas memastikan bahwa sistem TI dapat menghasilkan data yang akurat dan dapat diandalkan untuk proses pelaporan keuangan. Sementara itu, auditor keuangan menilai prosedur akuntansi yang berlaku dan pencatatan transaksi yang

dihasilkan oleh sistem TI. Auditor akan memastikan bahwa laporan keuangan yang dihasilkan sesuai dengan standar akuntansi yang berlaku dan mencerminkan kondisi keuangan perusahaan yang sebenarnya.

2. Model Kolaborasi Secara Paralel

Model Kolaborasi Secara Paralel dalam audit TI melibatkan pendekatan di mana auditor TI dan auditor keuangan bekerja secara independen namun bersamaan dalam area yang menjadi tanggung jawab masing-masing. Masing-masing auditor menilai komponen yang berbeda dari sistem yang mendukung laporan keuangan. Auditor TI fokus pada evaluasi terhadap kontrol teknologi informasi, pemrosesan data, dan infrastruktur TI yang mendukung operasional perusahaan. Di sisi lain, auditor keuangan memeriksa prosedur akuntansi, pengelolaan transaksi, dan penyusunan laporan keuangan berdasarkan data yang diolah oleh sistem TI. Hasil temuan dari kedua auditor ini baru akan dibahas bersama pada tahap akhir, untuk kemudian dibandingkan dan dianalisis secara komprehensif.

Pendekatan ini cocok untuk organisasi yang memiliki struktur terpisah antara departemen TI dan keuangan, di mana masing-masing departemen bekerja secara lebih mandiri. Dalam struktur seperti ini, fungsi TI dan keuangan sering kali tidak terintegrasi secara langsung, sehingga auditor memiliki kebebasan untuk mengevaluasi risiko di setiap area secara terpisah. Misalnya, auditor TI akan lebih fokus pada analisis risiko yang berkaitan dengan perangkat keras, perangkat lunak, dan kontrol sistem TI yang mendukung pengolahan data keuangan. Auditor keuangan, di sisi lain, akan memastikan bahwa data yang dihasilkan oleh sistem TI sesuai dengan standar akuntansi dan dapat diandalkan dalam laporan keuangan.

3. Model Kolaborasi Berdasarkan Proyek

Model Kolaborasi Secara Paralel dalam audit TI melibatkan pendekatan di mana auditor TI dan auditor keuangan bekerja secara independen namun bersamaan dalam area yang menjadi tanggung jawab masing-masing. Masing-masing auditor menilai komponen yang berbeda dari sistem yang mendukung laporan keuangan. Auditor TI fokus pada evaluasi terhadap kontrol teknologi informasi, pemrosesan data, dan infrastruktur TI yang mendukung operasional perusahaan. Di sisi lain, auditor keuangan memeriksa prosedur akuntansi, pengelolaan

transaksi, dan penyusunan laporan keuangan berdasarkan data yang diolah oleh sistem TI. Hasil temuan dari kedua auditor ini baru akan dibahas bersama pada tahap akhir, untuk kemudian dibandingkan dan dianalisis secara komprehensif.

Pendekatan ini cocok untuk organisasi yang memiliki struktur terpisah antara departemen TI dan keuangan, di mana masing-masing departemen bekerja secara lebih mandiri. Dalam struktur seperti ini, fungsi TI dan keuangan sering kali tidak terintegrasi secara langsung, sehingga auditor memiliki kebebasan untuk mengevaluasi risiko di setiap area secara terpisah. Misalnya, auditor TI akan lebih fokus pada analisis risiko yang berkaitan dengan perangkat keras, perangkat lunak, dan kontrol sistem TI yang mendukung pengolahan data keuangan. Auditor keuangan, di sisi lain, akan memastikan bahwa data yang dihasilkan oleh sistem TI sesuai dengan standar akuntansi dan dapat diandalkan dalam laporan keuangan.

D. Pelatihan dan Sertifikasi untuk Auditor IT (CISA, CISSP)

Seiring dengan semakin kompleksnya landscape teknologi informasi dan ancaman yang ada di dunia digital, kebutuhan untuk meningkatkan keahlian dan pengetahuan auditor IT semakin mendesak. Audit IT, yang mencakup pemeriksaan kontrol keamanan, pengelolaan risiko, dan kepatuhan terhadap standar serta regulasi, memerlukan auditor yang memiliki kompetensi yang cukup tinggi. Sertifikasi seperti *Certified Information Systems Auditor* (CISA) dan *Certified Information Systems Security Professional* (CISSP) telah menjadi acuan utama dalam memastikan auditor memiliki pemahaman yang mendalam mengenai aspek-aspek penting dalam audit IT.

1. CISA (*Certified Information Systems Auditor*)

CISA adalah sertifikasi profesional yang diberikan oleh ISACA (*Information Systems Audit and Control Association*). Sertifikasi ini dirancang untuk individu yang ingin mengembangkan keahlian dalam audit, kontrol, dan keamanan sistem informasi. CISA difokuskan pada pengelolaan dan pemeriksaan sistem informasi serta penilaian risiko yang terkait dengan penggunaan TI dalam organisasi. Melalui pelatihan CISA, auditor IT akan mempelajari aspek-aspek berikut:

a. Pengelolaan Risiko IT

Pengelolaan risiko IT adalah salah satu komponen kunci dalam sertifikasi *Certified Information Systems Auditor* (CISA). Auditor yang memiliki sertifikasi ini bertanggung jawab untuk menilai dan mengelola berbagai jenis risiko yang dapat memengaruhi teknologi informasi dalam organisasi. Risiko ini bisa berasal dari kegagalan sistem TI yang tidak terduga, ancaman eksternal seperti peretasan atau malware, serta kebijakan internal yang mungkin tidak memadai dalam melindungi infrastruktur TI. Dengan meningkatnya ketergantungan organisasi terhadap teknologi, risiko-risiko ini menjadi semakin kompleks dan berpotensi merusak operasional bisnis secara signifikan (ISACA, 2012).

Salah satu aspek penting dalam pengelolaan risiko IT adalah identifikasi dan penilaian terhadap potensi ancaman yang dapat mengganggu sistem informasi. Auditor CISA harus memahami seluruh spektrum risiko, mulai dari ancaman fisik yang dapat merusak perangkat keras, hingga ancaman yang lebih canggih seperti serangan dunia maya yang dapat mengakses data sensitif atau merusak integritas sistem. Untuk itu, auditor perlu memastikan bahwa setiap komponen dalam infrastruktur TI telah dievaluasi secara mendalam, dengan mempertimbangkan dampak yang dapat ditimbulkan jika ancaman tersebut terjadi.

b. Kontrol dan Keamanan Sistem Informasi

Kontrol dan keamanan sistem informasi merupakan aspek fundamental dalam audit TI, terutama bagi seorang *Certified Information Systems Auditor* (CISA). Auditor bertugas untuk memastikan bahwa kontrol TI yang diterapkan oleh organisasi sesuai dengan kebijakan internal, peraturan yang berlaku, dan standar industri. Pengelolaan kontrol ini mencakup pengamanan data dan perangkat keras, pengelolaan akses, serta penetapan kebijakan untuk mengurangi potensi risiko yang dapat memengaruhi integritas dan kerahasiaan informasi. CISA harus memastikan bahwa kontrol tersebut diterapkan secara konsisten dan efektif untuk mencegah ancaman yang dapat merusak sistem TI organisasi.

Sebagai contoh kontrol akses yang ketat harus diterapkan untuk membatasi siapa yang dapat mengakses informasi sensitif.

CISA perlu memverifikasi bahwa sistem kontrol akses berbasis peran (*role-based access control*) sudah diterapkan dengan baik, memastikan bahwa hanya individu yang berwenang yang dapat mengakses data dan aplikasi tertentu. Auditor juga perlu memeriksa kebijakan pengelolaan kata sandi, otentikasi dua faktor, serta prosedur untuk mengelola akses pengguna eksternal. Semua kontrol ini harus diselaraskan dengan peraturan privasi data yang relevan, seperti *General Data Protection Regulation* (GDPR) atau undang-undang serupa.

c. Keamanan Informasi dan Perlindungan Data

Keamanan informasi dan perlindungan data adalah elemen penting dalam peran seorang *Certified Information Systems Auditor* (CISA). Tugas utama auditor adalah melindungi data sensitif organisasi dengan cara mengidentifikasi potensi ancaman terhadap integritas, kerahasiaan, dan ketersediaan informasi tersebut. Hal ini dimulai dengan mengevaluasi kontrol pengamanan yang ada, seperti enkripsi data, pengelolaan akses pengguna, dan kebijakan keamanan. Auditor akan memastikan bahwa kontrol yang diterapkan sesuai dengan standar industri dan peraturan yang relevan, seperti *General Data Protection Regulation* (GDPR) untuk melindungi data pribadi.

Proses audit juga mencakup identifikasi risiko yang mungkin mengancam data organisasi, baik yang bersifat internal maupun eksternal. Ancaman bisa datang dari berbagai sumber, termasuk peretasan, kelalaian pegawai, atau bahkan bencana alam yang dapat merusak infrastruktur TI. Auditor TI akan menilai sejauh mana organisasi mampu mendeteksi dan merespons ancaman tersebut, serta apakah mekanisme pemulihan data yang ada sudah memadai untuk menghadapi skenario darurat. Misalnya, apakah organisasi memiliki prosedur cadangan data yang aman dan dapat diakses dalam keadaan kritis.

2. CISSP (*Certified Information Systems Security Professional*)

CISSP adalah sertifikasi yang diberikan oleh $(ISC)^2$ (*International Information System Security Certification Consortium*) dan dikenal sebagai salah satu sertifikasi terkemuka dalam bidang keamanan siber. Sertifikasi ini dirancang untuk profesional yang terlibat dalam pengelolaan dan perlindungan data organisasi melalui kontrol

keamanan yang efektif. Sertifikasi CISSP mengharuskan kandidat untuk memiliki pengetahuan yang mendalam tentang berbagai disiplin dalam keamanan sistem informasi, termasuk:

a. Keamanan Jaringan

Keamanan jaringan adalah salah satu pilar utama dalam perlindungan sistem informasi dan data dalam organisasi. Seorang *Certified Information Systems Security Professional* (CISSP) bertanggung jawab untuk merancang dan mengimplementasikan arsitektur jaringan yang aman, yang berfungsi untuk melindungi data yang dikirimkan antar sistem. Salah satu langkah penting dalam merancang keamanan jaringan adalah dengan menerapkan teknik segmentasi jaringan untuk membatasi akses hanya kepada pihak yang berwenang. Ini dapat mencakup penggunaan firewall, router, dan switch yang dikonfigurasi dengan baik untuk membatasi lalu lintas yang tidak sah (Gregg & Johnson, 2017).

Untuk meningkatkan keamanan, auditor CISSP juga akan memastikan penerapan teknologi enkripsi dalam transmisi data. Enkripsi berperan penting dalam mengamankan data yang bergerak melalui jaringan, sehingga meskipun data tersebut terintersepsi, ia tetap tidak dapat dibaca tanpa kunci dekripsi yang tepat. Dengan enkripsi end-to-end, data yang dikirimkan antar perangkat atau server akan tetap terjaga kerahasiaannya, meskipun berada dalam lingkungan jaringan yang berisiko.

b. Pengelolaan Keamanan Aplikasi

Pengelolaan keamanan aplikasi merupakan salah satu aspek penting dalam menjaga integritas dan kerahasiaan sistem informasi dalam organisasi. Seorang *Certified Information Systems Security Professional* (CISSP) bertanggung jawab untuk mengembangkan kebijakan dan prosedur yang memastikan bahwa aplikasi yang digunakan oleh organisasi aman dari potensi ancaman. Salah satu langkah pertama yang perlu diambil adalah identifikasi potensi kerentanannya sejak tahap pengembangan. Ini mencakup penerapan prinsip-prinsip pengembangan perangkat lunak yang aman, seperti input sanitization, validasi data, dan pembatasan hak akses.

Penting juga untuk menerapkan prinsip secure coding dalam pengembangan aplikasi. *Secure coding* adalah pendekatan untuk

menulis kode yang mencegah kerentanannya, seperti SQL *injection, cross-site scripting* (XSS), atau *buffer overflow*. CISSP bertugas memastikan bahwa para pengembang memahami dan mematuhi pedoman ini untuk mengurangi potensi eksploitasi dalam aplikasi. Selain itu, pengujian keamanan aplikasi secara berkala menggunakan teknik seperti penetration testing dan static analysis juga menjadi bagian dari pengelolaan keamanan aplikasi yang efektif.

c. Keamanan Operasional

Keamanan operasional adalah aspek penting dalam melindungi organisasi dari ancaman yang muncul selama operasi sehari-hari. Seorang *Certified Information Systems Security Professional* (CISSP) bertanggung jawab untuk memastikan bahwa semua sistem, perangkat, dan jaringan yang digunakan dalam operasional organisasi dilindungi dari potensi ancaman, baik yang berasal dari dalam maupun luar. Salah satu cara untuk mencapainya adalah dengan mengimplementasikan pengendalian keamanan yang komprehensif, yang mencakup pengawasan aktivitas pengguna, analisis log, dan penegakan kebijakan keamanan yang ketat untuk mencegah kebocoran atau pencurian data.

Pengawasan terhadap aktivitas mencurigakan menjadi komponen kunci dalam keamanan operasional. CISSP harus memastikan bahwa semua aktivitas di dalam sistem dan jaringan organisasi dipantau secara *real-time* menggunakan alat keamanan canggih seperti *intrusion detection systems* (IDS) dan *intrusion prevention systems* (IPS). Sistem ini membantu mendeteksi tanda-tanda awal dari serangan atau perilaku tidak wajar yang dapat mengindikasikan adanya ancaman. Pengawasan ini harus bersifat proaktif, memastikan bahwa potensi ancaman dapat diidentifikasi sebelum berkembang menjadi masalah serius.

E. Studi Kasus: Praktik Audit IT yang Sukses

Audit IT adalah bagian integral dari proses manajemen risiko dan pengawasan terhadap sistem informasi dalam organisasi. Keberhasilan audit IT dapat dilihat dari bagaimana audit tersebut mengidentifikasi

potensi masalah, meningkatkan kontrol internal, serta mendeteksi dan mencegah kerugian akibat risiko terkait teknologi informasi. Beberapa studi kasus yang berhasil di berbagai perusahaan di dunia menunjukkan bagaimana audit IT yang efektif dapat meningkatkan transparansi, akuntabilitas, serta keamanan data dalam sistem informasi.

1. Audit IT di Perusahaan Perbankan – HSBC

Audit Teknologi Informasi (IT) di HSBC, salah satu bank terbesar di dunia, berfungsi sebagai bagian integral dalam pengelolaan risiko, kepatuhan terhadap regulasi, dan penguatan keamanan data. Dengan operasi globalnya, HSBC menghadapi tantangan unik dalam memastikan sistem TI yang kuat dan sesuai dengan peraturan ketat seperti GDPR (*General Data Protection Regulation*) dan regulasi lain di sektor perbankan. Audit IT yang diterapkan bertujuan untuk mengidentifikasi kelemahan, memitigasi ancaman, dan meningkatkan efisiensi operasional. Tahapan audit IT di HSBC dimulai dengan penilaian risiko mendalam terhadap infrastruktur TI. Dalam proses ini, auditor menilai berbagai area kritis, seperti pengelolaan akses ke sistem yang sensitif, kontrol data pelanggan, dan pemantauan aktivitas transaksi yang mencurigakan. Audit juga mencakup analisis terhadap perangkat keras dan perangkat lunak untuk memastikan bahwa teknologi yang digunakan aman dan bebas dari kerentanan.

HSBC bekerja sama dengan auditor pihak ketiga untuk memastikan independensi dan objektivitas dalam menilai kontrol internal TI. Pendekatan ini memberikan pandangan yang lebih komprehensif dan membantu mengungkap kelemahan yang mungkin tidak terlihat oleh tim internal. Audit eksternal ini juga membantu bank memenuhi standar akuntabilitas yang lebih tinggi dan memastikan transparansi kepada regulator dan pemegang saham. Hasil dari audit ini menunjukkan berbagai peluang perbaikan. Salah satu temuan penting adalah kelemahan dalam pengelolaan data pelanggan, yang jika tidak diatasi, dapat meningkatkan risiko kebocoran data. Temuan lain terkait dengan proses pemulihan bencana, yang perlu disempurnakan untuk memastikan kelangsungan operasional jika terjadi gangguan besar. Identifikasi masalah ini memungkinkan HSBC untuk mengambil langkah-langkah proaktif guna mengurangi risiko.

Manfaat utama dari pelaksanaan audit IT adalah peningkatan kepatuhan terhadap regulasi internasional, seperti GDPR, yang

mengharuskan perusahaan untuk melindungi data pribadi pelanggan secara ketat. Dengan memastikan bahwa semua sistem TI memenuhi persyaratan regulasi, HSBC menghindari potensi sanksi dan menjaga reputasinya sebagai bank yang andal. Selain itu, audit ini juga membantu meningkatkan kesadaran internal tentang pentingnya keamanan data. Selain dari sisi kepatuhan, audit IT juga memberikan nilai tambah dalam memperkuat integritas operasional HSBC. Dengan mengidentifikasi celah dan memperbaiki kontrol internal, HSBC dapat mengurangi risiko serangan siber yang dapat merugikan pelanggan dan operasional bank.

2. Audit IT di Perusahaan E-commerce – Amazon

Audit Teknologi Informasi (IT) di Amazon, sebagai salah satu platform e-commerce terbesar di dunia, merupakan elemen kritis untuk menjaga keamanan data dan kelangsungan operasionalnya. Dengan volume transaksi yang sangat besar dan keberadaan globalnya, Amazon menghadapi tantangan besar dalam memastikan infrastruktur TI yang aman, andal, dan sesuai dengan regulasi. Audit IT menjadi alat penting untuk mengidentifikasi kelemahan, memitigasi risiko, dan meningkatkan efisiensi dalam pengelolaan data dan transaksi pelanggan. Salah satu fokus utama dalam audit IT Amazon adalah pada infrastruktur *cloud*, yang menjadi tulang punggung operasional perusahaan. Dengan memanfaatkan layanan *Amazon Web Services* (AWS) sendiri, Amazon mengandalkan audit untuk memastikan bahwa layanan *cloud* tersebut memenuhi standar keamanan internasional seperti ISO 27001 dan SOC 2. Evaluasi menyeluruh dilakukan terhadap kontrol keamanan, kebijakan privasi, dan protokol pengelolaan data untuk memastikan ketersediaan dan integritas sistem.

Amazon menggunakan teknologi mutakhir seperti big data analytics dan kecerdasan buatan (AI) dalam proses auditnya. Teknologi ini membantu mendeteksi pola anomali dalam lalu lintas data dan transaksi, yang dapat mengindikasikan potensi ancaman keamanan atau aktivitas mencurigakan. Dengan pendekatan berbasis data, auditor dapat lebih cepat mengidentifikasi kelemahan dalam sistem dan mengambil langkah korektif secara *real-time*. Kolaborasi antara auditor IT dan tim keamanan siber Amazon menjadi elemen kunci dalam audit ini. Kerjasama ini memungkinkan pengujian penetrasi (*penetration testing*) untuk mengukur kerentanannya terhadap serangan siber. Proses ini membantu Amazon mengidentifikasi potensi akses tidak sah ke data

pelanggan dan melindungi platformnya dari risiko pencurian data atau pelanggaran kebijakan.

Audit ini juga fokus pada privasi data pelanggan, mengingat Amazon memproses informasi sensitif seperti alamat, metode pembayaran, dan riwayat pembelian. Hasil audit memungkinkan Amazon untuk memperbaiki kontrol akses, meningkatkan enkripsi data, dan memastikan kebijakan privasi tetap relevan dengan peraturan seperti GDPR di Eropa dan CCPA di California. Keberhasilan audit IT Amazon tercermin dalam peningkatan kepercayaan pelanggan dan mitra bisnis. Dengan menunjukkan kepatuhan terhadap standar keamanan global, Amazon memperkuat posisinya sebagai platform e-commerce yang andal dan aman. Selain itu, audit ini mendukung operasional Amazon untuk tetap kompetitif dalam pasar digital yang semakin ketat.

BAB IX
MASA DEPAN AUDIT IT DALAM KEUANGAN

Masa depan audit IT dalam keuangan menggambarkan bagaimana dunia digital yang terus berkembang akan memengaruhi praktek audit IT, terutama dalam sektor keuangan. Seiring dengan kemajuan teknologi seperti kecerdasan buatan, big data, dan *blockchain*, auditor harus beradaptasi dengan cara baru dalam memeriksa, mengelola, dan melindungi data yang sangat sensitif. Perkembangan ini juga meningkatkan peran teknologi dalam mendukung audit keuangan, memungkinkan otomatisasi proses audit untuk meningkatkan efisiensi dan akurasi dalam identifikasi potensi risiko. Dengan semakin kompleksnya regulasi dan meningkatnya ancaman dari pelanggaran keamanan data, auditor IT di sektor keuangan juga menghadapi tantangan baru.

A. Dampak Digitalisasi pada Audit IT

Digitalisasi telah merubah lanskap berbagai sektor industri, termasuk dalam bidang keuangan. Sektor keuangan, yang mengelola data sensitif dan proses transaksi yang sangat penting, telah mengadopsi teknologi digital untuk meningkatkan efisiensi, mengurangi biaya, serta memberikan layanan yang lebih cepat dan lebih aman. Namun, digitalisasi juga membawa tantangan baru, terutama terkait dengan pengawasan dan audit.

1. Digitalisasi dalam Sektor Keuangan

Digitalisasi telah membawa transformasi besar dalam sektor keuangan, menjadikannya salah satu sektor paling adaptif terhadap perubahan teknologi. Bank, lembaga keuangan, dan perusahaan fintech

memanfaatkan teknologi seperti *cloud computing*, big data, kecerdasan buatan (AI), dan *blockchain* untuk meningkatkan efisiensi dan memperluas layanan. Misalnya, sistem berbasis *cloud* memberikan fleksibilitas dalam pengelolaan data, memungkinkan akses cepat dan *real-time* terhadap informasi keuangan, serta mendukung pengurangan biaya operasional yang signifikan (Knechel & Salterio, 2016). Salah satu kontribusi utama digitalisasi adalah peningkatan layanan pelanggan. Dengan aplikasi mobile banking, nasabah dapat melakukan berbagai transaksi seperti pembayaran, transfer, dan pengelolaan rekening tanpa harus pergi ke cabang fisik. Selain itu, teknologi seperti AI digunakan untuk meningkatkan personalisasi layanan, seperti memberikan rekomendasi investasi berdasarkan analisis kebutuhan nasabah dan pola keuangan. Ini tidak hanya meningkatkan pengalaman pelanggan tetapi juga memperkuat loyalitas terhadap lembaga keuangan.

Teknologi big data berperan penting dalam menganalisis dan memanfaatkan data dalam jumlah besar. Dengan memanfaatkan big data analytics, perusahaan keuangan dapat mendeteksi anomali, mengenali pola risiko, dan meningkatkan pengambilan keputusan strategis. Sebagai contoh, sistem berbasis AI dan *machine learning* dapat memprediksi potensi risiko kredit atau mendeteksi aktivitas mencurigakan yang mungkin terkait dengan penipuan. Namun, digitalisasi juga menghadirkan tantangan, khususnya dalam keamanan data dan keandalan sistem. Dengan meningkatnya ketergantungan pada teknologi digital, risiko pelanggaran data dan serangan siber menjadi perhatian utama. Data nasabah, yang sering kali mencakup informasi pribadi dan finansial yang sangat sensitif, harus dilindungi dengan teknologi enkripsi tingkat lanjut dan kontrol akses yang ketat.

2. Perubahan dalam Praktik Audit IT

Perubahan signifikan dalam praktik audit IT terjadi seiring dengan digitalisasi yang mengubah cara perusahaan menjalankan operasinya. Sebelum era digital, audit IT lebih sederhana, berfokus pada evaluasi sistem teknologi informasi untuk memastikan bahwa data dan transaksi keuangan tercatat dengan benar, aman, dan sesuai dengan peraturan. Auditor menilai efektivitas kontrol internal guna mencegah risiko seperti penipuan, kesalahan pencatatan, dan pelanggaran kebijakan perusahaan (Provancha, 2019). Namun, dengan berkembangnya teknologi digital, praktik audit IT menjadi lebih

kompleks dan dinamis. Auditor kini harus menghadapi infrastruktur IT yang terus berubah, termasuk komputasi awan, sistem berbasis *blockchain*, dan aplikasi berbasis kecerdasan buatan (AI). Audit IT modern beralih dari sekadar memverifikasi kontrol internal menjadi penilaian yang lebih luas terhadap risiko sistemik yang dapat berdampak pada keamanan data, integritas sistem, dan keberlanjutan operasional.

Digitalisasi telah memungkinkan auditor untuk menggunakan teknologi canggih dalam pekerjaan. Perangkat lunak analitik dan algoritma *machine learning*, misalnya, memungkinkan auditor menganalisis seluruh populasi data transaksi alih-alih hanya mengambil sampel acak. Dengan metode ini, auditor dapat mengidentifikasi pola atau anomali yang sebelumnya tidak terdeteksi oleh metode audit tradisional. Pendekatan ini meningkatkan akurasi dan efisiensi audit, sekaligus membantu mengidentifikasi risiko yang tersembunyi. Selain itu, teknologi *blockchain* membawa tantangan baru dalam audit IT. Sistem berbasis *blockchain*, yang dikenal karena transparansi dan keamanannya, memerlukan auditor untuk memverifikasi validitas dan integritas data yang tersimpan di jaringan *blockchain*..

B. Tren Teknologi Baru dalam Keuangan (DeFi, Fintech)

Sektor keuangan telah mengalami transformasi besar dalam beberapa tahun terakhir berkat kemajuan pesat dalam teknologi. Dengan munculnya teknologi baru, terutama dalam bidang *Decentralized Finance* (DeFi) dan Fintech (*Financial Technology*), sektor ini tidak hanya mengalami perubahan dalam cara transaksi dilakukan, tetapi juga dalam cara audit dilakukan.

1. *Decentralized Finance* (DeFi)

Decentralized Finance (DeFi) adalah ekosistem keuangan berbasis teknologi *blockchain* yang memungkinkan transaksi keuangan dilakukan tanpa perantara seperti bank atau lembaga keuangan tradisional. Dengan menggunakan prinsip desentralisasi, DeFi memanfaatkan *blockchain* untuk menawarkan solusi keuangan yang transparan, aman, dan terbuka. Semua transaksi dicatat secara publik di *blockchain*, sehingga dapat diaudit oleh siapa saja yang memiliki akses ke jaringan tersebut, memberikan tingkat akuntabilitas yang belum pernah ada sebelumnya (Nakamoto, 2008). DeFi telah tumbuh pesat

dalam beberapa tahun terakhir, menawarkan berbagai layanan seperti pinjaman, peminjaman, perdagangan aset, dan manajemen portofolio. Inovasi utama yang memungkinkan DeFi adalah penggunaan *smart contracts* program otomatis yang berjalan di *blockchain* untuk mengeksekusi transaksi tanpa memerlukan campur tangan manusia. Kontrak pintar ini mengurangi biaya transaksi secara signifikan karena menghilangkan kebutuhan akan perantara dan mempercepat waktu penyelesaian transaksi.

Salah satu keuntungan utama DeFi adalah inklusivitasnya. Orang-orang yang tidak memiliki akses ke layanan keuangan tradisional dapat memanfaatkan platform DeFi asalkan memiliki koneksi internet dan dompet digital. DeFi juga memberikan penggunanya kontrol penuh atas aset, berbeda dengan sistem keuangan tradisional di mana aset dikelola oleh pihak ketiga. Selain itu, teknologi ini memungkinkan likuiditas global yang lebih besar, dengan pengguna dari berbagai belahan dunia dapat berpartisipasi di pasar yang sama. Namun, terlepas dari keunggulannya, DeFi juga membawa tantangan baru, terutama dalam hal pengawasan dan regulasi. Sifat desentralisasi berarti tidak ada otoritas pusat yang dapat dimintai pertanggungjawaban jika terjadi kesalahan atau pelanggaran. Ini menciptakan kebutuhan bagi auditor IT untuk mengembangkan metodologi baru dalam memverifikasi transaksi dan menilai risiko keamanan dalam ekosistem DeFi.

2. *Financial Technology* (Fintech)

Financial Technology (Fintech) mengacu pada pemanfaatan teknologi untuk meningkatkan efisiensi, kecepatan, dan keamanan layanan keuangan. Sektor ini telah berkembang pesat, mencakup beragam layanan seperti pembayaran digital, pinjaman *peer-to-peer*, manajemen investasi, hingga asuransi berbasis digital. Fintech menghadirkan peluang besar untuk merevolusi cara masyarakat mengakses dan menggunakan layanan keuangan, terutama melalui pendekatan yang lebih ramah pengguna dan inovatif (Harvey *et al*., 2021). Salah satu keunggulan fintech adalah kemampuannya untuk menyediakan layanan keuangan yang lebih mudah diakses. Aplikasi pembayaran digital seperti Gojek dan GrabPay di Asia Tenggara memungkinkan pengguna melakukan transaksi hanya dengan smartphone, mengurangi kebutuhan akan uang tunai. Selain itu, platform pinjaman online seperti Kiva dan LendInvest membantu individu dan

usaha kecil mendapatkan pembiayaan tanpa melalui proses panjang dan birokrasi lembaga keuangan konvensional.

Keberhasilan fintech juga terlihat dalam kemampuannya mendorong inklusi keuangan. Di banyak wilayah di mana akses ke bank atau lembaga keuangan terbatas, fintech membuka peluang bagi masyarakat untuk mengelola uang, mendapatkan kredit, dan berinvestasi. Dengan biaya operasional yang lebih rendah dibandingkan bank tradisional, perusahaan fintech mampu menawarkan produk keuangan yang lebih terjangkau dan efisien. Namun, pertumbuhan fintech yang pesat membawa tantangan tersendiri. Salah satunya adalah pengelolaan data pribadi pengguna. Karena platform fintech sering memproses data sensitif seperti informasi keuangan dan identitas pribadi, risiko keamanan siber menjadi perhatian utama. Serangan siber atau kebocoran data dapat menimbulkan kerugian besar bagi pengguna dan merusak kepercayaan terhadap teknologi tersebut.

C. Pengaruh Regulasi Baru terhadap Audit IT

Regulasi baru dalam sektor keuangan terutama yang terkait dengan teknologi informasi (IT), telah membawa perubahan signifikan terhadap cara auditor melakukan pemeriksaan dan pengawasan sistem keuangan. Dalam beberapa tahun terakhir, munculnya regulasi baru, baik di tingkat nasional maupun internasional, telah memberikan tantangan maupun peluang baru dalam praktik audit IT. Peraturan tersebut, seperti *General Data Protection Regulation* (GDPR) di Eropa, undang-undang perlindungan data pribadi di banyak negara, serta perubahan regulasi mengenai teknologi *blockchain* dan keuangan digital, telah mempengaruhi cara auditor IT beroperasi.

1. Regulasi Peraturan Data dan Keamanan Siber

Regulasi perlindungan data dan keamanan siber, terutama yang terkait dengan data pribadi, telah mengalami perubahan signifikan dalam beberapa tahun terakhir, dengan *General Data Protection Regulation* (GDPR) sebagai contoh utama. GDPR, yang diberlakukan di Uni Eropa pada 2018, memberikan kontrol yang lebih besar kepada individu atas data pribadi. Hal ini mengharuskan organisasi untuk memperhatikan dan menjaga data pelanggan dengan sangat hati-hati, terutama dalam hal pengumpulan, penyimpanan, dan pemrosesan data. Bagi auditor IT, ini

berarti harus memastikan bahwa perusahaan atau lembaga keuangan mematuhi peraturan ini, mengadopsi kebijakan privasi yang sesuai, serta mengimplementasikan kontrol yang tepat untuk melindungi data sensitif pelanggan. Audit yang dilakukan harus mencakup pemeriksaan atas kepatuhan terhadap prinsip-prinsip GDPR, seperti hak akses, penghapusan data, dan transparansi.

Pada konteks pengelolaan keamanan siber, regulasi baru menuntut auditor untuk menilai dan memperkuat kontrol yang ada terhadap potensi ancaman, baik yang berasal dari serangan eksternal maupun kebocoran data internal. Hal ini mendorong auditor IT untuk mengembangkan metodologi baru dalam mengevaluasi sistem keamanan siber. Auditor harus memastikan bahwa perusahaan memiliki kontrol keamanan yang memadai untuk mencegah pencurian data atau kebocoran informasi yang dapat merusak reputasi dan kepercayaan pelanggan. Selain itu, auditor perlu mengevaluasi prosedur mitigasi yang ada, serta memeriksa keefektifan rencana tanggap insiden yang akan diaktifkan apabila terjadi pelanggaran data.

2. Regulasi terkait *Blockchain* dan Keuangan Digital

Peningkatan adopsi teknologi *blockchain* dan konsep keuangan terdesentralisasi (DeFi) telah memperkenalkan tantangan baru bagi regulator yang bertugas mengatur sektor keuangan global. Dengan kemajuan pesat dalam penggunaan cryptocurrency dan token digital, peraturan baru yang mengatur penerapan teknologi ini sangat diperlukan untuk menghindari potensi penyalahgunaan atau penghindaran pajak. Misalnya, di Uni Eropa, regulasi *Markets in Crypto-Assets Regulation* (MiCA) telah diperkenalkan untuk mengatur pasar aset kripto. Regulasi ini bertujuan untuk memberikan kerangka hukum yang jelas bagi operasional pasar kripto dan layanan DeFi, mencakup aspek perlindungan investor, pengawasan pasar, dan mitigasi risiko yang terkait dengan cryptocurrency. Regulasi semacam ini mengubah cara auditor IT melakukan evaluasi terhadap perusahaan-perusahaan yang bergerak di sektor ini (Gregg & Johnson, 2017).

Sebagai bagian dari audit, auditor IT perlu memahami teknologi *blockchain* secara mendalam, karena harus memverifikasi kepatuhan terhadap regulasi baru ini. Auditor harus menilai apakah perusahaan yang bergerak di sektor kripto memiliki sistem kontrol yang cukup untuk memastikan transaksi yang dilakukan tidak melanggar regulasi yang

berlaku. Hal ini termasuk evaluasi terhadap penggunaan token digital dalam transaksi, serta memastikan bahwa perusahaan-perusahaan tersebut mematuhi peraturan yang ada terkait dengan transparansi dan pelaporan transaksi. Dengan sifat *blockchain* yang transparan dan terdesentralisasi, auditor harus memastikan bahwa perusahaan menerapkan kontrol yang tepat untuk melindungi data dan transaksi pelanggan dari potensi penyalahgunaan.

3. Peningkatan Peraturan Perlindungan Konsumen

Peningkatan peraturan perlindungan konsumen telah menjadi faktor yang signifikan dalam mengubah cara audit IT dilaksanakan, terutama di sektor keuangan. Banyak negara kini menerapkan regulasi yang lebih ketat untuk melindungi konsumen, yang menuntut transparansi lebih besar dari penyedia layanan keuangan. Regulasi seperti pengungkapan biaya tersembunyi dalam layanan finansial atau pemberian informasi yang lebih jelas mengenai risiko produk investasi telah menjadi fokus utama. Peraturan semacam ini mendorong organisasi untuk memastikan bahwa ia tidak hanya menyediakan produk dan layanan yang mematuhi standar hukum, tetapi juga menjaga kepentingan konsumen dengan cara yang adil dan transparan.

Bagi auditor IT, perubahan regulasi ini membawa dampak besar, karena diharuskan untuk mengevaluasi apakah sistem teknologi yang digunakan dalam penyediaan layanan keuangan benar-benar melindungi konsumen. Auditor harus memastikan bahwa sistem TI yang digunakan mendukung transparansi dalam hal biaya yang dikenakan kepada konsumen serta mengungkapkan secara jelas potensi risiko yang terlibat dalam produk investasi atau layanan keuangan lainnya. Ini mencakup pemeriksaan terhadap kontrol internal yang ada untuk mengidentifikasi dan mengatasi potensi risiko yang dapat merugikan konsumen, seperti biaya tersembunyi atau informasi yang tidak jelas.

D. Automasi dan Peran Auditor di Masa Depan

Audit IT dalam sektor keuangan mengalami perubahan besar dalam beberapa tahun terakhir. Dengan semakin berkembangnya teknologi, terutama dalam bidang automasi, peran auditor IT semakin berkembang dan bertransformasi. Automasi dalam audit IT mengacu pada penerapan teknologi untuk menggantikan atau mendukung tugas-

tugas manual yang sebelumnya dikerjakan oleh auditor manusia. Teknologi ini tidak hanya membantu meningkatkan efisiensi tetapi juga meningkatkan akurasi dalam evaluasi sistem teknologi informasi di perusahaan.

1. Pengaruh Automasi pada Proses Audit IT

Automasi dalam audit IT telah menjadi transformasi penting yang meningkatkan efisiensi dan akurasi dalam proses audit. Dengan penerapan perangkat lunak berbasis data, auditor IT kini dapat memeriksa transaksi dalam jumlah besar dengan cepat dan lebih akurat. Teknologi ini memungkinkan pemrosesan data yang lebih efisien dan mengurangi kemungkinan terjadinya kesalahan manusia, yang sering kali menjadi tantangan dalam audit manual. Selain itu, automasi memastikan konsistensi yang lebih tinggi dalam hasil audit, yang penting untuk menjaga integritas dan kualitas laporan audit (Knechel & Salterio, 2016).

Salah satu contoh paling signifikan dari penerapan automasi adalah penggunaan analitik data dalam audit. Dengan kemampuan untuk menganalisis big data, auditor IT dapat memeriksa ribuan hingga jutaan transaksi dalam waktu yang lebih singkat dibandingkan dengan proses manual. Perangkat analitik canggih dan kecerdasan buatan (AI) memungkinkan auditor untuk mendeteksi pola yang mencurigakan atau anomali dalam data, yang mungkin tidak terlihat oleh manusia. Misalnya, dalam audit keuangan, sistem otomatis dapat mengidentifikasi transaksi yang tidak biasa atau potensi risiko keamanan dengan lebih cepat dan tepat, meningkatkan kualitas pengawasan dan mitigasi risiko.

2. Peran Auditor IT di Era Automasi

Di era automasi, peran auditor IT tidak akan sepenuhnya digantikan oleh teknologi, meskipun teknologi tersebut memberikan peningkatan efisiensi dan akurasi. Automasi lebih berfungsi untuk mempermudah proses analisis data besar, mempercepat identifikasi masalah, dan mengurangi potensi kesalahan manusia. Namun, auditor IT tetap memiliki peran yang sangat penting sebagai pengawas dan analis untuk memastikan bahwa sistem automasi bekerja sesuai dengan standar yang ditetapkan, serta memastikan bahwa data yang dihasilkan dapat dipercaya, harus memiliki keterampilan teknis yang lebih dalam bidang

keamanan siber, analitik data, dan penggunaan perangkat lunak otomatis untuk dapat menangani tantangan yang muncul.

Auditor IT akan lebih banyak menghabiskan waktunya untuk menginterpretasikan hasil dari analisis yang dilakukan oleh sistem automasi, serta memverifikasi keputusan yang diambil oleh perangkat otomatis. Misalnya, dalam analisis keamanan siber, perangkat lunak otomatis dapat mendeteksi potensi ancaman, namun auditor bertanggung jawab untuk menilai dampak dari ancaman tersebut, serta memastikan bahwa keputusan yang diambil oleh sistem sesuai dengan kebijakan dan prosedur organisasi, juga harus memastikan bahwa langkah-langkah mitigasi yang disarankan oleh sistem automasi diterapkan dengan benar untuk mengurangi risiko yang dapat merugikan organisasi.

3. Masa Depan Auditor IT di Era Automasi

Peran auditor IT akan sangat dipengaruhi oleh perkembangan pesat teknologi, terutama automasi dan teknologi canggih lainnya. Automasi sudah mulai mengubah cara auditor IT bekerja, dan seiring berjalannya waktu, auditor akan semakin bergantung pada perangkat otomatis untuk menganalisis dan memproses data dalam jumlah besar. Namun, keterampilan teknis dalam menggunakan alat-alat ini saja tidak cukup. Auditor IT juga akan membutuhkan keterampilan tambahan dalam mengelola dan memahami hasil dari analisis otomatis yang diberikan oleh perangkat tersebut. Oleh karena itu, pelatihan berkelanjutan dalam hal teknologi terkini, seperti keamanan data, kecerdasan buatan (AI), dan analitik data, akan menjadi kunci bagi auditor untuk tetap relevan dan efektif di masa depan.

Pendekatan berbasis risiko juga akan semakin penting bagi auditor IT. Di era yang didominasi oleh teknologi baru, auditor tidak hanya akan memeriksa kepatuhan terhadap regulasi dan kebijakan yang ada, tetapi juga akan perlu menganalisis potensi risiko yang muncul akibat penerapan teknologi baru dalam sistem perusahaan. Teknologi seperti *blockchain*, AI, dan *cloud computing* membuka peluang baru, tetapi juga memperkenalkan risiko-risiko baru yang harus dipahami dan dikelola oleh auditor. Misalnya, auditor perlu mengevaluasi seberapa baik perusahaan mengelola risiko yang terkait dengan penggunaan AI dalam proses pengambilan keputusan atau keamanan data yang disimpan dalam sistem berbasis *cloud*.

E. Peluang dan Tantangan dalam Audit IT yang Akan Datang

Audit IT telah berkembang pesat dalam beberapa tahun terakhir, dipengaruhi oleh kemajuan teknologi yang pesat dalam dunia keuangan. Berbagai inovasi seperti big data, *cloud computing*, *blockchain*, serta kecerdasan buatan (AI) dan pembelajaran mesin (*machine learning*) semakin mengubah cara audit dilakukan. Masa depan audit IT dalam sektor keuangan menawarkan berbagai peluang baru bagi auditor, tetapi juga datang dengan tantangan yang perlu dihadapi.

1. Peluang dalam Audit IT di Masa Depan

a. Penerapan Teknologi Canggih untuk Meningkatkan Efisiensi

Di masa depan, peluang besar dalam audit IT terletak pada penerapan teknologi canggih untuk meningkatkan efisiensi. Salah satu teknologi yang dapat mengubah cara audit dilakukan adalah analitik data besar (*big data*). Dengan volume data yang semakin besar, auditor dapat memanfaatkan alat analitik untuk memeriksa dan menganalisis informasi keuangan yang sebelumnya sulit dikelola secara manual. Contohnya, perangkat lunak analitik dapat mengidentifikasi pola transaksi mencurigakan atau potensi penipuan dengan lebih cepat dan akurat, sehingga memungkinkan auditor untuk mengambil tindakan preventif lebih awal.

Kecerdasan buatan (AI) dan pembelajaran mesin (*machine learning*) menawarkan peluang baru dalam mendeteksi anomali dalam data yang dapat menjadi indikasi masalah keuangan atau penipuan. Teknologi ini memungkinkan auditor untuk otomatis melakukan pengujian kontrol dan verifikasi transaksi secara *real-time*. Dengan kemampuan untuk mempelajari pola dan tren dari data, AI dapat memberikan wawasan yang lebih mendalam dan membantu dalam pengambilan keputusan berbasis data. Penggunaan AI ini juga meningkatkan kecepatan proses audit dan memungkinkan identifikasi risiko yang lebih cepat daripada metode tradisional.

b. Peningkatan Keamanan dan Kepatuhan

Keamanan siber menjadi semakin penting dalam dunia audit IT, mengingat ancaman yang terus berkembang terhadap data sensitif yang disimpan dan diproses oleh perusahaan.

Peningkatan serangan siber yang semakin canggih memberi auditor IT peluang untuk lebih fokus pada audit keamanan siber. Auditor akan melakukan evaluasi terhadap sistem dan infrastruktur teknologi untuk memastikan perusahaan memiliki kontrol yang cukup untuk melindungi data dari ancaman eksternal. Dengan serangan seperti ransomware dan data breaches yang semakin meningkat, audit IT akan menjadi garis depan dalam menjaga integritas dan kerahasiaan data.

Kepatuhan terhadap regulasi perlindungan data juga akan menjadi bagian penting dari peran auditor IT di masa depan. Regulasi yang lebih ketat, seperti *General Data Protection Regulation* (GDPR) di Eropa atau *Cybersecurity Maturity Model Certification* (CMMC) di sektor pertahanan AS, menuntut perusahaan untuk mematuhi standar yang ketat dalam hal perlindungan data pribadi dan sensitif. Auditor IT akan berperan penting dalam memastikan bahwa perusahaan mengikuti kebijakan yang tepat dalam mengelola dan melindungi informasi pelanggan, serta mematuhi peraturan yang berlaku di wilayah hukum masing-masing.

2. Tantangan dalam Audit IT di Masa Depan

a. Kompleksitas Teknologi yang Terus Berkembang

Salah satu tantangan besar yang dihadapi auditor IT adalah kompleksitas teknologi yang terus berkembang, terutama dengan meningkatnya adopsi teknologi canggih oleh perusahaan. Teknologi seperti *cloud computing*, big data, dan *Internet of Things* (IoT) telah memperkenalkan berbagai tantangan baru dalam proses audit. Misalnya, dalam konteks *cloud computing*, data perusahaan kini lebih banyak disimpan di luar jaringan lokal, yang menciptakan kesulitan dalam hal pengelolaan dan kepatuhan terhadap regulasi. Auditor IT harus memiliki pemahaman yang mendalam mengenai infrastruktur *cloud* untuk memastikan bahwa data yang disimpan di *cloud* memenuhi standar keamanan dan peraturan yang relevan. Selain itu, audit pada *cloud computing* memerlukan pemahaman tentang bagaimana data ditransfer dan diproses di berbagai server yang dikelola oleh penyedia layanan *cloud*, bukan oleh perusahaan itu sendiri.

Tantangan besar lainnya adalah integrasi sistem yang semakin kompleks. Banyak perusahaan sekarang menjalankan sistem yang terintegrasi dengan berbagai aplikasi yang beroperasi di platform berbeda, baik di infrastruktur lokal maupun *cloud*. Ini meningkatkan tingkat kompleksitas audit karena auditor IT harus memahami bagaimana data berpindah dan diproses di antara berbagai sistem tersebut, harus memverifikasi alur data dan memastikan bahwa proses pengolahan informasi yang melibatkan berbagai platform tetap memenuhi kebijakan internal dan peraturan eksternal yang berlaku. Dengan banyaknya sistem yang terlibat, auditor perlu memiliki keterampilan yang lebih tinggi untuk memahami interaksi antara sistem yang berbeda dan melakukan verifikasi secara efektif.

b. Masalah Keamanan dan Privasi Data

Masalah keamanan dan privasi data akan menjadi tantangan utama dalam audit IT di masa depan, mengingat semakin banyaknya data pribadi yang diproses oleh perusahaan. Keamanan data menjadi isu yang sangat krusial, terutama dengan berkembangnya ancaman siber yang semakin canggih. Penipuan dan peretasan yang ditujukan pada perusahaan dapat merusak integritas data, yang pada gilirannya dapat merugikan perusahaan secara finansial dan reputasional. Oleh karena itu, auditor IT harus terus mengikuti perkembangan terbaru dalam teknik keamanan siber dan ancaman yang mungkin timbul.

Auditor juga harus memiliki pemahaman yang lebih dalam mengenai sistem pertahanan yang digunakan untuk melindungi data sensitif dari ancaman luar. Meskipun perangkat dan alat teknologi dapat membantu dalam mendeteksi penipuan dan anomali, serangan siber yang semakin kompleks, seperti ransomware atau hacking berbasis AI, tetap menjadi ancaman serius. Auditor perlu melakukan uji penetrasi dan audit keamanan secara rutin untuk menilai apakah sistem yang ada dapat bertahan terhadap potensi ancaman yang berkembang.

BAB X
KESIMPULAN

Teknologi telah membawa perubahan besar dalam sektor keuangan di abad ke-21, dengan digitalisasi, cloud computing, blockchain, dan kecerdasan buatan menjadi pilar utama dalam pelaksanaan audit TI. Inovasi-inovasi ini tidak hanya meningkatkan kecepatan, ketelitian, dan efisiensi proses audit, tetapi juga menghadirkan tantangan baru, seperti ancaman terhadap keamanan data, ketergantungan pada sistem otomatis, serta kebutuhan untuk meningkatkan kompetensi auditor. Oleh karena itu, auditor TI diharapkan mampu menguasai analisis big data, mengelola risiko siber, dan memahami teknologi terkini yang diterapkan dalam sistem keuangan saat ini.

Peran auditor IT sangat penting dalam memastikan keamanan dan keterjaminan perusahaan terhadap regulasi yang semakin kompleks. Auditor IT bertanggung jawab untuk memitigasi risiko yang terkait dengan keamanan siber, melindungi data sensitif, dan memastikan bahwa sistem keuangan perusahaan memenuhi standar yang berlaku. Buku ini membahas pentingnya penerapan standar internasional, seperti ISO/IEC 27001 dan COBIT, yang memberikan kerangka kerja bagi auditor dalam mengawasi dan menerangi sistem TI secara efektif. Standar-standar ini tidak hanya meningkatkan kepatuhan, tetapi juga memperkuat kepercayaan pemangku kepentingan terhadap integritas dan transparansi laporan keuangan.

Salah satu inovasi yang memberikan dampak besar adalah blockchain. Teknologi ini menciptakan buku besar terdesentralisasi yang transparan dan tahan terhadap manipulasi, meminimalkan risiko penipuan dalam sistem keuangan. Dengan blockchain, auditor dapat memverifikasi transaksi secara langsung, sehingga meningkatkan efisiensi dan akurasi proses audit. Selain itu, teknologi big data dan analitik prediktif memungkinkan auditor mendeteksi pola mencurigakan

dengan lebih cepat, membantu mengidentifikasi risiko sistemik yang dapat mengancam stabilitas keuangan perusahaan.

Perubahan lanskap teknologi juga membawa tuntutan regulasi yang lebih ketat. Contohnya, Peraturan Perlindungan Data Umum (GDPR) di Eropa mewajibkan perusahaan untuk menjaga keamanan data pribadi, menambahkan elemen baru dalam cakupan audit TI. Auditor kini tidak hanya memverifikasi angka, tetapi juga memastikan bahwa kebijakan privasi dan keamanan data perusahaan sesuai dengan peraturan yang berlaku. Dalam situasi ini, praktik audit TI semakin berkembang untuk mencakup evaluasi yang lebih komprehensif terhadap sistem dan kebijakan perusahaan.

Tantangan besar lainnya yang dihadapi auditor TI semakin meningkat ancamannya. Dengan semakin canggihnya teknologi yang digunakan oleh perusahaan, serangan siber juga semakin kompleks. Oleh karena itu, auditor harus memiliki keahlian dalam keamanan TI, termasuk pengujian penetrasi dan audit keamanan siber, untuk memastikan sistem perusahaan tahan terhadap potensi ancaman eksternal. Otomatisasi, termasuk penggunaan otomatisasi proses robotik (RPA), telah meningkatkan efisiensi audit, memungkinkan auditor untuk fokus pada analisis strategi dan mitigasi risiko daripada tugas rutin.

Audit TI dalam sektor keuangan berperan penting dalam menjaga integritas, keamanan, dan hilangnya sistem keuangan. Seiring dengan perkembangan teknologi, auditor harus terus memperbarui keterampilan melalui pelatihan dan sertifikasi, seperti CISA dan CISSP, untuk menghadapi tantangan masa depan. Dalam dunia yang semakin digital, auditor TI dituntut untuk mengelola risiko dengan lebih baik, menerapkan teknologi canggih, dan memastikan kepatuhan terhadap regulasi yang semakin kompleks. Dengan menjalankan audit yang transparan, aman, dan efisien, auditor TI akan terus menjadi penjaga stabilitas sektor keuangan dan landasan kepercayaan publik.

DAFTAR PUSTAKA

Agutter, C., & Villa, K. (2020). *ITIL Foundation Essentials ITIL 4 Edition - The ultimate revision guide, second edition*. Walter de Gruyter GmbH. https://books.google.co.id/books?id=UencDwAAQBAJ

Alahmari, A., & Duncan, B. (2020). Cybersecurity risk management in small and medium-sized enterprises: A systematic review of recent evidence. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, 1–5.

Aloqab, A., Alobaidi, F., & Raweh, B. (2018). Operational risk management in financial institutions: An overview. *Business and Economic Research*, *8*(2), 11–32.

Arslanian, H., & Fischer, F. (2019). *The Future of Finance: The Impact of FinTech, AI, and Crypto on Financial Services*. Springer International Publishing. https://books.google.co.id/books?id=u9KiDwAAQBAJ

Atkins, S., & Lawson, C. (2021). Cooperation amidst competition: cybersecurity partnership in the US financial services sector. *Journal of Cybersecurity*, *7*(1), tyab024.

Badev, A. I., & Chen, M. (2014). *Bitcoin: Technical background and data analysis*.

Balios, D., Kotsilaras, P., Eriotis, N., & Vasiliou, D. (2020). Big data, data analytics and external auditing. *Journal of Modern Accounting and Auditing*, *16*(5), 211–219.

Bernard, P. (2012). *COBIT® 5 - A Management Guide*. Van Haren Publishing. https://books.google.co.id/books?id=5F1eAgAAQBAJ

Bouveret, A. (2018). *Cyber Risk for the Financial Sector: A Framework for Quantitative Assessment*. INTERNATIONAL MONETARY FUND. https://books.google.co.id/books?id=n7QZEAAAQBAJ

Bravi, L., Santos, G., Pagano, A., & Murmura, F. (2020). Environmental management system according to ISO 14001: 2015 as a driver to sustainable development. *Corporate Social Responsibility and Environmental Management*, *27*(6), 2599–2614.

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *White Paper*, *3*(37), 1–2.

Calder, A. (2018). *NIST Cybersecurity Framework: A pocket guide*. Walter de Gruyter GmbH. https://books.google.co.id/books?id=rWxvDwAAQBAJ

Camillo, M. (2017). Cybersecurity: Risks and management of risks for global banks and financial institutions. *Journal of Risk Management in Financial Institutions*, *10*(2), 196–200.

Carter, W. (2017). *Forces shaping the cyber threat landscape for financial institutions*.

Cascarino, R. E. (2017). *Data Analytics for Internal Auditors*. CRC Press. https://books.google.co.id/books?id=6SFdDgAAQBAJ

Chapelle, A. (2019). *Operational Risk Management: Best Practices in the Financial Services Industry*. Wiley. https://books.google.co.id/books?id=Tu51DwAAQBAJ

Cichonski, P., Millar, T., Grance, T., & Scarfone, K. (2012). Computer security incident handling guide. *NIST Special Publication*, *800*(61), 1–147.

Conrad, E., Misenar, S., & Feldman, J. (2012). *CISSP Study Guide*. Elsevier Science. https://books.google.co.id/books?id=8DvPN8FKQbkC

Critical Infrastructure Cybersecurity. (2014). Framework for improving critical infrastructure cybersecurity. *Framework*, *1*(11).

Dastbaz, M., Pattinson, C., & Akhgar, B. (2015). *Green Information Technology: A Sustainable Approach*. Morgan Kaufmann. https://books.google.co.id/books?id=Le2cBAAAQBAJ

Davenport, T. H., & Patil, D. J. (2022). Is data scientist still the sexiest job of the 21st century? *Harvard Business Review*, *90*.

Dawodu, S. O., Omotosho, A., Akindote, O. J., Adegbite, A. O., & Ewuga, S. K. (2023). Cybersecurity risk assessment in banking: methodologies and best practices. *Computer Science & IT Research Journal*, *4*(3), 220–243.

de Alencar, M. S. (2022). *Cryptography and Network Security*. River Publishers. https://books.google.co.id/books?id=a6CSEAAAQBAJ

Doshi, H. (2020). *CISA – Certified Information Systems Auditor Study Guide: Aligned with the CISA Review Manual 2019 to help you audit, monitor, and assess information systems*. Packt Publishing. https://books.google.co.id/books?id=DSj5DwAAQBAJ

Dupont, B. (2019). The cyber-resilience of financial institutions: significance and applicability. *Journal of Cybersecurity*, *5*(1), tyz013.

Earley, C. E. (2015). Data analytics in auditing: Opportunities and challenges. *Business Horizons*, *58*(5), 493–500.

Ewuga, S. K., Egieya, Z. E., Omotosho, A., & Adegbite, A. O. (2023). ISO 27001 in banking: An evaluation of its implementation and effectiveness in enhancing information security. *Finance & Accounting Research Journal*, *5*(12), 405–425.

Fakeyede, O. O. O., Okeleke, P. A., Hassan, A. O., Iwuanyanwu, U., & Adaramodu, O. R. (2023). Navigating data privacy through IT audits: GDPR, CCPA, and beyond. *International Journal of Research in Engineering and Science*, *11*(11).

Fonseca-Herrera, O. A., Rojas, A. E., & Florez, H. (2021). A model of an information security management system based on NTC-ISO/IEC 27001 standard. *IAENG Int. J. Comput. Sci*, *48*(2), 213–222.

Ganji, D., Kalloniatis, C., Mouratidis, H., & Gheytassi, S. M. (2019). Approaches to develop and implement iso/iec 27001 standard-information security management systems: A systematic literature review. *Int. J. Adv. Softw*, *12*(3).

Gleim, M. R., & Stevens, J. L. (2021). *Blockchain*: a game changer for marketers? *Marketing Letters*, *32*, 123–128.

Gregg, M., & Johnson, R. (2017). *Certified Information Systems Auditor (CISA) Cert Guide*. Pearson Education. https://books.google.co.id/books?id=KF06DwAAQBAJ

Griffiths, P. (2016). *Risk-Based Auditing*. Taylor & Francis. https://books.google.co.id/books?id=ppLsCwAAQBAJ

Härle, P., Lüders, E., Pepanides, T., Pfetsch, S., Poppensieker, T., & Stegemann, U. (2010). Basel III and European banking: Its impact, how banks might respond, and the challenges of implementation. *EMEA Banking*, *13*, 2012.

Harvey, C. R., Ramachandran, A., Santoro, J., Ehrsam, F., & Buterin, V. (2021). *DeFi and the Future of Finance*. Wiley. https://books.google.co.id/books?id=YCY_EAAAQBAJ

Hughes, C., & Robinson, N. (2024). *Effective Vulnerability Management: Managing Risk in the Vulnerable Digital Ecosystem*. Wiley. https://books.google.co.id/books?id=H_H8EAAAQBAJ

Hull, J. (2012). *Risk Management and Financial Institutions, + Web Site*. Wiley. https://books.google.co.id/books?id=ixLD1gjPfoMC

Hume, J. B., Thacker, J. N., & Wilson, R. M. (2010). *Wells, Fargo & Co. Stagecoach and Train Robberies, 1870-1884: The Corporate Report of 1885 with Additional Facts About the Crimes and Their Perpetrators, revised edition*. McFarland, Incorporated, Publishers. https://books.google.co.id/books?id=oTY--EXdfGcC

ISACA. (2012). *Cobit 5*. ISA.

Jartelius, M. (2020). The 2020 Data Breach Investigations Report–a CSO's perspective. *Network Security*, *2020*(7), 9–12.

Karim, N. A., Khashan, O. A., Kanaker, H., Abdulraheem, W. K., Alshinwan, M., & Albanna, A. (2023). Online Banking User Authentication Methods: A Systematic Literature Review. *IEEE Access*.

Knechel, W. R., & Salterio, S. (2016). *Auditing: Assurance and Risk*. Taylor & Francis. https://books.google.co.id/books?id=_CklDwAAQBAJ
Lacity, M., & Willcocks, L. P. (2018). *Robotic process and cognitive automation: The next phase*. SB Publishing.
Lewis, A. (2021). *The Basics of Bitcoins and Blockchains: An Introduction to Cryptocurrencies and the Technology that Powers Them*. Mango Media. https://books.google.co.id/books?id=C8YpzgEACAAJ
Manvi, S., & Shyam, G. (2021). *Cloud Computing: Concepts and Technologies*. CRC Press. https://books.google.co.id/books?id=tPwgEAAAQBAJ
Messier Jr, W. F., Glover, S. M., & Prawitt, D. F. (2017). *Auditing & assurance services: A systematic approach*. McGraw-Hill.
Mills, A., & Haines, P. (2015). *Essential Strategies for Financial Services Compliance*. Wiley. https://books.google.co.id/books?id=1LaFCgAAQBAJ
Moeller, R. R. (2013). *Executive's Guide to COSO Internal Controls: Understanding and Implementing the New Framework*. Wiley. https://books.google.co.id/books?id=GZs3AgAAQBAJ
Moghadasi, M., Mousavi, S. M., & Fazekas, G. (2018). *Cloud computing* auditing. *International Journal of Advanced Computer Science and Applications (IJACSA)*, *9*(12).
Mohammed, D. (2015). Cybersecurity compliance in the financial sector. *Journal of Internet Banking and Commerce*, *20*(1), 1–11.
Mondschein, C. F., & Monda, C. (2019). The EU's *General Data Protection Regulation* (GDPR) in a research context. *Fundamentals of Clinical Data Science*, 55–71.
Mugo, C. (2023). Fintech-driven Financial Inclusion and Consumer Protection: Kenya's Case Study. *Available at SSRN 4318699*.
Mulder, V., Mermoud, A., Lenders, V., & Tellenbach, B. (2023). *Trends in Data Protection and Encryption Technologies*. Springer Nature Switzerland. https://books.google.co.id/books?id=KXHOEAAAQBAJ
Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Satoshi Nakamoto*.
O'brien, J. A., & Marakas, G. M. (2006). *Management information systems* (Vol. 6). McGraw-Hill Irwin New York, NY, USA:
Otero, A. R. (2020). *Information Technology Control and Audit, Fifth Edition*. Taylor & Francis Group. https://books.google.co.id/books?id=Fii5zQEACAAJ
Ozkaya, E. (2021). *Incident Response in the Age of Cloud: Techniques and best practices to effectively respond to cybersecurity incidents*.

Packt Publishing. https://books.google.co.id/books?id=hAAhEAAAQBAJ

Ozkaya, E., & Aslaner, M. (2019). *Hands-On Cybersecurity for Finance: Identify vulnerabilities and secure your financial services from security breaches*. Packt Publishing. https://books.google.co.id/books?id=CGSGDwAAQBAJ

Patel, B., Mullangi, K., Roberts, C., Dhameliya, N., & Maddula, S. S. (2019). *Blockchain*-Based Auditing Platform for Transparent Financial Transactions. *Asian Accounting and Auditing Advancement*, *10*(1), 65–80.

Peltier, T. R. (2016). *Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management*. CRC Press. https://books.google.co.id/books?id=mM_LsS-W4f4C

Phirke, A., & Ghorpade-Aher, J. (2019). Best practices of auditing in an organization using ISO 27001 standard. *Int. J. Recent Technol. Eng*, *8*(2), 691–695.

Provancha, C. A. (2019). *Kaiser Permanente: A Case Study on the Influence of Decentralized Organizational Structure on Supply Chain Transformation*. Northcentral University.

Rohan, R., Papasratorn, B., Chutimaskul, W., Hautamäki, J., Funilkul, S., & Pal, D. (2023). Enhancing Cybersecurity Resilience: A Comprehensive Analysis of Human Factors and Security Practices Aligned with the NIST Cybersecurity Framework. *Proceedings of the 13th International Conference on Advances in Information Technology*, 1–16.

Safitri, A., Syafii, I., & Adi, K. (2021). Measuring the performance of information system governance using framework COBIT 2019. *Int. J. Comput. Appl*, *174*(31), 23–30.

Saunders, A., Cornett, M. M., & Erhemjamts, O. (2021). *Financial institutions management: A risk management approach*. McGraw-Hill.

Schneier, B. (2015). *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*. W. W. Norton. https://books.google.co.id/books?id=MwF-BAAAQBAJ

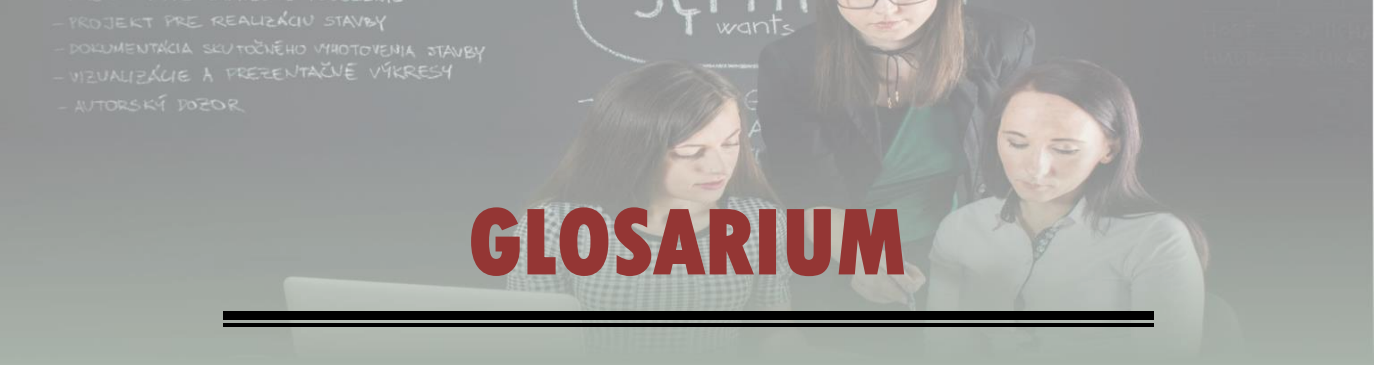
Seaman, J. (2020). *PCI DSS: An Integrated Data Security Standard Guide*. Apress. https://books.google.co.id/books?id=a-7gDwAAQBAJ

Self-Study Committee, N. C. A. (2014). *International Standards for the Professional Practice of Internal Auditing*.

Sharma, S. (2019). *Data Privacy and GDPR Handbook*. Wiley. https://books.google.co.id/books?id=Db64DwAAQBAJ

Singh, M. (2023). *Is blockchain a paradigmatic shift in accounting*

technology. RMIT University.
Stallings, W., & Brown, L. (2015). *Computer security: principles and practice*. Pearson.
Stewart, J. M., Chapple, M., & Gibson, D. (2012). *CISSP: Certified Information Systems Security Professional Study Guide*. Wiley. https://books.google.co.id/books?id=bw7WhC6ekU8C
Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards a review and comprehensive overview. *Electronics*, *11*(14), 2181.
Thompson, E. C. (2018). *Cybersecurity Incident Response: How to Contain, Eradicate, and Recover from Incidents*. Apress. https://books.google.co.id/books?id=DXhvDwAAQBAJ
Williams, B., & Adamson, J. (2022). *PCI Compliance: Understand and Implement Effective PCI Data Security Standard Compliance*. CRC Press. https://books.google.co.id/books?id=qWScEAAAQBAJ
Wirth, C., Bennett, A., & Parry, J. (2021). *Fundamentals of Finance: Financial Institutions and Markets, Personal Finance, Financial Management*. Massey University Press. https://books.google.co.id/books?id=Qpk3EAAAQBAJ
Yoo, S. (2017). *Blockchain* based financial case analysis and its implications. *Asia Pacific Journal of Innovation and Entrepreneurship*, *11*(3), 312–321.



GLOSARIUM

Analisis Proses pemeriksaan data secara mendalam untuk memahami pola, hubungan, atau tren tertentu.

Aset Sumber daya yang dimiliki oleh individu atau organisasi yang memiliki nilai ekonomi atau fungsional.

Audit Proses sistematis untuk menilai, memverifikasi, dan memastikan keandalan serta kepatuhan suatu sistem atau aktivitas terhadap standar tertentu.

COBIT Kerangka kerja internasional yang dirancang untuk membantu organisasi dalam tata kelola dan manajemen teknologi informasi.

Efisiensi Kemampuan untuk mencapai hasil yang diinginkan dengan memanfaatkan sumber daya secara optimal dan minimal.

Evaluasi Penilaian sistematis terhadap suatu sistem, proses, atau program berdasarkan kriteria tertentu.

Integritas Keadaan di mana informasi, sistem, atau proses tetap utuh, konsisten, dan dapat diandalkan.

ISO Standar internasional yang memberikan panduan dan persyaratan dalam berbagai bidang, termasuk manajemen keamanan informasi.

IT Teknologi yang mencakup perangkat keras, perangkat lunak, jaringan, dan proses yang mendukung pengolahan serta penyebaran informasi.

Kepatuhan	Tindakan memastikan suatu proses atau entitas mematuhi hukum, peraturan, dan standar yang berlaku.
Keuangan	Bidang yang berkaitan dengan pengelolaan sumber daya moneter, termasuk perencanaan, pengendalian, dan pelaporan.
Kinerja	Tingkat pencapaian suatu individu, sistem, atau organisasi terhadap target yang telah ditentukan.
Kompliansi	Pemenuhan terhadap persyaratan hukum, peraturan, atau standar yang berlaku.
Kontrol	Mekanisme atau tindakan yang diterapkan untuk mengelola risiko dan menjaga kualitas suatu sistem atau proses.
Manajemen	Proses pengelolaan sumber daya secara efektif untuk mencapai tujuan yang telah ditetapkan.
Mitigasi	Upaya untuk mengurangi dampak negatif dari risiko yang mungkin terjadi.
Organisasi	Kelompok yang terstruktur dan terkoordinasi untuk mencapai tujuan bersama melalui aktivitas tertentu.
Proses	Serangkaian langkah atau aktivitas yang dilakukan untuk menghasilkan keluaran tertentu.
Regulasi	Aturan atau kebijakan yang ditetapkan oleh pihak berwenang untuk mengatur suatu aktivitas atau sistem.
Risiko	Kemungkinan terjadinya peristiwa yang dapat memengaruhi pencapaian tujuan atau operasional secara negatif.
Teknologi	Alat, metode, atau sistem yang dikembangkan untuk mempermudah pekerjaan atau menyelesaikan masalah.

INDEKS

K

L

M

O

P

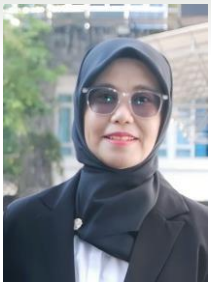
R

S

T

V

BIOGRAFI PENULIS



Dr. Susanti Usman, S.E., M.M.S.I., Akt., CA

Lahir di Jurung, 20 September 1976. Menyelesaikan studi S1 Akuntansi tahun 1998, Magister Manajemen Sistem Informasi tahun 2002 dan Program Doktor Ilmu Ekonomi Universitas Gunadarma tahun 2019 serta Program Studi Profesi Akuntan Fakultas Ekonomika dan Bisnis Universitas Gadjah Mada Bulan Agustus 2024. Sejak tahun 1999, sebagai Dosen pada Program Studi Akuntansi Universitas Gunadarma.

Dr. Syntha Noviyana, S.E., M.M.S.I., Akt., CA

Lahir di Jakarta, 26 November 1976. Menyelesaikan studi S1 Akuntansi tahun 1999, Magister Manajemen Sistem Informasi tahun 2003 dan lulus S3 di Program Doktor Ilmu Ekonomi Universitas Gunadarma tahun 2012 serta Program Studi Profesi Akuntan Fakultas Ekonomika dan Bisnis Universitas Gadjah Mada di Bulan Agustus 2024. Saat ini sebagai Dosen Tetap Universitas Gunadarma pada Fakultas Ekonomi Program Studi Akuntansi.

Dr. Dyah Mieta Setyawati, S.E., M.M.S.I., Akt., CA

Lahir di Jakarta, 24 Agustus 1977. Menyelesaikan studi S1 Akuntansi tahun 1999, Magister Manajemen Sistem Informasi tahun 2002 dan Program Doktor Ilmu Ekonomi Universitas Gunadarma tahun 2018 serta Program Pendidikan Profesi Akuntan Fakultas Ekonomika dan Bisnis UGM tahun 2022. Sejak tahun 2002, berkarya sebagai Dosen Program Studi Akuntansi Universitas Gunadarma.

Dr. Feny Fidyah, S.E., M.M.S.I., Akt., CA

Lahir di Jakarta, 10 Maret 1977. Menyelesaikan studi S1 Akuntansi tahun 2000, Magister Manajemen Sistem Informasi tahun 2005 dan Program Doktor Ilmu Ekonomi Universitas Gunadarma tahun 2019 serta Program Pendidikan Profesi Akuntan Fakultas Ekonomika dan Bisnis UGM tahun 2022. Sejak tahun 2005, sebagai Dosen Fakultas Ekonomi, Program Studi Akuntansi Universitas Gunadarma.

Buku Referensi

AUDIT IT DALAM KEUANGAN

PRAKTIK TERBAIK DAN STANDAR INTERNASIONAL

Buku referensi "Audit IT dalam Keuangan: Praktik Terbaik dan Standar Internasional" merupakan panduan komprehensif yang membahas peran penting audit teknologi informasi (IT) dalam pengelolaan keuangan modern. Dengan perkembangan teknologi yang semakin kompleks, sistem keuangan berbasis IT menghadirkan peluang sekaligus tantangan, terutama dalam aspek keamanan, keandalan, dan kepatuhan terhadap regulasi. Buku referensi ini membahas konsep dasar audit IT, standar internasional seperti COBIT dan ISO 27001, serta langkah-langkah praktis untuk menerapkannya. Dilengkapi dengan studi kasus nyata, buku referensi ini membahas tentang bagaimana audit IT dapat membantu organisasi memitigasi risiko, meningkatkan efisiensi, dan memastikan transparansi keuangan.

PT MEDIA PENERBIT INDONESIA

mediapenerbitindonesia.com
+6281362150605
Penerbit Idn
@pt.mediapenerbitidn

ISBN 978-634-7012-64-7
9 786347 012647