Dr. Siti Kurnia Rahayu, SE., M.Ak., Ak., CA

Keamanan Digital dalam Audit Pajak

Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance

UNIKOM
UNGGUL
PRESS

UNIKOM PRESS

Keamanan Digital

Dalam Audit Pajak:

Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance

Dr. Siti Kurnia Rahayu, S.E., M.Ak., Ak. CA

UNIKOM PRESS

Keamanan Digital
Dalam Audit Pajak:
Integrasi Cyber Security dengan CRM, BDA, dan BI untuk Revolusi Compliance

Penulis : Dr. Siti Kurnia Rahayu, S.E., M.Ak., Ak. CA
Penerbit UNIKOM PRESS
Jl. Dipati Ukur No.112-116, Lebakgede, Kecamatan Coblong,
Kota Bandung, Jawa Barat 40132
Web : press.unikom.ac.id

ISBN 978-602-18602-7-4

KATA PENGANTAR

Dalam menghadapi kompleksitas perubahan ekonomi global dan perkembangan teknologi informasi yang begitu pesat, perpajakan harus dapat beradaptasi dengan cepat untuk meningkatkan efisiensi serta efektivitasnya dalam mengumpulkan penerimaan negara. Audit pajak berbasis risiko telah menjadi salah satu pendekatan strategis yang banyak diterapkan oleh otoritas pajak di berbagai negara, dalam upayanya meningkatkan kepatuhan wajib pajak dan memaksimalkan penerimaan pajak.

Monograf dengan judul "Optimalisasi Audit Pajak Berbasis Risiko: Meningkatkan Kepatuhan Perpajakan dan Efisiensi Administrasi Perpajakan Melalui Integrasi Teknologi Informasi" ini merupakan sebuah upaya untuk mengeksplorasi lebih dalam tentang bagaimana integrasi teknologi informasi dapat membantu otoritas perpajakan dalam meningkatkan kinerja audit pajak berbasis risiko.

Dalam penulisan monograf ini, saya mengucapkan terima kasih kepada semua pihak yang telah memberikan dukungan, baik dalam bentuk data, masukan, kritik konstruktif, maupun saran. Khususnya kepada pihak-pihak informan yang telah berbagi pengetahuan dan pengalaman dalam proses audit, serta para ahli teknologi informasi yang telah memberikan wawasan tentang potensi teknologi dalam mendukung optimalisasi audit pajak.

Saya berharap bahwa monograf ini dapat memberikan kontribusi positif bagi pengembangan sistem administrasi pajak termasuk audit pajak di Indonesia, serta menjadi referensi yang berguna bagi para pemangku kepentingan dalam bidang perpajakan. Semoga upaya integrasi teknologi informasi dalam audit pajak dapat mewujudkan keadilan dan kepatuhan perpajakan yang lebih baik di Indonesia.

Akhir kata, saya menyadari sepenuhnya bahwa monograf ini tentu saja memiliki keterbatasan. Oleh karena

itu, segala kritik dan saran dari pembaca sangat saya nantikan demi penyempurnaan di masa mendatang.

Terima kasih.

Siti Kurnia Rahayu

DAFTAR ISI

BAB I

Transformasi Audit Pajak Melalui Integrasi dengan Cybersecurity

1.1 Revolusi Mendatang dalam Cybersecurity untuk Audit Pajak

Di era digital saat ini, interaksi antara teknologi informasi dengan berbagai sektor industri telah meredefinisi lanskap keamanan siber dan manajemen data. Audit pajak, yang tadinya hanya dianggap sebagai proses verifikasi kepatuhan finansial, kini telah berkembang menjadi bidang yang lebih kompleks dengan tantangan keamanan siber yang terus bertambah. Karena itu, integrasi keamanan siber ke dalam audit pajak menjadi sebuah keharusan yang tidak bisa diabaikan, memerlukan adaptasi dan inovasi yang berkelanjutan dalam pendekatan dan metodologinya.

Pentingnya integrasi antara audit pajak dan keamanan siber terutama terlihat dalam konteks perlindungan data sensitif. Proses audit pajak yang melibatkan pengumpulan dan analisis data finansial yang sensitif memerlukan tingkat perlindungan data yang tinggi untuk menghadapi peningkatan insiden keamanan siber. Maka dari itu, menjaga informasi keuangan perusahaan dan individu dari serangan siber, kebocoran data, dan akses tidak sah menjadi prioritas utama.

Halima et al. (2018) menyoroti pentingnya menerapkan metodologi dan kerangka kerja khusus dalam audit pajak, khususnya yang berhubungan dengan aspek keamanan siber. Studi ini menekankan pada perlunya langkah-langkah manajemen risiko yang terstruktur, yang mencakup pembuatan skenario serangan siber, penilaian risiko, penentuan potensi serangan, dan identifikasi tingkat risiko. Pendekatan ini secara signifikan meningkatkan keamanan data sensitif yang terlibat dalam proses audit pajak.

Selanjutnya, Bandara (2021) memberikan perspektif tambahan mengenai dampak keamanan siber dan kebijakan IT. Temuannya, yang berhubungan erat dengan audit pajak, menggarisbawahi pentingnya manajemen risiko keamanan siber dan penerapan kebijakan IT yang efektif sebagai langkah penting dalam melindungi data dan informasi sensitif. Hal ini memperkuat argumen untuk integrasi antara audit pajak dan keamanan siber dalam menciptakan lingkungan digital yang aman dan terproteksi.

Integrasi antara audit pajak dan keamanan siber merupakan langkah krusial, terutama dalam melindungi data sensitif. Federal Trade Commission (FTC) melaporkan hampir 90.000 kasus pencurian identitas terkait pajak tahun lalu, memperjelas risiko signifikan yang ada dalam sektor ini. IRS menyarankan beberapa langkah keamanan dan privasi, termasuk pembentukan rencana keamanan informasi yang tertulis dan penguatan kontrol internal untuk melindungi data para wajib pajak. Disarankan juga bagi praktisi pajak untuk memiliki rencana respons insiden yang komprehensif, untuk mengurangi dampak dan biaya perbaikan bila terjadi pelanggaran data.

Dalam implementasinya, sangat penting untuk memilih perangkat lunak keamanan yang andal dan merancang proses bisnis yang efektif untuk menghindari serangan siber. Faktor-faktor seperti pengelolaan administratif, keamanan fasilitas, backup dan pemulihan data, manajemen personel, serta sertifikasi sistem informasi, harus diperhatikan dalam pembangunan program keamanan informasi. Penerapan strategi keamanan ini oleh otoritas pajak tidak hanya meningkatkan perlindungan data finansial tetapi juga memastikan kepatuhan terhadap beragam regulasi dan standar keamanan siber, yang esensial untuk menjaga integritas dan kepercayaan publik dalam proses audit pajak.

Kepatuhan terhadap regulasi merupakan aspek kritis dalam integrasi antara keamanan siber dan audit pajak. Regulasi seperti GDPR di Eropa telah menetapkan standar untuk perlindungan data finansial, dan integrasi keamanan siber dalam audit pajak memastikan pemenuhan terhadap standar ini, sekaligus menghindari potensi denda dan sanksi. Anette Choii (2020) menekankan peran penting Manajemen Risiko Kepatuhan dalam penerapan hukum pajak yang efektif, menunjukkan bahwa langkah-langkah manajemen risiko, termasuk penerapan teknologi terbaru, sangat relevan untuk meningkatkan kepatuhan dan efisiensi operasional dalam audit pajak.

Pentingnya kepatuhan terhadap regulasi erat kaitannya dengan pengelolaan risiko dan kontroversi pajak. Survei EY Tax Risk and Controversy 2023 mengungkapkan bahwa 84% dari eksekutif pajak dan keuangan di 47 yurisdiksi mengakui peningkatan signifikan dalam nilai implementasi atau peningkatan kerangka kerja global untuk

manajemen risiko dan kontroversi pajak. Hal ini menjadi semakin penting mengingat ekspektasi akan peningkatan jumlah dan intensitas audit sebesar 79% dalam dua tahun mendatang dibandingkan dengan periode sebelumnya. Luis Coronado dari EY Global menyoroti bahwa tata kelola pajak yang kuat dan efektif kini menjadi keharusan bagi bisnis, mencakup strategi tata kelola pajak yang ditingkatkan, transformasi pendekatan pengelolaan data pajak dan keuangan, serta penggunaan teknologi khusus untuk mengumpulkan dan menilai risiko pajak, mengelola kontrol pajak, dan memantau sengketa yang sedang berlangsung.

Permintaan informasi yang lebih sering dan detail dari otoritas pajak mendorong kegiatan audit pajak, dengan lebih dari setengah (56%) eksekutif pajak dan keuangan mengantisipasi peningkatan jumlah dan intensitas audit sebagai akibat dari permintaan informasi yang lebih banyak atau detail serta persyaratan transparansi dan pengungkapan yang meningkat. Oleh karena itu, integrasi keamanan siber dalam audit pajak menjadi sangat penting untuk memastikan kepatuhan terhadap regulasi yang semakin ketat, mengelola risiko terkait pertukaran informasi antar otoritas pajak, dan memastikan kesiapan audit, terutama dalam konteks transfer pricing dan persyaratan baru yang ditetapkan oleh Pillar Two (EY Americas, 2023).

1.2 Strategi Responsif dan Adaptif dalam Cybersecurity untuk Audit Pajak

Peningkatan kepercayaan dan kredibilitas stakeholder merupakan hasil langsung dari kemampuan organisasi untuk melindungi data keuangan dari serangan cyber.

Bandara (2021) menyatakan bahwa pengelolaan risiko keamanan siber yang efektif dalam institusi berdampak positif pada kepercayaan stakeholder. Konsep serupa berlaku dalam audit pajak, di mana kepercayaan dan kredibilitas organisasi meningkat seiring dengan keamanan informasi yang efektif. Peningkatan kepercayaan dan kredibilitas stakeholder merupakan hasil langsung dari kemampuan organisasi untuk melindungi data keuangan dari serangan cyber. Laporan 'Cyber Trust Insights' KPMG (2022) menekankan bahwa membangun dan melindungi kepercayaan kini menjadi bagian integral dari cara bisnis beroperasi dan berinteraksi dengan stakeholder. Lebih dari 80% eksekutif menyadari pentingnya peningkatan keamanan siber dan perlindungan data untuk mengamankan kepercayaan stakeholder. Keamanan siber dan perlindungan data termasuk mengenali pentingnya Chief Information Security Officers (CISOs) sebagai pembangun kepercayaan digital, dengan perannya yang perlu berkembang untuk mendukung organisasi dalam menghadapi tantangan keamanan siber yang semakin meningkat dan standar regulasi yang semakin ketat. Peningkatan kepercayaan ini berdampak positif pada keuntungan, retensi, dan hubungan yang lebih kuat. Inovasi, retensi talenta juga menjadi mungkin jika organisasi mengakui bahwa kepercayaan digital penting. Dalam konteks audit pajak, ini berarti bahwa kepercayaan dan kredibilitas otoritas pajak meningkat seiring dengan keamanan informasi yang efektif, memberikan dampak positif tidak hanya dalam hal kepatuhan dan perlindungan data, tetapi juga dalam memperkuat hubungan dengan wajib pajak dan stakeholder lainnya (KPMG, 2022).

Peningkatan peran pemerintah dalam keamanan siber, dari hanya melindungi jaringan publik menjadi mengkoordinasi keamanan di seluruh ekosistem publik-swasta, penting untuk mengamankan baik jaringan publik maupun swasta. Pusat Keamanan Siber Nasional Inggris, misalnya, telah dibentuk untuk memberikan respons nasional yang terpadu terhadap ancaman dan serangan siber, mendukung sektor publik, swasta, dan umum. Ekosistem keamanan siber, yang terdiri dari hubungan antar lembaga, memerlukan berbagi informasi dan penentuan norma perilaku. Kolaborasi dan pengambilan keputusan bersama semakin meningkat di setiap tingkatan, dari tingkat internasional hingga lokal. CSIRTAmericas, komunitas tim respons insiden keamanan komputer di wilayah Amerika, berbagi informasi dan pengetahuan secara real-time. Di Belanda, organisasi dari pemerintah, bisnis, sektor pengetahuan, dan pendidikan tinggi telah bergabung membentuk Delta Keamanan Hague, sebuah badan kerjasama yang bekerja untuk inovasi dalam keamanan. Peningkatan kepercayaan ini merupakan hasil langsung dari kemampuan untuk melindungi data keuangan dan operasional dari serangan siber, memperkuat hubungan dengan wajib pajak dan stakeholder lainnya, dan menunjukkan komitmen terhadap keamanan siber yang efektif di era digital (Junaideen et al., 2021).

Efisiensi operasional dalam audit pajak dapat ditingkatkan melalui penerapan prinsip-prinsip cybersecurity. Teknologi seperti enkripsi data dan analisis big data mempercepat dan meningkatkan akurasi pengolahan data pajak. Aspek yang dibahas termasuk pentingnya manajemen risiko keamanan siber dalam menjaga kerahasiaan, integritas, dan ketersediaan data, yang

sangat relevan dengan konteks menjaga integritas proses audit pajak dari manipulasi data atau penipuan pajak. Anette Choii (2020) menunjukkan bahwa Manajemen Risiko Kepatuhan, termasuk penerapan teknologi terkini, krusial untuk penegakan hukum pajak yang efektif. Hal ini menegaskan pentingnya integrasi inovasi teknologi dan cybersecurity dalam mencapai efisiensi operasional yang lebih tinggi dalam audit pajak. Kemampuan untuk responsif terhadap ancaman cyber yang berkembang dan kompleks merupakan aspek penting lainnya. Otoritas pajak di seluruh dunia sedang mendigitalisasi sistem administrasi pajak untuk memungkinkan integrasi dengan wajib pajak dan penilaian real-time di ekonomi global saat ini. Teknologi ini memungkinkan otoritas pajak untuk mengumpulkan dan mengelola data pajak lebih efisien, menggunakan proses analitik canggih untuk menemukan anomali dan menargetkan kinerja audit pajak. Kolaborasi antara otoritas pajak nasional, yang dikoordinasikan oleh OECD, juga menjadi bagian penting dalam peningkatan efisiensi operasional digitalisasi sistem administrasi. Hal ini memungkinkan berbagi pendekatan dan praktik terbaik, memperkaya sumber data untuk berbagai aktivitas audit dan penegakan hukum. Melalui penggunaan teknologi ini, otoritas pajak dapat meningkatkan keamanan data, meminimalkan risiko manipulasi data atau penipuan pajak, serta meningkatkan kepatuhan dan efisiensi operasional dalam proses audit pajak (Junaideen, 2021).

Halima et al. (2018) dan Bandara (2021) secara kolektif menunjukkan pentingnya cybersecurity yang adaptif dan responsif sebagai bagian integral dari strategi audit pajak modern. Pendekatan ini mengurangi risiko kerugian finansial dan kerusakan reputasi, menekankan pentingnya

responsivitas terhadap dinamika ancaman cyber yang terus berubah. Dalam audit pajak, pentingnya cybersecurity yang adaptif dan responsif dalam mengurangi risiko kerugian finansial dan kerusakan reputasi sangat ditekankan. Menurut KPMG, terjadi peningkatan serangan cyber di berbagai industri, termasuk dalam sektor keuangan, yang menuntut perubahan pendekatan dalam audit IT untuk mencakup penilaian risiko cybersecurity. Hal ini termasuk pemahaman yang lebih baik tentang ancaman cyber, fokus pada tata kelola, proses, dan keamanan teknis dalam sistem IT. Metodologi 'Cyber in the Audit' (CitA) dari KPMG dikembangkan untuk mengelola risiko yang mengancam kerahasiaan, integritas, dan ketersediaan fasilitas penyimpanan dan pengolahan data. Metodologi ini mendukung audit IT dengan menguji ukuran keamanan siber yang mendeteksi dan mencegah pengabaian Kontrol Aplikasi IT dan Kontrol IT Umum. Faktor-faktor yang perlu dipertimbangkan auditor saat melakukan penilaian risiko cyber termasuk ancaman spesifik industri, risiko pihak ketiga, lanskap regulasi, ancaman internal, dan peningkatan otomatisasi. Hasil penilaian risiko cyber ini kemudian diintegrasikan ke dalam rencana audit keseluruhan untuk menentukan dampaknya pada laporan keuangan dan kontrol internal. Pilihan pengambilan sampel atau pengujian substantif dari bukti yang bersumber secara digital dari sistem yang terkena pelanggaran tergantung pada analisis dampak ini. Dengan demikian, penerapan cybersecurity yang adaptif dan responsif dalam audit pajak di otoritas pajak tidak hanya mengurangi risiko keuangan dan reputasi, tetapi juga meningkatkan kepatuhan terhadap standar dan regulasi yang berlaku, serta memastikan integritas dan keakuratan proses audit pajak (Backer, 2022).

Organisasi, termasuk institusi keuangan, sering menghadapi ancaman cyber yang mencakup intrusi cybersecurity, penipuan, dan kejahatan finansial seperti pencucian uang, penyuapan, dan penggelapan pajak. Pada tahun 2016, saat hacker mencoba mencuri US$1 miliar dari Bank Bangladesh, menunjukkan betapa pentingnya keamanan informasi dalam transaksi finansial internasional. Menurut Laporan Investigasi Pelanggaran Data Verizon (2021), keuntungan finansial tetap menjadi motivasi utama untuk serangan cyber. Laporan ini mengungkapkan bahwa meskipun pengeluaran untuk produk dan layanan keamanan siber meningkat, jumlah kejahatan terkait belum melambat dan malah meningkat. Hal ini menekankan pentingnya pendekatan terintegrasi dalam manajemen risiko, di mana organisasi harus melihat ketiga jenis risiko - cybersecurity, penipuan, dan kejahatan finansial - sebagai ancaman terpadu terhadap perusahaan. Integrasi ini dapat menghemat biaya, mengurangi hambatan di antara kontrol, dan memungkinkan inovasi, serta telah terbukti mengurangi risiko yang terkait dengan cybercrime. Pendekatan terpadu ini sangat relevan dengan otoritas pajak, di mana kepercayaan dan keamanan informasi sangat penting. Dengan menerapkan prinsip-prinsip keamanan siber yang adaptif dan responsif, otoritas pajak dapat lebih efektif melindungi data keuangan dan mengurangi risiko keuangan serta kerusakan reputasi, dengan tetap responsif terhadap dinamika ancaman cyber (Chawla, 2022).

1.3 Menanggapi Ancaman Meningkat dan Perlindungan Data

Cybersecurity telah menjadi fokus utama, terutama mengingat peristiwa-peristiwa terkini yang menyoroti kerentanan sistem terhadap serangan siber. Fenomena seperti aksi pembocoran data oleh hacker Bjorka, serangan ransomware pada Direktorat Jenderal Pajak (DJP), dan serangan phishing yang terkait dengan pelaporan SPT Pajak Tahunan menunjukkan betapa pentingnya pengamanan data dalam lingkungan pajak. Fenomena tersebut bukan hanya soal menjaga keamanan data wajib pajak, tetapi juga tentang mempertahankan kepercayaan publik dalam sistem pajak yang integritasnya kini sedang diuji ketahanannya. Respons pemerintah terhadap ancaman ini, termasuk kerjasama dengan Badan Siber dan Sandi Negara (BSSN) dan pembentukan satuan tugas keamanan data, merupakan langkah-langkah penting yang mencerminkan keseriusan dalam menanggapi tantangan cybersecurity ini.

Dalam audit pajak, pentingnya cybersecurity menjadi lebih jelas saat melihat dampak dari serangan siber yang telah terjadi. Integrasi strategi cybersecurity dalam audit pajak bukan lagi pilihan, melainkan kebutuhan. Kajian yang fokus pada integrasi ini tidak hanya relevan, tetapi juga vital untuk mengembangkan solusi yang bisa mengatasi ancaman nyata yang dihadapi. Studi dan evaluasi terkait hal ini dapat membantu dalam mengidentifikasi kelemahan dalam protokol keamanan yang ada, mengevaluasi efektivitas regulasi seperti Undang-Undang Perlindungan Data Pribadi, dan mengembangkan strategi pencegahan yang lebih efektif terhadap serangan phishing dan social engineering. Hal

tersebut tentang upaya untuk memastikan bahwa sistem pajak tidak hanya efisien, tetapi juga aman dan tahan terhadap ancaman siber yang semakin meningkat.

Data terkini mengenai insiden keamanan siber menyoroti perlunya integrasi kuat cybersecurity dalam audit pajak. Tahun lalu, biaya rata-rata pelanggaran data mencapai rekor tertinggi, $4,35 juta, dengan biaya rata-rata serangan ransomware sebesar $4,54 juta. Rata-rata, memerlukan waktu 277 hari untuk mengidentifikasi dan menangani pelanggaran. Lebih dari separuh organisasi mengalami serangan siber tahun lalu, dengan 75% melaporkan peningkatan insiden keamanan. Ancaman internal berperan dalam 43% pelanggaran, dengan 94% malware dikirim melalui email. Frekuensi serangan hacker sangat tinggi, dengan rata-rata 26.000 serangan per hari, dan diperkirakan akan ada 15,4 juta serangan DDoS tahun ini. Data ini menggarisbawahi pentingnya perlindungan data dalam konteks audit pajak, mengingat biaya dan prevalensi serangan yang meningkat (Garza, 2023).

Menurut International Monetary Fund (IMF), ancaman siber terhadap sistem keuangan, termasuk sektor pajak, semakin meningkat, dengan kebutuhan kerja sama global yang mendesak untuk melindunginya. Pada tahun 2016, hacker menargetkan bank sentral Bangladesh dan mengeksploitasi kerentanan dalam sistem pesan pembayaran elektronik global SWIFT, mencoba mencuri $1 miliar. Kejadian ini menunjukkan bahwa risiko siber sistemik dalam sistem keuangan telah diremehkan secara serius. Kekhawatiran utama adalah serangan yang merusak integritas data keuangan, seperti catatan, algoritma, dan transaksi. Aktor jahat di balik serangan ini mencakup pelaku kriminal yang semakin berani dan negara atau aktor yang

didukung negara. Korea Utara telah mencuri sekitar $2 miliar dari setidaknya 38 negara dalam lima tahun terakhir. Untuk mengatasi masalah ini, Carnegie Endowment for International Peace, bekerja sama dengan World Economic Forum, mengeluarkan laporan yang merekomendasikan tindakan spesifik untuk mengurangi fragmentasi dengan mendorong kolaborasi yang lebih besar, baik secara internasional maupun di antara lembaga pemerintah, perusahaan keuangan, dan perusahaan teknologi (Maurer & Nelson 2021).

1.4 Inovasi Teknologi dan Cybersecurity dalam Audit Pajak

Penggunaan analitik data diharapkan dapat meningkatkan kualitas dan efisiensi audit, dengan memungkinkan analisis volume data yang besar untuk mengidentifikasi pola dan anomali, termasuk pendeteksian penipuan. Selain itu, pertimbangan cybersecurity dalam proses audit menjadi semakin penting, yang melibatkan penilaian efektivitas langkah-langkah keamanan siber, termasuk perlindungan data sensitif, sistem, dan jaringan. Auditor harus menilai kecukupan kontrol internal klien terkait cybersecurity dan mengidentifikasi kelemahan yang dieksploitasi oleh pelaku cybercrime.

Penggunaan teknologi cloud juga mengalami peningkatan, memberikan keamanan data yang lebih baik, kolaborasi antar tim yang lebih efisien, dan aksesibilitas data secara real-time. Hal ini memungkinkan auditor untuk melakukan pekerjaan audit secara remote, mengurangi biaya perjalanan dan pertemuan tatap muka. Fokus pada otomatisasi audit juga semakin meningkat, dengan

pemanfaatan teknologi untuk tugas-tugas audit yang repetitif dan berbiaya rendah, seperti pengumpulan data, analisis, dan generasi laporan. Hal ini mengurangi risiko kesalahan dan memungkinkan auditor untuk lebih fokus pada tugas bernilai tinggi seperti analisis dan interpretasi temuan audit. Keseluruhan, masa depan audit pajak dalam ranah cybersecurity diharapkan akan lebih otomatis, terintegrasi, dan aman, dengan penekanan pada penggunaan teknologi canggih untuk meningkatkan efisiensi dan efektivitas proses audit (Ramaswamy, 2023).

Integrasi keamanan siber dalam audit pajak, mendapat peningkatan signifikan melalui pemanfaatan Compliance Risk Management, Big Data Analytics, dan Business Intelligence. Manajemen Risiko Kepatuhan memfokuskan pada identifikasi, evaluasi, dan manajemen risiko yang berkaitan dengan kepatuhan pajak. Keamanan siber berperan krusial dalam melindungi data dan sistem dari ancaman eksternal yang dapat mengganggu integritas data pajak dan proses audit. Anette Choii (2020) menyajikan analisis tentang penerapan Manajemen Risiko Kepatuhan oleh otoritas pajak untuk mendukung penerapan hukum pajak secara efektif, termasuk dalam audit pajak. Artikel ini mendetailkan bagaimana berbagai langkah dalam CRM, seperti identifikasi dan evaluasi risiko kepatuhan, pengembangan, dan implementasi strategi mitigasi risiko, serta penggunaan teknologi terkini dan pendekatan berbasis data, dapat memperkuat kepatuhan dan meningkatkan efisiensi dalam audit pajak.

Farooq (2023) mengungkapkan pentingnya BDA. Teknologi analitik data memfasilitasi auditor pajak untuk menganalisis pernyataan keuangan dengan lebih akurat dan

efisien, yang vital dalam mendeteksi kecurangan dan ketidaksesuaian dalam informasi keuangan. Hal ini memperkuat kontrol internal dan integritas sistem pelaporan keuangan. Implementasi BDA dalam administrasi pajak mengurangi risiko kecurangan dan kesalahan, meningkatkan kepatuhan pajak, dan memperbaiki kualitas audit. Selain itu, integrasi BDA dalam cybersecurity memperkuat sistem keamanan informasi dalam organisasi pajak. Alat BI dan analitik data besar berperan penting dalam upaya keamanan dan pencegahan penipuan, yang mempengaruhi integritas dan keandalan sistem pelaporan keuangan. Farooq (2023) menekankan bahwa penggunaan yang tepat dari alat BI dan BDA dapat meningkatkan akurasi dan efisiensi sistem pelaporan keuangan, mendukung proses pengambilan keputusan manajemen, dan memastikan bahwa data yang digunakan dalam audit pajak dilindungi dari ancaman siber, meningkatkan kepercayaan publik terhadap administrasi pajak. Pendekatan ini menunjukkan potensi peran BI dalam menguatkan proses audit pajak dan menjaga keamanan data, serta menegaskan pentingnya adaptasi dan kecermatan dalam penerapan teknologi ini.

Anette Choii (2020) menyatakan kebutuhan untuk mengembangkan metodologi yang lebih efektif untuk mengidentifikasi dan menilai risiko kepatuhan dalam lingkungan yang sangat digital dan cepat berubah. Selain itu, ada urgensi dalam penerapan strategi mitigasi risiko yang inovatif dan adaptif yang dapat menjawab dinamika baru dalam kepatuhan pajak, serta evaluasi dampak teknologi baru pada perilaku kepatuhan pajak. Peningkatan penggunaan data dan analitik canggih dalam CRM untuk memprediksi dan mencegah perilaku non-kepatuhan pajak juga disoroti sebagai area kajian lebih lanjut yang dapat

mendukung peningkatan kepatuhan pajak dan efektivitas audit pajak. In Lee (2020) menyoroti kesenjangan dalam kerangka kerja manajemen risiko siber yang komprehensif untuk mengatasi masalah keamanan siber yang kompleks di sistem IoT, khususnya terkait perangkat medis IoT.

1.5 Optimasi Audit Pajak Global

Integrasi cybersecurity dalam audit pajak di Singapura, seperti yang dilaksanakan oleh Otoritas Pendapatan Dalam Negeri Singapura (IRAS), dapat menjadi benchmark dalam memadukan teknologi canggih dan keamanan data. IRAS menerapkan 'e-Audit', sebuah inisiatif yang menggabungkan protokol keamanan siber ketat, berhasil mendeteksi kebocoran data di perusahaan besar pada 2021 dan menanggapi dinamika regulasi dan ancaman siber yang terus berkembang dengan pelatihan tim auditnya. Implementasi ini telah menarik perhatian internasional, memposisikan Singapura sebagai pemimpin dalam praktik audit pajak yang aman dan efektif, menggambarkan bahwa integrasi keamanan siber yang efektif dapat meningkatkan kepercayaan publik dan efisiensi audit pajak (Cybersecurity Act, 2018).

Berbagai negara telah mengadopsi integrasi cybersecurity dalam audit pajak melalui AI dan analisis data, seperti Norwegia yang memperbaiki efisiensi audit VAT, Perancis yang meningkatkan pendapatan pajak sebesar 11 miliar Euro pada 2019 melalui AI, dan Chile serta Peru yang memanfaatkan AI untuk analisis transaksi pajak. Kolombia, Kosta Rika, Brazil, Inggris Raya, Finlandia, dan Kanada juga mengimplementasikan sistem serupa untuk meningkatkan akurasi dan efisiensi dalam proses audit pajak, menunjukkan

pentingnya teknologi dalam mengamankan data keuangan (Collosa, 2020). Penerapan AI dan cybersecurity dalam audit pajak oleh berbagai negara menunjukkan pentingnya teknologi dalam meningkatkan efisiensi dan keamanan. Norwegia, dengan peningkatan efisiensi audit VAT, dan Perancis, yang meningkatkan pendapatan pajaknya secara signifikan, membuktikan keefektifan AI dalam mengidentifikasi ketidaksesuaian. Chile dan Peru menggunakan AI untuk menganalisis transaksi pajak, meningkatkan akurasi dan pengawasan. Kolombia, Kosta Rika, Brazil, Inggris Raya, Finlandia, dan Kanada juga telah mengimplementasikan teknologi serupa, menggarisbawahi pentingnya cybersecurity dalam menjaga integritas data keuangan. Singapura, khususnya dengan 'e-Audit' IRAS, telah berhasil mendeteksi kebocoran data dan merespons dinamika ancaman siber, menunjukkan bagaimana integrasi cybersecurity dapat memperkuat kepercayaan publik dan efisiensi dalam audit pajak. Kesimpulannya, penggunaan AI dan cybersecurity dalam audit pajak tidak hanya mengoptimalkan proses tetapi juga memberikan lapisan keamanan tambahan yang sangat penting dalam era digital saat ini.

Salah satu isu penting adalah menemukan keseimbangan antara keamanan dan privasi. Teknologi baru memungkinkan otoritas pajak untuk melakukan analisis data yang lebih cepat dan otomatis, mengurangi kesalahan dan menghemat waktu. Namun, teknologi ini juga membawa ketidakpastian terkait dengan sejauh mana otomatisasi dapat digunakan tanpa melanggar hak privasi. General Data Protection Regulation (GDPR) Uni Eropa telah memperkenalkan ketentuan baru tentang cara individu dapat diprofilkan. Meskipun teknologi yang digunakan oleh

administrasi pajak untuk manajemen risiko dan analitik data lanjutan dapat menimbulkan kesulitan dalam hal ini, penggunaannya dalam bidang pajak dibenarkan oleh kebutuhan untuk menjaga kepentingan publik. Namun, keamanan hak privasi wajib pajak tetap perlu dijaga (Luisa Scarcella, 2019).

1.6 Investasi dan Inovasi dalam Cybersecurity untuk Meningkatkan Efisiensi Audit Pajak

Mengenai biaya implementasi teknologi cybersecurity, terdapat faktor-faktor yang mempengaruhi besaran investasi yang dibutuhkan. Rata-rata, sebuah bisnis perlu mengalokasikan antara 0,2% hingga 0,9% dari pendapatannya untuk cybersecurity, dengan biaya per karyawan berkisar antara $1,300 hingga $3,000. Deloitte mencatat bahwa industri keuangan rata-rata menghabiskan 10% dari anggaran TI-nya untuk cybersecurity. Ukuran perusahaan juga menentukan biaya cybersecurity, di mana perusahaan besar seperti Microsoft menghabiskan sekitar $1 miliar untuk inisiatif ini. Tipe data yang ditangani, seperti data yang tunduk pada regulasi kepatuhan seperti HIPAA atau PCI, dan volume layanan cybersecurity yang digunakan juga mempengaruhi biaya. Pertanyaan tentang apakah biaya ini sepadan dengan manfaatnya terutama relevan di negara-negara dengan sumber daya terbatas, mengingat variasi kebutuhan dan anggaran yang ada (Chancey, 2021).

Membahas efektivitas praktik integrasi cybersecurity dalam audit pajak, faktor-faktor penting termasuk pendirian dan pengelolaan Cybersecurity Operations Center (CSOC). CSOC vital untuk struktur perusahaan apapun, menggabungkan sumber daya terampil, praktik terbaik, dan solusi teknologi untuk deteksi yang tepat waktu, pemantauan real-time, dan respons terhadap ancaman siber. Namun, mendirikan CSOC merupakan komitmen besar yang memerlukan investasi modal substansial dan komitmen untuk mengelola sumber daya teknis yang terampil. Efektivitas CSOC bergantung pada perencanaan yang efektif, investasi yang bijak, pengelolaan sumber daya, prosedur yang terdokumentasi, dan infrastruktur yang dirancang dengan baik. CSOC juga harus melaporkan Key Performance Indicators (KPI) yang sesuai dengan standar dan kerangka kerja seperti ISO 27001/27002, NIST SP 800-53, PCI DSS, FFIEC, dan HIPAA. Meskipun investasi dalam tim, alat, dan aplikasi cybersecurity penting, teknologi saja tidak cukup. Keseimbangan harus dicapai antara investasi dalam pelatihan karyawan, alat-alat cyber, dan kebijakan untuk memastikan perusahaan berada dalam posisi optimal untuk merespons ancaman siber. AI dalam cybersecurity belum cukup matang untuk menggantikan kecerdasan manusia (Putrus, 2021).

Dalam konteks audit pajak, integrasi cybersecurity menjadi sangat penting mengingat peningkatan data keuangan yang diproses secara digital. Teknologi baru memungkinkan otoritas pajak melakukan analisis data yang efisien, namun menimbulkan tantangan dalam menjaga privasi. Aturan seperti GDPR Uni Eropa memberikan pedoman tentang bagaimana data pribadi dapat diproses, memastikan bahwa kepentingan publik dan privasi wajib

pajak seimbang. Biaya implementasi teknologi ini signifikan, terutama di negara-negara dengan sumber daya terbatas. Untuk menjawab tantangan ini, pendirian CSOC menjadi kunci. CSOC menggabungkan sumber daya manusia dan teknologi untuk merespons ancaman siber secara efektif, meskipun dengan investasi yang besar. Keseimbangan antara penggunaan teknologi dan pelatihan karyawan juga penting, mengingat keterbatasan AI dalam menggantikan kecerdasan manusia dalam aspek-aspek tertentu dari keamanan siber.

Kolaborasi antar-agensi merupakan aspek krusial dalam memperkuat cybersecurity dalam audit pajak, di mana perusahaan seringkali melibatkan tim audit internal untuk mengevaluasi kontrol internal, mengatur risiko, dan merampingkan operasi. Tim IT dan audit internal, masing-masing dengan tanggung jawab dan fokus yang berbeda, harus bekerja sama dalam kerangka strategi cybersecurity yang lebih luas. Efektivitas kolaborasi ini tergantung pada kepercayaan dan koordinasi antar tim, dan melibatkan langkah-langkah seperti menyelaraskan bahasa, meningkatkan komunikasi, dan berbagi tujuan data. Tujuan utama dari kolaborasi ini adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan data sensitif, serta mengurangi kemungkinan penipuan, memahami jenis dan lokasi data sensitif, dan mengembangkan pendekatan sistematis dalam manajemen risiko dan proses control (Fineberg et al, 2021).

Teknologi masa depan seperti quantum computing diharapkan memberikan dampak besar pada cybersecurity dalam audit pajak, dengan potensi merevolusi pemodelan pajak, resolusi audit, dan deteksi penipuan. Kemampuannya untuk melakukan perhitungan triliunan kali lebih cepat dari

komputer konvensional memungkinkan analisis pajak yang lebih dalam dan deteksi anomali yang lebih efektif. Inisiatif seperti Quantum Computing Cybersecurity Preparedness Act di AS menyoroti pentingnya mengamankan data terhadap ancaman quantum. Walaupun quantum computing berpotensi meningkatkan efisiensi audit pajak dan deteksi penipuan, ada juga risiko penyalahgunaan oleh organisasi kriminal, memicu perlombaan senjata teknologi dengan otoritas pajak (EY Global, 2023).

Regulasi internasional memainkan peran penting dalam cybersecurity audit pajak, dengan regulator layanan keuangan mengidentifikasi risiko cyber sebagai ancaman utama terhadap stabilitas keuangan. Hal ini mendorong inisiatif mitigasi risiko dan ketahanan melawan ancaman cyber yang canggih, serta memperkuat pengelolaan identitas dan akses untuk mencegah pengambilalihan akun. Regulasi penting seperti Executive Order 14208 di AS menuntut peningkatan keamanan siber, dan ada penekanan yang berkembang pada perlindungan privasi data pelanggan dengan prinsip "privacy by design". Peraturan yang akan datang diharapkan meningkatkan tindakan perlindungan data, seperti yang tercermin dalam California Privacy Rights Act yang akan menggantikan CCPA pada 2023, menekankan perlindungan data lanjutan dan audit cyber (KPMG, 2022).

Big Data Analytic (BDA) dan Business Intelligence (BI) memainkan peran krusial dalam pengelolaan data keuangan yang sensitif, menjadikan keamanan siber sebagai prioritas utama. Pentingnya menjaga integritas dan kerahasiaan data ini tidak bisa diremehkan, mengingat risiko besar yang terkait dengan kebocoran atau manipulasi data. Untuk menjamin keamanan ini, sistem BDA dan BI harus dilindungi

dari berbagai risiko keamanan siber. Evaluasi keamanan terhadap sistem BDA dan BI sangat penting untuk mengungkap celah keamanan yang mungkin dieksploitasi oleh pelaku siber. Identifikasi celah ini memungkinkan penerapan langkah-langkah pencegahan yang tepat, mencegah potensi serangan sebelum terjadi. Hal ini adalah langkah penting dalam membangun pertahanan yang kuat terhadap ancaman siber yang selalu berkembang. Selanjutnya, analisis data dari BDA dan BI memberikan wawasan penting yang bisa digunakan untuk mengidentifikasi risiko keamanan siber lebih awal. Dengan wawasan ini, Direktorat Jenderal Pajak (DJP) dapat mengambil tindakan proaktif untuk mencegah insiden keamanan, bukan sekadar merespons setelah insiden terjadi. Penggunaan data ini juga memungkinkan DJP untuk mengoptimalkan strategi keamanan siber, sehingga melindungi organisasi dari serangan siber yang semakin canggih dan beragam. Penerapan strategi mitigasi berbasis data merupakan pendekatan efektif dalam mengatasi risiko keamanan siber yang dihadapi oleh DJP. Rekomendasi strategis yang dibangun atas dasar data nyata dan analisis risiko akan lebih akurat dalam menargetkan ancaman siber spesifik. Strategi ini sangat penting untuk memastikan keamanan proses audit pajak dari manipulasi dan penipuan siber, memperkuat integritas seluruh proses. Memahami dampak insiden keamanan siber terhadap audit pajak membantu DJP untuk meningkatkan respons terhadap ancaman serupa di masa depan. Selain itu, pemanfaatan BDA dan BI dalam mengatasi tantangan keamanan siber bisa meningkatkan kinerja dan efisiensi audit.

1.7 Identifikasi Masalah

Identifikasi masalah dalam keamanan digital audit pajak dalam integrasi cyber security dengan teknologi lanjutan dapat dirumuskan sebagai berikut:

1) Evaluasi dampak isu keamanan siber terhadap kinerja audit pajak. Menilai bagaimana insiden keamanan siber dan kerentanan sistem informasi pajak dapat mempengaruhi akurasi, waktu, dan keandalan proses audit pajak.
2) Evaluasi bagaimana Compliance Risk Management (CRM) yang dilindungi dari risiko keamanan siber, dimanfaatkan dalam audit pajak. Menyelidiki perlindungan cyber security pada sistem CRM yang digunakan dalam audit pajak untuk memastikan kepatuhan dan mengurangi risiko keamanan siber.
3) Investigasi terhadap bagaimana sistem Business Development Analytics (BDA) dan Business Intelligence (BI) saat ini dilindungi dari risiko keamanan siber, serta identifikasi potensi kerentanan yang dimanfaatkan dalam audit pajak. Menganalisis keamanan siber pada sistem BDA dan BI yang mendukung audit pajak, termasuk identifikasi celah keamanan yang dieksploitasi.
4) Pengembangan strategi mitigasi BDA, BI, dan CRM untuk meningkatkan keamanan siber dan integritas audit pajak. Merumuskan strategi mitigasi risiko keamanan siber untuk sistem BDA, BI, dan CRM yang mendukung audit pajak.
5) Merumuskan rekomendasi kebijakan untuk mengembangkan kerangka kerja keamanan siber yang

berorientasi pada hasil analitik dari BDA dan BI serta CRM.

BAB II

Eksplorasi Literatur

Audit Pajak dan Keamanan Siber

2.1 Pengenalan Keamanan Siber

2.1.1 Pengertian Keamanan Siber

Keamanan siber merupakan sebuah area kritis yang memfokuskan pada perlindungan infrastruktur digital dan informasi yang terhubung melalui internet. Di era digital yang terus berkembang ini, pentingnya keamanan siber menjadi semakin signifikan, mengingat peningkatan ancaman siber yang terus-menerus mengintai integritas sistem informasi dan privasi pengguna. Dalam konteks ini, keamanan siber dapat didefinisikan melalui berbagai perspektif dan pendekatan.

Wong (2007) mendefinisikan keamanan siber sebagai inisiatif peningkatan kualitas yang diadopsi oleh organisasi untuk memantau dan memastikan integritas sistem terhadap entri yang tidak sah. Hal ini menekankan pentingnya pemantauan aktif dan pencegahan untuk melindungi aset digital.

Seemma, Nandhini, & Sowmiya (2018) memperluas definisi ini dengan menyatakan bahwa keamanan siber melibatkan teknik yang dirancang untuk mempertahankan dan melindungi lingkungan siber tertentu dari serangan potensial. Pendekatan ini menggarisbawahi pentingnya

strategi pertahanan yang adaptif untuk melawan ancaman yang terus berkembang.

Menurut Shea, Gills, & Clark (tanpa tahun), keamanan siber mencakup perlindungan jaringan, perangkat lunak, dan perangkat keras dari ancaman dunia maya. Hal ini menunjukkan bahwa keamanan siber adalah upaya holistik yang melibatkan berbagai aspek teknologi informasi.

Reddy & Reddy (2014) menambahkan bahwa keamanan siber adalah proses penerapan teknologi, praktik terbaik, kebijakan, dan sumber daya manusia. Pendekatan ini menyoroti pentingnya kolaborasi antara teknologi dan manusia dalam melindungi infrastruktur sensitif.

Akhirnya, Abomhara & Koien (2015) serta Craigen, Diakub-Thibault, & Purse (2014) mengidentifikasi keamanan siber sebagai kumpulan praktik terbaik dan pengorganisasian sumber daya untuk melindungi ruang siber. Peneliti ini mengakui bahwa langkah-langkah keamanan siber harus dikembangkan untuk melawan ancaman baik dari dalam maupun luar organisasi.

Dari berbagai perspektif ini, jelas bahwa keamanan siber merupakan sebuah bidang yang kompleks dan multidisipliner. Hal ini mengharuskan pemahaman mendalam tentang ancaman siber, serta penerapan strategi pertahanan yang efektif untuk melindungi aset digital dan informasi sensitif. Dalam kajian pustaka ini, penting untuk mengakui berbagai definisi dan pendekatan keamanan siber sebagai dasar untuk memahami dan mengatasi ancaman siber dalam konteks audit pajak.

2.1.2 Komponen Keamanan Siber

Pemahaman mendalam mengenai komponen keamanan siber menjadi krusial dalam mengembangkan dan menerapkan strategi keamanan yang efektif. Setiap komponen keamanan siber memainkan peran penting dalam menciptakan pertahanan yang komprehensif terhadap berbagai ancaman dunia maya. Komponen Keamanan Siber (Amos, 2022) meliputi:

1) Keamanan Jaringan
   Keamanan jaringan adalah pondasi dasar dalam strategi keamanan siber, yang berfokus pada perlindungan jaringan perusahaan dari ancaman dan serangan jahat. Keamanan jaringan ini mencakup penerapan firewall, sistem deteksi dan pencegahan intrusi, serta enkripsi untuk menjaga integritas dan privasi data yang ditransfer melalui jaringan. Keamanan jaringan memastikan bahwa akses tidak sah diblokir, dan data perusahaan tetap aman dari tangan yang salah.
2) Keamanan Aplikasi
   Keamanan aplikasi menekankan pada pentingnya pengujian dan pembaruan berkelanjutan untuk memastikan bahwa aplikasi yang digunakan oleh organisasi tidak memiliki celah keamanan. Keamanan aplikasi ini melibatkan pemeriksaan kode sumber, penggunaan alat otomatis untuk mendeteksi kerentanan, dan penerapan patch keamanan secara teratur. Dengan keamanan aplikasi yang kuat, organisasi dapat mengurangi risiko eksploitasi melalui aplikasi yang dikembangkan atau gunakan.
3) Keamanan Titik Akhir

Dengan meningkatnya tren bekerja dari jarak jauh, keamanan titik akhir menjadi semakin penting. Komponen ini bertujuan untuk melindungi perangkat individu yang terhubung ke jaringan perusahaan, seperti komputer, laptop, dan perangkat mobile, dari serangan perangkat lunak jahat dan ancaman lainnya. Keamanan titik akhir memastikan bahwa semua perangkat yang memiliki akses ke jaringan perusahaan aman, sehingga mencegah pencurian data melalui titik lemah sistem.

4) Keamanan Data

Keamanan data berkaitan dengan perlindungan informasi sensitif, baik itu data perusahaan maupun data pelanggan. Keamanan data mencakup enkripsi data, pengendalian akses yang ketat, dan penerapan kebijakan keamanan data untuk mencegah akses atau penggunaan data tanpa izin. Keamanan data memastikan bahwa informasi kritikal terlindung dari kebocoran dan eksploitasi.

5) Keamanan Cloud

Seiring dengan adopsi cloud computing yang luas, keamanan cloud menjadi elemen penting dalam keamanan siber. Keamanan cloud melibatkan perlindungan data dan aplikasi yang disimpan di lingkungan cloud dari ancaman dunia maya. Hal ini mencakup penerapan kebijakan akses yang ketat, enkripsi data, dan penggunaan layanan keamanan cloud yang disediakan oleh vendor cloud. Dengan keamanan cloud yang efektif, organisasi dapat memanfaatkan fleksibilitas dan skalabilitas cloud computing dengan aman.

2.1.2.1 Keamanan Jaringan

Keamanan jaringan merupakan aspek kritikal dalam pengelolaan risiko keamanan siber dan bertindak sebagai garis pertahanan pertama terhadap ancaman siber. Keamanan jaringan ini mencakup serangkaian teknologi, perangkat, dan proses yang dirancang untuk melindungi integritas, kerahasiaan, dan ketersediaan data dan jaringan perusahaan. Keamanan jaringan menangani perlindungan infrastruktur jaringan serta informasi yang dikirimkan melalui jaringan terhadap berbagai jenis serangan siber.

Keamanan jaringan sangat penting karena jaringan perusahaan menjadi semakin kompleks dan terbuka terhadap lebih banyak ancaman dan kerentanan. Dengan peningkatan konektivitas internet dan penggunaan aplikasi berbasis cloud, jaringan perusahaan harus dilindungi dari berbagai jenis serangan, seperti malware, ransomware, phishing, dan serangan man-in-the-middle. Keamanan jaringan yang efektif memastikan bahwa aset dan data perusahaan dilindungi, memungkinkan operasi bisnis berjalan lancar dan meminimalkan risiko kerusakan reputasi dan kerugian finansial.

Komponen Utama Keamanan Jaringan:

A. Firewall

Menurut Cheswick dan Bellovin (2003), firewall didefinisikan sebagai s**istem atau perangkat yang dirancang untuk memblokir akses yang tidak sah ke atau dari jaringan.** Firewall memiliki beberapa fungsi utama, yaitu:

- memeriksa setiap paket data yang masuk dan keluar dari jaringan dan memutuskan apakah paket tersebut boleh melewati atau tidak.
- membantu mencegah serangan, seperti serangan denial-of-service (DoS), spoofing IP, dan phishing.

- membantu melindungi data sensitif, seperti data pribadi atau keuangan, dari akses yang tidak sah.

Firewall bekerja dengan menggunakan aturan yang menentukan paket data mana yang boleh melewati firewall dan mana yang tidak. Aturan ini dapat didasarkan pada berbagai faktor, seperti yang dijelaskan Kurose dan Ross (200) yaitu Firewall dapat memblokir lalu lintas dari alamat IP tertentu, memblokir lalu lintas yang menggunakan port tertentu, dan memblokir lalu lintas yang menggunakan protokol tertentu.

B. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS)

Sistem Deteksi Intrusi (IDS) dan Sistem Pencegahan Intrusi (IPS) adalah teknologi penting yang memonitor lalu lintas jaringan untuk aktivitas mencurigakan. Sistem Deteksi dan Pencegahan Intrusi (IDS/IPS) adalah teknologi keamanan jaringan yang dirancang untuk memonitor dan menganalisis aktivitas jaringan untuk mendeteksi dan mencegah aktivitas berbahaya (Kruegel, et al, 2004).

IDS berfungsi dengan mendeteksi upaya intrusi dan memberi tahu administrator jaringan, sedangkan IPS melangkah lebih jauh dengan secara otomatis mengambil tindakan untuk mencegah atau memblokir serangan tersebut (McClure et al., 2005).

C. Enkripsi

Enkripsi adalah proses mengubah informasi menjadi bentuk yang tidak terbaca, yang disebut ciphertext, dengan menggunakan algoritma dan kunci tertentu. Ciphertext ini hanya dapat diubah kembali menjadi informasi asli (plaintext) dengan menggunakan kunci yang sesuai (Menezes, 2018). Tujuan Enkripsi menurut Stallings (2017):

- melindungi informasi sensitif dari akses oleh pihak yang tidak berwenang.
- membantu memastikan bahwa data tidak diubah atau dimanipulasi selama transmisi, serta data tidak dirusak atau dihapus.

Dalam keamanan jaringan, enkripsi digunakan untuk mengamankan data in transit antara perangkat di jaringan, sehingga menjaga informasi sensitif dari pengintaian atau penyadapan oleh pihak yang tidak berwenang.

2.1.2.2 Keamanan Aplikasi

Keamanan data berkaitan dengan perlindungan informasi sensitif, baik itu data perusahaan maupun data pelanggan. Keamanan data mencakup enkripsi data, pengendalian akses yang ketat, dan penerapan kebijakan keamanan data untuk mencegah akses atau penggunaan data tanpa izin. Keamanan data memastikan bahwa informasi kritikal terlindung dari kebocoran dan eksploitasi.

Keamanan data yang efektif memerlukan kombinasi berbagai komponen utama menurut Whitman dan Mattord (2014) terdiri dari:

1) Kerahasiaan
    - Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
    - Menetapkan hak akses yang ketat untuk membatasi siapa yang dapat mengakses data.
    - Mengkategorikan data berdasarkan tingkat sensitivitasnya untuk menentukan tingkat perlindungan yang diperlukan.
2) Integritas
    - Memastikan bahwa data akurat dan konsisten.
    - Membuat salinan data teratur untuk pemulihan jika terjadi kehilangan atau kerusakan data.

- Memastikan bahwa perubahan data dilakukan dengan cara yang terotorisasi dan terdokumentasi.

3) Ketersediaan
   - Menyimpan data di beberapa lokasi untuk memastikan aksesibilitas jika terjadi kegagalan sistem.
   - Memiliki rencana untuk memulihkan data dan sistem jika terjadi bencana.
   - Memastikan sistem dan jaringan tersedia untuk pengguna saat dibutuhkan.
4) Keamanan fisik
   - Melindungi infrastruktur fisik dari akses tidak sah.
   - Membatasi akses ke perangkat keras dan media penyimpanan data.
   - Menjaga suhu, kelembaban, dan kondisi lingkungan lainnya yang optimal untuk perangkat keras.
5) Keamanan operasional
   - Menginstal patch keamanan terbaru untuk sistem operasi dan perangkat lunak.
   - Melatih karyawan tentang praktik keamanan data terbaik.
   - Melakukan audit berkala untuk mengidentifikasi dan mengatasi kerentanan keamanan.
6) Manajemen risiko
   - Mengidentifikasi dan menilai risiko yang terkait dengan data.
   - Memahami potensi dampak dari setiap risiko.
   - Menerapkan langkah untuk mengurangi risiko.

2.1.2.3 Keamanan Titik Akhir

Dengan meningkatnya tren bekerja dari jarak jauh, keamanan titik akhir menjadi semakin penting. Komponen ini bertujuan untuk melindungi perangkat individu yang terhubung ke jaringan perusahaan, seperti komputer, laptop, dan perangkat mobile, dari serangan perangkat lunak jahat dan ancaman lainnya. Keamanan titik akhir memastikan bahwa semua perangkat yang memiliki akses ke jaringan perusahaan aman, sehingga mencegah pencurian data melalui titik lemah sistem.

Keamanan titik akhir yang efektif memerlukan kombinasi berbagai komponen utama yang perlu dipertimbangkan menurut Cole (2021):

1) Perangkat lunak antivirus dan anti-malware
    - Melindungi perangkat dari virus, malware, dan ransomware.
    - Memindai file, email, dan web traffic untuk mencari ancaman.
    - Menghapus atau mengkarantina ancaman yang ditemukan.
2) Firewall
    - Memblokir akses yang tidak sah ke perangkat dan jaringan.
    - Mengontrol traffic jaringan masuk dan keluar.
    - Melindungi dari serangan seperti port scanning dan denial-of-service attacks.
3) Sistem deteksi intrusi (IDS) dan sistem pencegahan intrusi (IPS)
    - Memantau aktivitas jaringan untuk mendeteksi dan mencegah aktivitas berbahaya.
    - Mengidentifikasi pola dan anomali yang mungkin mengindikasikan serangan.

- Mengirimkan alert kepada administrator keamanan jika terjadi aktivitas mencurigakan.

4) Enkripsi data
   - Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
   - Melindungi data saat disimpan di perangkat atau transit di jaringan.
   - Mencegah pencurian data jika perangkat hilang.
5) Pengendalian akses
   - Menetapkan hak akses yang ketat untuk membatasi siapa yang dapat mengakses perangkat dan data.
   - Memastikan bahwa hanya pengguna yang sah yang dapat mengakses informasi sensitif.
   - Mencegah penyalahgunaan data.
6) Pembaruan perangkat lunak
   - Menginstal patch keamanan terbaru untuk sistem operasi dan perangkat lunak.
   - Memperbaiki kerentanan yang dapat dieksploitasi oleh penyerang.
   - Menjaga perangkat dan data tetap aman.
7) Manajemen risiko
   - Mengidentifikasi dan menilai risiko yang terkait dengan keamanan titik akhir.
   - Memahami potensi dampak dari setiap risiko.
   - Menerapkan langkah- untuk mengurangi risiko.

2.1.2.4 Keamanan Data

Keamanan data berkaitan dengan perlindungan informasi sensitif, baik itu data perusahaan maupun data pelanggan. Keamanan data mencakup enkripsi data, pengendalian akses yang ketat, dan penerapan kebijakan keamanan data untuk mencegah akses atau penggunaan data

tanpa izin. Keamanan data memastikan bahwa informasi kritikal terlindung dari kebocoran dan eksploitasi. Keamanan data yang efektif memerlukan kombinasi berbagai komponen utama menurut Whitman & Mattord (2014) yang perlu dipertimbangkan:

1) Kerahasiaan
    - Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi.
    - Menetapkan hak akses yang ketat untuk membatasi siapa yang dapat mengakses data.
    - Mengkategorikan data berdasarkan tingkat sensitivitasnya untuk menentukan tingkat perlindungan yang diperlukan.
2) Integritas
    - Memastikan bahwa data akurat dan konsisten.
    - Membuat salinan data secara teratur untuk pemulihan jika terjadi kehilangan/kerusakan data.
    - Memastikan bahwa perubahan data dilakukan dengan cara yang terotorisasi dan terdokumentasi.
3) Ketersediaan
    - Menyimpan data di beberapa lokasi untuk memastikan aksesibilitas jika terjadi kegagalan sistem.
    - Memiliki rencana untuk memulihkan data dan sistem jika terjadi bencana.
    - Memastikan sistem dan jaringan tersedia untuk pengguna saat dibutuhkan.

2.1.2.5 Keamanan Cloud

Seiring dengan adopsi cloud computing yang luas, keamanan cloud menjadi elemen penting dalam keamanan siber. Keamanan cloud melibatkan perlindungan data dan aplikasi yang disimpan di lingkungan cloud dari ancaman dunia maya. Hal ini mencakup penerapan kebijakan akses yang ketat, enkripsi data, dan penggunaan layanan keamanan cloud yang disediakan oleh vendor cloud. Dengan keamanan cloud yang efektif, organisasi dapat memanfaatkan fleksibilitas dan skalabilitas cloud computing dengan aman.

Keamanan cloud adalah seperangkat praktik dan teknologi yang dirancang untuk melindungi data, aplikasi, dan infrastruktur yang disimpan di lingkungan cloud dari berbagai ancaman siber (Rittinghouse & Ransome, 2010).

Fungsi utama keamanan cloud (Cloud Security Alliance (CSA):

- Keamanan cloud membantu memastikan bahwa data sensitif yang disimpan di cloud terlindungi dari akses yang tidak sah, kebocoran, dan pencurian.
- Keamanan cloud membantu organisasi memenuhi berbagai peraturan dan standar kepatuhan yang terkait dengan keamanan data.
- Keamanan cloud membantu meningkatkan keandalan dan ketersediaan layanan cloud dengan melindungi dari downtime dan gangguan layanan.
- Keamanan cloud membantu organisasi mengurangi risiko kerugian finansial dan reputasi akibat serangan siber.

Komponen Utama Keamanan Cloud Cloud Security Alliance (CSA):

- Menetapkan hak akses ketat untuk membatasi siapa yang dapat mengakses data dan aplikasi di cloud.
- Mengubah data menjadi format yang tidak dapat dibaca tanpa kunci dekripsi untuk melindungi data saat transit dan saat disimpan di cloud.
- Mengelola identitas pengguna dan akses ke sumber daya cloud.
- Vendor cloud menawarkan berbagai layanan keamanan cloud, seperti firewall aplikasi web, solusi anti-malware, dan layanan deteksi intrusi.
- Memantau aktivitas di lingkungan cloud untuk mendeteksi dan merespon terhadap ancaman siber.
- Memastikan bahwa layanan cloud dapat terus beroperasi bahkan ketika terjadi gangguan.

2.1.3 Strategi Cybersecurity dalam Era Konektivitas

2.1.3.1 Konektivitas dan Interoperabilitas

Dalam dekade terakhir, transisi monumental dalam teknologi informasi dan komunikasi telah secara fundamental mengubah paradigma hidup, bekerja, dan berinteraksi manusia. Era ini ditandai oleh penciptaan lingkungan digital yang terhubung secara luas, seperti yang diungkapkan oleh Vishik et al. (2016), yang menyoroti ledakan jumlah perangkat yang terhubung ke internet. Integrasi antara domain komputasi dan jaringan, yang sebelumnya beroperasi secara independen, telah melahirkan ekosistem digital yang kompleks, didukung oleh konektivitas dan interoperabilitas tanpa batas. Dalam konteks ini, infrastruktur global saling terkait mendukung

beragam fungsi mulai dari pusat data hingga penggunaan sensor sekali pakai, mendorong efisiensi dan inovasi.

Keberagaman perangkat yang terhubung ini tidak hanya membuka peluang baru bagi pengguna teknologi dan ekonomi tetapi juga menimbulkan tantangan signifikan dalam konteks keamanan siber. Konektivitas universal dan interoperabilitas memperluas permukaan serangan, membuat analisis ancaman dan kerentanan menjadi lebih kompleks. Sistem dan elemen infrastruktur yang saling terhubung sering kali memiliki tingkat perlindungan yang tidak merata, memperbesar risiko keamanan dalam lingkungan teknologi yang luas ini.

Sementara perkembangan teknologi informasi dan komunikasi membuka jalan bagi era baru konektivitas dan interoperabilitas, kompleksitas dan tantangan keamanan siber yang dihasilkan memerlukan pendekatan yang lebih nuansa dan kritis dalam pembentukan kebijakan dan regulasi. Memastikan keamanan siber dalam lingkungan global yang terhubung erat tidak hanya tentang melindungi infrastruktur teknologi tetapi juga tentang mempertahankan integritas dan fungsi ekonomi global.

A. Tantangan Keamanan Siber

Perluasan eksponensial dalam konektivitas dan interoperabilitas ini, sementara memberikan peluang baru untuk pertumbuhan teknologi dan ekonomi, juga menimbulkan tantangan keamanan siber yang signifikan. Vishik et al. (2016) menggambarkan bagaimana permukaan serangan yang diperluas dan kompleksitas sistem yang meningkat mempersulit analisis ancaman dan kerentanan. Infrastruktur teknologi yang saling terkait sering kali menampilkan tingkat perlindungan yang tidak merata, meningkatkan risiko keamanan siber secara keseluruhan.

B. Keamanan Siber Permukaan Serangan yang Diperluas

Salah satu tantangan utama dalam lingkungan teknologi yang terhubung erat ini adalah eskalasi permukaan serangan yang disebabkan oleh prevalensi konektivitas dan interoperabilitas. Setiap perangkat yang terhubung menjadi potensi titik masuk untuk serangan siber, menantang integritas dari infrastruktur teknologi yang luas dan heterogen. Kompleksitas jaringan dan diversifikasi teknologi memperumit implementasi standar keamanan yang kohesif, memperbesar potensi kerentanan terhadap eksploitasi siber.

C. Kebijakan dan Regulasi

Pembuatan kebijakan menjadi penting untuk mendukung konektivitas dan interoperabilitas untuk mengatasi tantangan keamanan yang muncul. Vishik et al. (2016) menyoroti pentingnya kebijakan standar, peraturan keamanan jaringan dan informasi, serta perlindungan data dalam mendukung interoperabilitas global. Kebijakan yang menghambat sifat terbuka internet, seperti lokalisasi data atau ketergantungan pada standar lokal, dapat menghambat interoperabilitas global dan membatasi potensi internet sebagai mesin pertumbuhan ekonomi.

Konektivitas dan interoperabilitas yang meluas meningkatkan permukaan serangan, mempersulit penerapan standar keamanan yang konsisten. Hal ini menuntut strategi pertahanan mendalam yang mencakup langkah-langkah teknis dan organisasi/administratif. Pembuatan kebijakan yang efektif menjadi krusial untuk mendukung interoperabilitas global dan mengatasi tantangan keamanan, memastikan bahwa kebijakan tidak menghambat sifat terbuka internet dan potensi pertumbuhan ekonomi.

2.1.3.2 Respons terhadap Kompleksitas dan Dinamisme

Lingkungan teknologi yang sangat kompleks dan dinamis membutuhkan pendekatan kebijakan yang dinamis dan adaptif, yang dapat merespons terhadap perkembangan teknologi dan tantangan keamanan dengan efektivitas tinggi. Kebijakan harus cukup fleksibel untuk menyesuaikan dengan berbagai model keamanan dan kerangka kerja dalam lingkungan teknologi yang kompleks, mendorong kolaborasi antara sektor publik dan privat.

A. Kompleksitas Lingkungan Teknologi

Lingkungan teknologi modern, dengan konektivitas dan interoperabilitasnya yang luas, membawa kompleksitas intrinsik dan dinamisme yang signifikan. Kerangka kerja operasional yang membentuk dasar dari lingkungan teknologi ini sering kali mengandung kerentanan yang belum teridentifikasi, sebagai hasil dari pengaruh komposisi model keamanan yang beragam. Vishik et al. (2016) menggambarkan kompleksitas ini sebagai karakteristik dominan dari proses multi-domain yang saat ini umum digunakan, di mana sejumlah domain teknis berkolaborasi untuk mencapai satu operasi. Meskipun tujuannya seragam, kapasitas keamanan dalam setiap tahapan proses tersebut bisa sangat berbeda.

Proses multi-domain ini, dirancang untuk mencapai tujuan operasional tertentu, sering kali menampilkan tingkat kerentanan yang bervariasi, yang membuat analisis risiko dan penerapan kontrol keamanan menjadi tantangan. Kerumitan ini tidak hanya terbatas pada teknologi dan proses, tetapi juga merambah ke data dan perlindungan data, menuntut pemikiran ulang tentang konsep-konsep mendasar seperti anonimitas dan interoperabilitas data.

B. Dampak Kompleksitas pada Kebijakan Siber

Kompleksitas lingkungan komputasi ini merupakan hasil dari agregasi berbagai kerangka kerja serta model keamanan dan privasi yang dirancang secara terpisah. Vishik et al. (2016) menekankan bahwa pemahaman mendalam tentang kompleksitas ini sangat penting dalam memberikan masukan yang relevan untuk pengembangan kebijakan siber yang efektif. Seringkali, pembuat kebijakan menanggapi permasalahan keamanan siber pada tingkat yang sangat sederhana, membuat generalisasi yang tidak mencerminkan kemampuan teknologi kompleks yang terus berkembang.

Kebijakan yang dibuat harus bersifat netral terhadap teknologi, menurut Wikia ('Technology Neutrality'), namun juga harus memperhatikan karakteristik utama dari lingkungan teknologi untuk mengintegrasikan hubungan penting antara norma dan praktik terbaik dalam keamanan siber. Hal ini menuntut pendekatan yang lebih dinamis dan adaptif dalam pembuatan kebijakan, yang dapat merespons terhadap perubahan teknologi dan tantangan keamanan dengan lebih efektif.

C. Kebijakan yang Responsif terhadap Kompleksitas dan Dinamisme

Pendekatan kebijakan yang responsif terhadap kompleksitas dan dinamisme lingkungan teknologi harus mempertimbangkan beberapa faktor kunci:

- Kebijakan harus mampu beradaptasi dengan pengembangan teknologi baru dan tidak menghambat inovasi.
- Kebijakan perlu cukup fleksibel untuk menyesuaikan dengan berbagai model keamanan dan kerangka kerja yang berbeda-beda dalam lingkungan teknologi yang kompleks.

- Menggunakan pendekatan berlapis dalam keamanan siber, yang mempertimbangkan aspek fisik, logis, dan perilaku dalam menyusun strategi keamanan.
- Mendorong kolaborasi antara sektor publik dan privat dalam pembuatan kebijakan untuk memastikan bahwa perspektif yang luas diintegrasikan dalam pendekatan keamanan.

2.1.3.3 Pembauran Komponen Siber dan Fisik

Dalam keamanan siber, pembauran antara komponen siber dan fisik mengambil peran kritikal, terutama melalui pengembangan dan implementasi Sistem Cyber-Fisik (CPS). CPS merupakan integrasi dari sistem komputasi, komunikasi, dan fisik yang beroperasi secara terkoordinasi untuk mengontrol proses fisik dengan cara yang cerdas dan efisien. Konsep ini, seperti yang didefinisikan oleh Cyber-Physical Systems Public Working Group, menunjukkan bagaimana dunia maya dan lingkungan fisik tidak hanya saling terhubung tetapi juga saling bergantung.

A. Kompleksitas Keamanan dalam CPS

CPS, yang kini terintegrasi dalam berbagai aspek kehidupan kita, dari infrastruktur kritikal hingga perangkat konsumen, memperkenalkan tingkat kompleksitas baru dalam keamanan dan manajemen risiko. Tantangan unik muncul dari kebutuhan untuk memastikan keselamatan, ketahanan, keandalan, keamanan, dan privasi dalam satu sistem terintegrasi. Dalam CPS, domain-domain ini yang biasanya dipisahkan menjadi saling terkait dan tidak dapat lagi dianalisis secara terpisah tanpa mengabaikan risiko keseluruhan sistem.

Penilaian risiko yang terfragmentasi pada salah satu domain dapat secara tidak sengaja meningkatkan kerentanan dalam domain lain, menunjukkan kebutuhan untuk pendekatan holistik dalam manajemen risiko. Misalnya, optimasi terhadap keandalan dalam pengaturan kontrol fisik mungkin mengurangi keamanan siber jika tidak diperhatikan dengan seksama.

B. Kompleksitas dengan Kolaborasi Multidisiplin

Untuk mengatasi risiko yang ditimbulkan oleh pembauran komponen siber dan fisik, diperlukan kolaborasi yang erat antara tim kebijakan dan teknologi dari berbagai disiplin ilmu. Pendekatan multidisiplin ini memungkinkan pembuatan norma keamanan yang kompleks yang mencakup berbagai domain risiko, memastikan bahwa tidak ada aspek penting yang terlewatkan. Penggunaan alat seperti ontologi yang diusulkan dapat mendukung agregasi dan analisis berbagai bidang risiko, memfasilitasi pengembangan kebijakan dan praktik terbaik yang komprehensif dan terpadu.

Pengembangan dan implementasi Sistem Cyber-Fisik (CPS) menyoroti pembauran antara komponen siber dan fisik, memperkenalkan kompleksitas baru dalam keamanan dan manajemen risiko. Pendekatan multidisiplin dalam pengembangan norma keamanan yang mencakup berbagai domain risiko menjadi penting untuk memastikan keselamatan, ketahanan, keandalan, keamanan, dan privasi dalam sistem terintegrasi.

2.1.3.4 Infrastruktur Global Bersama Berdasarkan Standar Terbuka

Infrastruktur global bersama dan standar terbuka memainkan peran kunci dalam memfasilitasi interoperabilitas dan konektivitas tanpa batas. Namun, distribusi keahlian dan sumber daya yang tidak merata menekankan pentingnya peningkatan kapasitas keamanan siber untuk memastikan perlindungan yang konsisten dan efektif. Koordinasi upaya di tingkat global dan pengembangan kapasitas di negara-negara dengan sumber daya terbatas menjadi krusial.

A. Pentingnya Infrastruktur Global dan Standar Terbuka

Infrastruktur global bersama dan standar terbuka memainkan peran kunci dalam memfasilitasi interoperabilitas dan konektivitas tanpa batas di seluruh dunia. Keuntungan dari sistem semacam itu adalah universal; memungkinkan perangkat, aplikasi, jaringan, dan proses untuk beroperasi secara konsisten di berbagai negara dan lintas benua, menciptakan bahasa universal untuk teknologi. Standar terbuka mendukung inovasi dan pertumbuhan ekonomi dengan memudahkan pengembangan dan adopsi teknologi baru.

1) Interoperabilitas dan Konektivitas
    - Perangkat, aplikasi, jaringan, dan proses dapat beroperasi secara konsisten di berbagai negara dan lintas benua.
    - Manfaat:
        - Meningkatkan efisiensi dan produktivitas.
        - Memperluas jangkauan dan akses ke informasi dan layanan.

- Mendorong inovasi dan kolaborasi global.

2) Standar Terbuka

Standar yang tersedia global tanpa batasan.

Manfaat:

- Meningkatkan interoperabilitas dan kompatibilitas.
- Mempercepat inovasi dengan memungkinkan pengembangan teknologi baru yang kompatibel dengan standar yang ada.
- Meningkatkan pilihan dan kompetisi bagi konsumen.

B. Tantangan dalam Infrastruktur Bersama

Meskipun infrastruktur global bersama menawarkan banyak manfaat, distribusi keahlian dan sumber daya yang tidak merata di seluruh dunia menciptakan ketidakuniforman dalam tingkat keamanan siber dan perlindungan privasi. Infrastruktur ini digunakan oleh berbagai sektor, termasuk pendidikan, transportasi, dan energi, serta oleh berbagai wilayah geografis, yang semuanya bergantung pada fungsi sistem dan proses yang sama. Variabilitas dalam tingkat keamanan siber menekankan pentingnya terus meningkatkan kapasitas di bidang ini untuk memastikan perlindungan yang konsisten dan efektif terhadap ancaman siber NIST.

1) Keamanan Siber

- Distribusi keahlian dan sumber daya yang tidak merata. Negara-negara dengan sumber daya terbatas mungkin memiliki tingkat keamanan siber yang lebih rendah. Hal ini dapat membuat infrastruktur global rentan terhadap serangan siber.

- Mencakup berbagai teknologi dan sistem dari berbagai vendor. Hal ini dapat membuat infrastruktur sulit diamankan dan dikelola.
- Ancaman siber yang terus berkembang. Serangan siber menjadi semakin canggih dan sulit dideteksi.

2) Perlindungan Privasi.
   - Pengumpulan dan penggunaan data pribadi. Infrastruktur global dapat digunakan untuk mengumpulkan dan menggunakan data pribadi dari berbagai sumber.
   - Hal ini menimbulkan kekhawatiran tentang privasi dan keamanan data.
   - Ketidakpatuhan terhadap peraturan privasi. Negara-negara memiliki peraturan privasi yang berbeda-beda. Hal ini dapat membuat perusahaan sulit untuk mematuhi semua peraturan yang berlaku.

C. Kebijakan dan Inisiatif untuk Penguatan Infrastruktur

Untuk mengatasi tantangan ini, penting bagi para pembuat kebijakan dan ahli teknologi untuk bekerja sama dalam mengembangkan strategi yang dapat meningkatkan keamanan siber di seluruh infrastruktur global. Inisiatif ini termasuk:

- Mengkoordinasikan upaya di tingkat global untuk memastikan bahwa standar keamanan siber yang kuat diterapkan secara universal.
- Memfokuskan pada pembangunan kapasitas di negara-negara dengan sumber daya terbatas untuk meningkatkan tingkat keamanan siber dan perlindungan privasi.

- Mendorong pengembangan dan adopsi standar terbuka yang mendukung keamanan siber, memungkinkan integrasi lebih mudah dari teknologi keamanan terbaru.
- Menyebarkan kesadaran mengenai keamanan siber untuk meningkatkan kemampuan individu dan organisasi dalam melindungi diri dari ancaman siber.

Integrasi antara kebijakan keamanan yang komprehensif dan pendekatan yang responsif terhadap kompleksitas dan dinamisme lingkungan teknologi menawarkan strategi efektif untuk mengatasi tantangan keamanan siber saat ini. Pendekatan berlapis, yang mencakup kebijakan dan regulasi yang mendukung, pembauran komponen siber dan fisik, serta penguatan infrastruktur global melalui standar terbuka, menjadi kunci untuk melindungi data penting organisasi dalam era konektivitas dan interoperabilitas yang semakin meningkat.

2.2 Urgensi Keamanan Siber dalam Audit Pajak

2.2.1 Konsep Keamanan Siber dalam Audit Pajak

Konsep keamanan siber dalam konteks audit pajak mencakup serangkaian strategi, teknologi, dan prosedur yang dirancang untuk melindungi sistem, jaringan, dan data dari ancaman siber. Keamanan siber berperan dalam audit pajak, mengingat pentingnya menjaga keamanan data dan transaksi pajak dari berbagai risiko seperti kebocoran informasi, penipuan, dan gangguan operasional.

Menghadapi ancaman siber yang meningkat dan berubah-ubah, penting bagi komite audit dan dewan direksi untuk memiliki ekspektasi yang jelas terhadap audit internal dalam memahami dan mengevaluasi bagaimana organisasi mengelola risiko terkait keamanan siber. Hal ini mengindikasikan pentingnya keterlibatan auditor dengan keahlian teknis yang mendalam dan pemahaman terkini mengenai lingkungan risiko yang ada, seperti diungkapkan oleh Deloitte (2017).

Pendekatan yang komprehensif dalam mengevaluasi kerangka kerja keamanan siber sangat diperlukan, yang melibatkan tidak hanya seleksi item spesifik tapi juga pemahaman menyeluruh terhadap kondisi saat ini, arah strategis organisasi, dan standar keamanan siber yang diharapkan di industri atau sektor terkait. Evaluasi ini bertujuan untuk memastikan bahwa praktik keamanan siber yang diadopsi tidak hanya memenuhi ekspektasi minimum tapi juga sejalan dengan tujuan dan arah strategis organisasi, sebagaimana dijelaskan oleh Deloitte (2017).

Integrasi manajemen risiko siber ke dalam proses pengambilan keputusan dan operasional sehari-hari menandai lapisan pertama pertahanan sebuah organisasi. Diikuti oleh peran penting pemimpin manajemen risiko informasi dan teknologi sebagai lapisan kedua, yang bertanggung jawab untuk menetapkan kerangka tata kelola dan pengawasan, memonitor aktivitas keamanan, serta mengambil langkah-langkah korektif bila diperlukan. Pentingnya keamanan siber dalam audit pajak sebagai alat untuk menjaga integritas, kerahasiaan, dan ketersediaan data pajak, mendorong pendekatan yang lebih holistik dan

berbasis risiko terhadap keamanan siber, sebagaimana disarankan oleh Deloitte (2017).

Meningkatnya risiko keamanan siber, karena semakin banyak data keuangan dan non-keuangan yang disimpan secara digital. Tren ini menyebabkan peningkatan signifikan dalam insiden siber, mendorong perusahaan untuk berinvestasi dalam pengelolaan risiko keamanan siber dan pengungkapan terkait. AICPA telah mengeluarkan kerangka kerja untuk pelaporan sukarela tentang upaya pengelolaan risiko keamanan siber (Eaton, et al, 2019).

1) Akuntan memainkan peran penting di semua tahapan pengelolaan risiko keamanan siber yang efektif, termasuk identifikasi dan pengukuran risiko, desain dan pengujian sistem kontrol, pelaporan eksternal, dan jaminan independen. Keahlian di bidang ini sangat penting untuk mengelola dan melaporkan risiko keamanan siber secara efektif.
2) Proses ini melibatkan identifikasi dan prioritasasi risiko keamanan siber, desain dan implementasi kontrol untuk mengurangi risiko ini, serta pemantauan efektivitas kontrol tersebut. Akuntan sangat instrumental dalam proses ini, menggunakan pengetahuan tentang kontrol internal dan IT/keamanan siber. Akuntan juga memainkan peran penting dalam pelaporan keamanan siber eksternal dan memberikan jaminan independen atas laporan ini.
3) Lanskap keamanan siber yang berkembang menawarkan peluang signifikan bagi akuntan. Firma akuntansi semakin diakui atas keahlian dalam keamanan siber dan termasuk di antara yang teratas di bidang ini. Keterlibatan dalam pengelolaan risiko

keamanan siber mencakup kapasitas penasehat dan jaminan, memanfaatkan pengetahuan dalam kontrol internal, pelaporan eksternal, dan jaminan.

2.2.2 Memperkuat Audit Pajak

2.2.2.1 Memperkuat Audit Pajak dalam Menghadapi Serangan Siber

Audit pajak merupakan proses kritis yang menuntut pemeriksaan mendetail atas catatan keuangan entitas, dimana keandalan dan keamanan informasi yang diaudit menjadi sangat penting. Di era digital saat ini, data pajak yang sering disimpan dan diproses secara elektronik menjadi sangat rentan terhadap serangan siber. Keamanan siber dalam konteks audit pajak adalah langkah penting dalam melindungi data dan sistem dari serangan atau akses ilegal. Pentingnya keamanan siber terutama relevan karena semakin banyak aktivitas bisnis, termasuk audit pajak, yang dilakukan secara digital. Tanpa langkah keamanan yang tepat, data sensitif bisa dicuri dan operasi bisnis dapat terganggu.

Cyber security pada dasarnya mengacu pada praktik yang memastikan kerahasiaan, integritas, dan ketersediaan informasi, yang dikenal sebagai CIA Triad. Jenis serangan siber termasuk malware, injeksi SQL, phishing, serangan Man-in-the-Middle, dan serangan Denial-of-Service. Malware adalah perangkat lunak berbahaya yang menyebar melalui email atau unduhan. Injeksi SQL digunakan untuk mengambil kontrol dan mencuri data dari database. Phishing adalah teknik penipuan untuk mengumpulkan data pribadi. Serangan Man-in-the-Middle merupakan penyadapan komunikasi untuk mencuri data, dan serangan Denial-of-

Service mencegah akses sah ke sistem dengan membanjiri jaringan/server dengan lalu lintas data (Niagahoster, 2023).

Mengakui peningkatan serangan siber, organisasi di seluruh dunia telah meningkatkan usaha dalam mengimplementasikan langkah-langkah keamanan untuk melindungi sistem TI dan data penting. Dalam konteks ini, audit internal dihadapkan pada kebutuhan untuk memperluas fokusnya, mencakup risiko keamanan siber yang terkait dengan laporan keuangan dan pelaporan tahunan. Hal ini menuntut evolusi dalam pendekatan audit TI, menganjurkan untuk adopsi penilaian risiko keamanan siber yang lebih berbasis risiko (Backer, 2022).

Cyber in the Audit (CitA) dari KPMG sebagai kerangka kerja untuk mengatasi risiko yang dapat mengancam kerahasiaan, integritas, dan ketersediaan data. Metodologi ini memperkuat audit TI dengan secara khusus menguji langkah-langkah keamanan siber yang dirancang untuk mendeteksi dan mencegah pengabaian Kontrol Aplikasi TI dan Kontrol TI Umum, sebagaimana ditunjukkan dalam penelitian oleh Backer (2022).

Dalam praktik audit CitA, penting bagi auditor untuk memberikan perhatian khusus pada aplikasi dan sistem yang mengelola data terkait laporan keuangan. Namun, penting juga untuk memperluas cakupan audit ke sistem terkait lainnya, termasuk lapisan perimeter jaringan dan internal, yang sering menjadi target utama serangan siber. Hal ini menandai perluasan dari fokus tradisional audit TI yang biasanya terbatas pada aplikasi, basis data, dan sistem operasi yang langsung berpengaruh terhadap laporan keuangan (Backer, 2022).

Hasil dari penilaian risiko siber penting untuk diintegrasikan ke dalam rencana audit keseluruhan, memberikan pandangan yang komprehensif tentang bagaimana risiko siber dapat mempengaruhi laporan keuangan dan kontrol internal. Keputusan terkait dengan pengambilan sampel atau pengujian substantif atas bukti digital dari sistem yang mungkin telah dikompromikan dibuat berdasarkan analisis dampak ini, menekankan pentingnya pendekatan yang terinformasi dan berbasis risiko dalam menghadapi ancaman siber dalam audit pajak.

2.2.2.2 Memperkuat Audit Pajak Melalui Strategi Keamanan Siber

Ketika integritas data pajak terancam, validitas hasil audit pajak menjadi bahan pertanyaan. Informasi pajak yang terkorupsi dapat menyebabkan kesalahan perhitungan pajak, mempengaruhi pembuatan keputusan, dan mengikis kepercayaan publik terhadap sistem perpajakan. Sebagai respons, keamanan siber yang efektif tidak hanya esensial untuk melindungi data dari ancaman eksternal, tetapi juga krusial dalam menjaga akurasi dan kepercayaan dalam proses audit pajak.

Penting bagi administrasi pajak dan auditor, sebagaimana diuraikan dalam IRS (2021), untuk menyertakan langkah-langkah keamanan siber sebagai bagian integral dari proses audit. Langkah-langkah ini meliputi:

1) Penerapan teknologi keamanan tinggi, dengan menggunakan firewall canggih, solusi antivirus, dan teknik enkripsi data untuk membentengi jaringan dan sistem terhadap serangan siber, memastikan bahwa

infrastruktur TI yang mendukung proses audit pajak dilindungi secara maksimal.

2) Menerapkan kebijakan kontrol akses yang ketat untuk memastikan hanya staf yang memiliki otorisasi akses informasi pajak sensitif, sehingga meminimalisir risiko kebocoran atau penyalahgunaan data.
3) Mengembangkan program pelatihan untuk meningkatkan kesadaran staf tentang ancaman keamanan siber dan mengajarkan praktik terbaik dalam menghindari potensi serangan, sebagai langkah preventif untuk memperkuat baris pertahanan pertama terhadap serangan siber.
4) Memasang alat pemantauan canggih untuk secara aktif mendeteksi dan menanggapi tanda-tanda aktivitas mencurigakan dalam jaringan dan sistem, memungkinkan deteksi dini dan pencegahan serangan sebelum menyebabkan kerusakan signifikan.
5) Menyusun protokol respons insiden untuk mengatasi pelanggaran keamanan siber dengan cepat dan efisien, serta mengembangkan rencana pemulihan yang robust untuk memulihkan data dan sistem dengan minimal downtime dan kerugian setelah insiden terjadi.

Melalui implementasi langkah-langah ini, administrasi pajak dan auditor dapat meningkatkan keandalan dan keamanan proses audit pajak, meminimalkan risiko serangan siber, dan mempertahankan kepercayaan publik dalam sistem perpajakan. Implementasi strategi keamanan siber yang komprehensif ini tidak hanya melindungi aset data yang berharga tetapi juga memperkuat integritas keseluruhan proses audit pajak.

2.2.3 Tren dan Strategi Global Keamanan Siber dalam Audit Pajak

Dalam audit pajak, memahami tren, tantangan, dan strategi administrasi pajak global sangat penting, terutama dengan perubahan yang cepat dan kompleks. Laporan OECD 2022, yang mencakup data dari 58 yurisdiksi sampai tahun 2020, menyediakan wawasan kritis untuk audit pajak. Laporan tersebut menyoroti adaptasi administrasi pajak global terhadap perubahan kondisi, termasuk dampak pandemi COVID-19, dan menekankan pentingnya pendekatan proaktif dalam mengelola kepatuhan pajak dan kebutuhan sumber daya. Pandemi telah secara signifikan mengubah cara administrasi pajak beroperasi, dengan penurunan 55% dalam interaksi tatap muka dan peningkatan 30% dalam interaksi digital. Perubahan ini telah mempercepat adopsi transformasi digital, mendorong pengembangan metode kerja baru dan integrasi peran baru.

Laporan OECD 2022 ini menyoroti pergeseran berkelanjutan menuju administrasi pajak yang sepenuhnya digital, termasuk proses pengisian dan pembayaran pajak secara online serta adopsi sistem pengisian pajak secara pra-isi. Sebanyak 75% administrasi pajak telah menetapkan strategi transformasi digital, dengan tujuan membuat layanan digital lebih cerdas dan efisien, sekaligus meningkatkan kepatuhan pajak. Pentingnya memastikan identitas digital yang aman dan kolaborasi dengan penyedia layanan pihak ketiga menjadi semakin terlihat. Inisiatif ini tidak hanya meningkatkan kepatuhan pajak tetapi juga mengurangi beban administratif, menunjukkan sinergi antara keamanan siber dan efisiensi administrasi pajak. Pendekatan ini, yang awalnya diterapkan pada wajib pajak

dengan pendapatan tetap, kini diperluas untuk mencakup berbagai sumber pendapatan dan kelas wajib pajak. Inisiatif ini dimungkinkan oleh peningkatan ketersediaan dan berbagi data, yang relevan dengan praktik audit pajak modern yang mengutamakan data dan analisis risiko.

Administrasi pajak semakin memanfaatkan teknologi canggih seperti big data, analitik, AI, dan machine learning untuk manajemen risiko. Hal ini relevan bagi auditor pajak, yang dapat memanfaatkan teknologi serupa untuk analisis dan evaluasi risiko pajak yang lebih efektif. Meskipun dihadapkan pada kendala anggaran, penerapan teknologi seperti Automasi Proses Robotik (RPA) dapat meningkatkan efisiensi operasional. Pandemi juga telah mendorong adopsi kerja jarak jauh, menuntut penyesuaian dalam praktik kerja dan penggunaan teknologi digital. Kerjasama internasional dan peningkatan berbagi pengetahuan menjadi kunci saat administrasi pajak mengimplementasikan transformasi signifikan. Partisipasi dalam inisiatif seperti Paket BEPS OECD/G20 membantu mengatasi tantangan pajak lintas batas, relevan untuk audit pajak yang efektif di era globalisasi.

Regulasi global seperti GDPR di Uni Eropa telah menetapkan standar baru dalam perlindungan data dan privasi, yang juga berdampak pada operasional administrasi pajak. Kepatuhan terhadap regulasi semacam ini memastikan bahwa data wajib pajak diproses dan disimpan dengan cara yang aman dan transparan, mengurangi risiko pelanggaran data yang dapat mempengaruhi audit pajak. Investasi dalam pembangunan kapasitas dan pelatihan untuk staf audit dan administrasi pajak adalah kunci untuk memastikan bahwa staf dilengkapi dengan pengetahuan dan

keterampilan yang diperlukan untuk menghadapi ancaman siber yang berkembang. Hal ini termasuk pelatihan tentang teknik phishing terbaru, cara mengidentifikasi dan merespons serangan ransomware, serta praktik terbaik dalam manajemen akses dan kontrol keamanan data.

Penggunaan teknologi blockchain dalam administrasi pajak menawarkan potensi untuk meningkatkan transparansi, keamanan, dan efisiensi dalam pengumpulan dan pengolahan data pajak. Dengan sifat desentralisasi dan keamanan yang inheren, blockchain bisa membantu mengurangi risiko manipulasi data dan memperkuat integritas audit pajak. Adopsi kecerdasan buatan (AI) dan pembelajaran mesin tidak hanya meningkatkan kemampuan analisis data dalam skala besar tetapi juga memungkinkan prediksi dan deteksi proaktif terhadap risiko kepatuhan pajak. Dengan memanfaatkan AI, administrasi pajak dapat lebih efektif dalam mengidentifikasi perilaku transaksi yang mencurigakan, menyediakan insight untuk auditor pajak.

Kerjasama internasional melalui pertukaran informasi antar yurisdiksi memainkan peran penting dalam menanggulangi penghindaran pajak dan penipuan pajak yang kompleks. Inisiatif seperti Common Reporting Standard (CRS) oleh OECD memfasilitasi pertukaran otomatis informasi keuangan, membantu auditor pajak dalam mengidentifikasi risiko pajak lintas batas dengan lebih efektif.

Dengan mempertimbangkan tren dan strategi ini, auditor pajak dapat menyesuaikan pendekatan untuk mencerminkan evolusi dalam administrasi pajak global, memastikan bahwa audit tetap relevan, efektif, dan sesuai dengan standar keamanan siber terbaru.

2.3 Integrasi Keamanan Siber dalam Audit Pajak

Integrasi keamanan siber dalam audit pajak adalah proses penting yang memastikan data dan sistem pajak terlindungi dari ancaman digital. Hal ini melibatkan penggunaan strategi, alat, dan teknologi yang dirancang khusus untuk melindungi informasi sensitif dan infrastruktur TI selama proses audit pajak.

2.3.1 Strategi, Alat, dan Teknologi dalam Cybersecurity

2.3.1.1 Strategi dalam Cybersecurity

Strategi cybersecurity bertujuan untuk meningkatkan keamanan informasi organisasi dengan membuat kebijakan yang jelas mengenai keamanan cyber, melatih karyawan tentang pentingnya dan cara menjaga keamanan informasi, serta secara rutin mengevaluasi potensi risiko dan kelemahan sistem untuk mencegah serangan cyber (Martin, 2022). Dengan menggabungkan strategi, alat, dan teknologi ini dalam keamanan siber, terutama di area sensitif seperti audit pajak, sangat penting untuk melindungi dari ancaman siber. Pendekatan ini harus holistik, menyeimbangkan orang, proses, dan teknologi, dan dipandu oleh kerangka kerja yang telah ditetapkan seperti NIST Cybersecurity Framework, yang menyediakan tindakan terperinci untuk mengidentifikasi, mendeteksi, dan menanggapi serangan siber.

Strategi keamanan siber yang penting bagi setiap organisasi melibatkan rencana tingkat tinggi untuk mengamankan aset dan meminimalkan risiko siber. Strategi ini, yang dapat diadaptasi dengan lanskap ancaman dan lingkungan bisnis yang berubah, berfungsi sebagai cetak biru untuk membimbing pemangku kepentingan utama.

Fokusnya adalah mencapai ketahanan siber dengan beralih dari pendekatan reaktif menjadi proaktif, sehingga mencegah serangan siber dan mempersiapkan respons yang efektif terhadap insiden (Stone, 2021).

Pelatihan karyawan sangat penting untuk menjaga keamanan data perusahaan. Karyawan sering mengabaikan kebijakan keamanan data perusahaan, menjadi titik lemah dalam upaya keamanan siber. Pelatihan ini meningkatkan kesadaran staf terhadap ancaman potensial, seperti serangan phishing, mengurangi kemungkinan terkena ancaman tersebut. Misalnya, dilaporkan bahwa setiap sesi pelatihan menurunkan risiko serangan phishing yang berhasil sebesar 20%. Pelatihan harus mencakup kesadaran tentang tanda-tanda peringatan dalam komunikasi, seperti email tak terduga yang meminta informasi sensitif, dan menekankan pentingnya otentikasi multifaktor dan akses terbatas ke jaringan (Wisenberg Brin, 2021).

Penilaian risiko secara berkala adalah dasar dalam mengidentifikasi kerentanan yang dapat mengancam operasi dan reputasi organisasi. Penilaian ini sangat penting untuk memahami ancaman dan kerentanan yang spesifik untuk proses dan industri organisasi. National Institute of Standards and Technology (NIST) menekankan bahwa penilaian risiko adalah fondasi dari manajemen risiko keseluruhan organisasi, dengan fokus pada identifikasi, klasifikasi, dan prioritas risiko terhadap operasi, aset, individu, dan organisasi lain (RSI Security, 2021).

2.3.1.2 Alat Cybersecurity

Alat-alat penting seperti perangkat lunak anti-virus, firewall, dan sistem deteksi intrusi memegang peranan krusial dalam identifikasi dan pencegahan serangan cyber. Stimpson (2018) menekankan pentingnya alat-alat ini dalam infrastruktur keamanan informasi.

A. Perangkat lunak anti-virus,

Perangkat lunak anti-virus bertindak sebagai garis pertahanan pertama melawan perangkat lunak berbahaya dan virus, dengan memindai, mendeteksi, dan menghapusnya dari sistem (Symantec, 2019). Perangkat lunak anti-virus beroperasi sebagai garis pertahanan pertama terhadap perangkat lunak berbahaya (malware) dan virus dengan menggunakan beberapa metode utama:

1) Pemindaian dan Deteksi
   Perangkat lunak anti-virus secara teratur memindai file dan program yang ada di sistem komputer untuk mencari pola yang dikenal sebagai tanda-tanda malware. Tanda-tanda malware ini termasuk virus, worm, trojan, ransomware, spyware, dan bentuk malware lainnya. Pemindaian ini dapat dilakukan secara real-time, yaitu pemindaian aktif ketika file diakses atau dijalankan atau berdasarkan jadwal yang ditetapkan, atau pemindaian terjadwal.
2) Basis Data Signature
   Anti-virus menggunakan basis data signature (tanda tangan) yang berisi informasi tentang virus dan malware yang diketahui. Signature ini adalah potongan kode unik atau pola perilaku yang terkait dengan malware tertentu. Perangkat lunak anti-virus

membandingkan file dan program dengan database ini untuk mengidentifikasi ancaman.

3) Heuristik dan Deteksi Berbasis Perilaku
   Untuk mengidentifikasi malware baru yang belum termasuk dalam database signature, perangkat lunak anti-virus menggunakan metode heuristik. Hal ini melibatkan menganalisis perilaku file atau program untuk mendeteksi aktivitas yang mencurigakan yang mungkin menunjukkan malware. Analisis ini penting karena malware terus berevolusi dan beberapa mungkin belum dikenali melalui signature tradisional.
4) Karantina dan Penghapusan
   Ketika sebuah ancaman terdeteksi, perangkat lunak anti-virus biasanya akan mengisolasi (karantina) atau menghapus file yang terinfeksi. Karantina menyimpan file dalam area aman sistem di mana file tidak dapat berjalan atau menyebabkan kerusakan. Pengguna kemudian bisa memilih untuk menghapus file tersebut secara permanen atau, dalam beberapa kasus, mencoba membersihkannya dari infeksi.
5) Pembaruan Otomatis
   Karena jenis dan bentuk malware terus berkembang, penting bagi perangkat lunak anti-virus untuk memperbarui database signature dan algoritma deteksi. Pembaruan ini dilakukan otomatis untuk memastikan perlindungan terhadap ancaman terbaru.

B. Firewall

Firewall berfungsi sebagai penghalang antara jaringan internal yang aman dan sumber luar yang tidak terpercaya, mengontrol lalu lintas jaringan berdasarkan serangkaian aturan yang ditentukan (Cisco, 2020).

Firewall adalah perangkat keamanan jaringan yang bertindak sebagai penghalang antara jaringan internal (yang dianggap aman) dan sumber luar (yang mungkin tidak terpercaya) (Cisco, 2020). Fungsi utamanya adalah mengontrol lalu lintas jaringan yang masuk dan keluar berdasarkan serangkaian aturan yang ditentukan. Cara kerja firewall:

1) Firewall memeriksa setiap paket data yang masuk atau keluar dari jaringan, dilakukan dengan membandingkan informasi dalam paket (seperti alamat IP sumber dan tujuan, nomor port, dan protokol yang digunakan) dengan serangkaian aturan yang telah ditetapkan.
2) Aturan-aturan ini ditetapkan berdasarkan kebijakan keamanan jaringan, mencakup kriteria seperti alamat IP yang diizinkan atau ditolak, port yang dapat digunakan untuk komunikasi, dan jenis protokol yang diizinkan (seperti TCP, UDP, ICMP, dll.).
3) Firewall memutuskan apakah sebuah paket harus diteruskan atau diblokir. Jika paket cocok dengan aturan yang mengizinkannya, paket akan diteruskan ke tujuan berikutnya. Jika tidak, paket akan diblokir dan dibuang.
4) Beberapa jenis firewall, termasuk firewall berbasis paket (packet-filtering firewall), yang membuat keputusan berdasarkan setiap paket secara individual; firewall negara (stateful firewall), yang melacak status koneksi dan membuat keputusan berdasarkan konteks koneksi; dan firewall lapisan aplikasi (application-layer firewall), yang memeriksa lalu lintas pada tingkat aplikasi.

5) Konfigurasi dan manajemen firewall membutuhkan pemahaman yang baik tentang kebijakan keamanan jaringan dan ancaman yang ada. Konfigurasi yang tidak tepat dapat mengakibatkan kelemahan keamanan atau mengganggu operasi jaringan normal.

Secara keseluruhan, firewall merupakan komponen penting dalam arsitektur keamanan jaringan, menyediakan pertahanan pertama terhadap akses tidak sah dan serangan cyber, sambil memungkinkan lalu lintas yang sah untuk beroperasi tanpa gangguan.

C. Sistem deteksi intrusi (IDS) dan Intrusion Prevention Systems (IPS)

Sistem pemantauan jaringan yang canggih memainkan peran penting dalam deteksi aktivitas mencurigakan dan memberikan peringatan dini tentang potensi pelanggaran keamanan. Menurut Easttom (2019), sistem pemantauan ini dirancang untuk mengawasi lalu lintas jaringan secara real-time, mengidentifikasi pola yang tidak biasa atau perilaku yang mencurigakan yang mungkin menunjukkan adanya serangan siber.

Teknologi seperti Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS) sering digunakan dalam monitoring ini. IDS bertugas untuk memindai jaringan dan mendeteksi aktivitas yang tidak sesuai dengan pola normal, sementara IPS melangkah lebih jauh dengan mengambil tindakan untuk mencegah atau mengurangi dampak serangan tersebut. Easttom juga menekankan pentingnya analisis log secara teratur. Log dari server, firewall, dan perangkat lain dalam jaringan dapat memberikan wawasan penting tentang aktivitas jaringan dan potensi ancaman. Alat pemantauan canggih sering kali

dilengkapi dengan kemampuan analisis log otomatis untuk mengidentifikasi ancaman yang lebih halus atau kompleks. Dalam buku tersebut, Easttom membahas secara mendalam tentang berbagai aspek keamanan siber, termasuk pentingnya sistem pemantauan dan pengawasan dalam menjaga keamanan jaringan.

Sistem deteksi intrusi (IDS) memonitor jaringan untuk aktivitas mencurigakan dan serangan yang sedang berlangsung, memberikan peringatan ketika potensi ancaman terdeteksi (Palo Alto Networks, 2021). Sistem Deteksi Intrusi (Intrusion Detection System, IDS) adalah alat yang sangat penting dalam keamanan jaringan. Fungsi utamanya adalah untuk memonitor jaringan dan sistem untuk aktivitas yang tidak biasa atau mencurigakan.

1) IDS terus-menerus memindai trafik yang masuk dan keluar dalam jaringan untuk mendeteksi pola-pola yang mencurigakan. Kegiatan ini meliputi pemeriksaan paket data, protokol yang digunakan, port dan endpoint yang terlibat, serta isi dari komunikasi itu sendiri.
2) Banyak IDS beroperasi berdasarkan basis aturan atau signature yang sudah ditentukan. Signature adalah pola-pola yang diketahui dari perilaku serangan yang telah dicatat sebelumnya. Jika trafik jaringan cocok dengan salah satu signature ini, IDS akan menandainya sebagai potensi serangan.
3) Beberapa IDS menggunakan pendekatan deteksi berbasis anomali, mempelajari pola trafik normal dan kemudian mengidentifikasi penyimpangan dari norma tersebut sebagai indikator potensi serangan.

4) Setelah potensi ancaman terdeteksi, IDS dapat dikonfigurasi untuk mengambil tindakan otomatis. Hal ini mungkin termasuk mengirimkan peringatan kepada administrator, memblokir trafik yang mencurigakan, atau mengisolasi bagian jaringan yang terpengaruh.
5) IDS sering kali terintegrasi dengan sistem keamanan lainnya seperti Sistem Pencegahan Intrusi (IPS) dan firewall. Hal ini memungkinkan respons yang lebih cepat dan efektif terhadap ancaman.
6) IDS modern mampu beradaptasi dengan ancaman baru dengan secara berkala memperbarui basis data signature dan aturannya, memastikan perlindungan terhadap jenis serangan terbaru.

Menggabungkan alat-alat ini dalam strategi cybersecurity memungkinkan organisasi untuk menanggapi secara proaktif terhadap ancaman yang berkembang dan meningkatkan keseluruhan postur keamanan. Keefektifan alat-alat tersebut sangat bergantung pada pembaruan reguler dan konfigurasi yang tepat, yang memastikan dapat melawan ancaman terkini dan canggih (Kaspersky, 2022).

2.3.1.3 Teknologi Enkripsi dalam Cybersecurity

Teknologi enkripsi data memastikan bahwa informasi sensitif, seperti data perpajakan, tetap tidak dapat diakses dan tidak terbaca oleh pihak yang tidak berwenang. Proses ini melibatkan konversi teks biasa (plaintext) menjadi teks terenkripsi (ciphertext) menggunakan algoritma enkripsi yang kuat seperti Advanced Encryption Standard (AES), RSA, dan Triple Data Encryption Standard (3DES). Menurut

IRS (2023), penerapan teknologi enkripsi ini sangat penting untuk melindungi data pribadi dan keuangan.

A. Algoritma Enkripsi AES

Algoritma AES merupakan standar enkripsi yang digunakan secara luas karena keamanannya yang tinggi dan efisiensi dalam berbagai aplikasi. Algoritma ini menggunakan kunci enkripsi yang panjang dan kompleks untuk mengamankan data (NIST, 2021).

Algoritma ini menggunakan kunci enkripsi dengan panjang yang bervariasi, yaitu 128, 192, atau 256 bit, dengan ukuran blok tetap sebesar 128 bit.

AES merupakan bagian dari keluarga Rijndael yang dipilih oleh NIST, dan telah diadopsi oleh pemerintah AS. Algoritma ini menggantikan Data Encryption Standard (DES) yang lebih tua, yang pertama kali diterbitkan pada tahun 1977 (Veritas, 2023).

AES-256, menggunakan kunci enkripsi 256-bit untuk mengenkripsi dan mendekripsi blok pesan. Setiap cipher dalam AES mengenkripsi dan mendekripsi data dalam blok-blok 128 bit menggunakan kunci kriptografi 128, 192, dan 256 bit. Sebagai algoritma kunci simetris (juga dikenal sebagai kunci rahasia), AES menggunakan kunci yang sama untuk proses enkripsi dan dekripsi.

Teknik enkripsi AES cepat dan efektif, sehingga dapat digunakan dalam berbagai aplikasi. AES dianggap aman dari serangan seperti brute force dan kriptoanalisis diferensial, menjadikannya salah satu algoritma enkripsi yang paling tepercaya dan sering digunakan saat ini (Corinne Bernstein, 2021).

B. RSA (Rivest-Shamir-Adleman)

RSA adalah sistem enkripsi berbasis kunci publik yang sering digunakan untuk pengamanan transaksi online dan pertukaran data yang aman (RSA Security, 2022). Dalam sistem RSA, enkripsi dilakukan dengan menggunakan dua kunci berbeda, yaitu kunci publik dan kunci privat. Kunci publik dapat dibagikan secara terbuka dan digunakan untuk mengenkripsi pesan, sementara kunci privat digunakan untuk mendekripsi pesan tersebut.

Konsep utama RSA didasarkan pada kesulitan dalam memfaktorkan bilangan bulat besar. Kunci publik terdiri dari dua angka, di mana salah satu angkanya merupakan hasil perkalian dua bilangan prima besar. Kunci privat juga diturunkan dari dua bilangan prima yang sama. Jika seseorang dapat memfaktorkan bilangan besar ini, maka kunci privat dianggap terkompromi (Josh Lake, 2021).

RSA umumnya digunakan untuk pengamanan transaksi online dan pertukaran data yang aman, seperti enkripsi email dan transaksi digital lainnya melalui Internet. Pengguna memilih sepasang bilangan prima yang besar, p dan q, sehingga faktorisasi produk jauh di luar kemampuan komputasi yang diproyeksikan (Simmons & Gustavus, 2022).

Dengan sifat matematika yang khas dari algoritma RSA, setelah pesan dienkripsi dengan kunci publik, hanya bisa didekripsi oleh kunci privat yang terkait. Hal ini menciptakan tingkat keamanan yang tinggi untuk data yang ditransmisikan melalui jaringan yang tidak aman, seperti Internet.

C. Triple Data Encryption Standard (3DES)

3DES adalah teknik enkripsi yang menggunakan algoritma DES secara tiga kali berturut-turut pada setiap blok data. Hal ini dilakukan sebagai respons terhadap kelemahan kunci 56-bit yang digunakan oleh DES, yang tidak lagi dianggap cukup aman terhadap teknik kriptoanalisis modern dan kekuatan superkomputer. Oleh karena itu, 3DES dibuat untuk meningkatkan keamanan dengan cara yang lebih kompleks.

Proses enkripsi 3DES beroperasi dalam tiga tahap: Enkripsi-Dekripsi-Enkripsi (Encrypt-Decrypt-Encrypt atau EDE). Hal ini dilakukan dengan mengambil tiga kunci 56-bit (K1, K2, dan K3), yang dikenal sebagai bundel kunci, dan melakukan enkripsi pertama dengan K1, dekripsi selanjutnya dengan K2, dan enkripsi terakhir dengan K3. Ada juga versi 3DES dua-kunci, di mana algoritma yang sama dijalankan tiga kali tetapi dengan dua kunci (Cobb, 2023).

3DES adalah algoritma simetris-key yang berbasis pada jaringan Feistel. Sebagai algoritma kunci simetris, ia menggunakan kunci yang sama untuk proses enkripsi dan dekripsi. Teknik ini membutuhkan generasi dua atau tiga kunci, tergantung pada varian spesifik yang digunakan. Setiap kunci berukuran 56 bit tetapi biasanya diperluas menjadi 64 bit untuk memastikan kompatibilitas dengan DES yang lebih tua (Lake, 2023) dan (Dimitri Antonenko, 2023).

2.3.2 Integrasi Cybersecurity dalam Audit Pajak

Integrasi keamanan siber dalam audit pajak merupakan aspek kritis dalam era digital. Integrasi keamanan siber dalam audit pajak bukan hanya tentang melindungi data tetapi juga tentang memastikan keandalan, keadilan, dan transparansi dalam sistem perpajakan, yang pada akhirnya membantu mempertahankan kepercayaan publik dan integritas sistem fiskal. Pendekatan ini melibatkan penerapan strategi dan teknologi canggih untuk melindungi data dari ancaman siber. Aspek-aspek utama dari integrasi ini meliputi:

1) Penerapan Strategi dan Teknologi Canggih
   Organisasi perpajakan mengadopsi berbagai teknologi keamanan canggih, seperti enkripsi data, otentikasi dua faktor, dan penggunaan firewall serta sistem deteksi intrusi. Pendekatan ini bertujuan untuk mengamankan data pajak yang sensitif dari serangan siber, seperti phishing, ransomware, dan akses tidak sah.
2) Pemeliharaan Integritas Sistem Pajak
   Melindungi data pajak tidak hanya berkaitan dengan keamanan informasi tetapi juga tentang menjaga integritas sistem perpajakan. Johnson (2015) menyebutkan bahwa keamanan siber yang efektif adalah kunci dalam memastikan bahwa sistem perpajakan bekerja secara adil dan akurat.
3) Menjaga Kepercayaan Publik
   Kepercayaan publik adalah aset penting dalam administrasi pajak. Ferrillo (2017) menjelaskan bahwa kepercayaan ini sangat bergantung pada kemampuan otoritas pajak untuk melindungi data wajib pajak dari kebocoran dan penyalahgunaan.

4) Kebijakan dan Regulasi
   Organisasi perpajakan juga harus mematuhi berbagai kebijakan dan regulasi keamanan siber, seperti yang dijelaskan Sammons & Cross (2016). Kebijakan ini sering kali mencakup pedoman mengenai perlindungan data, respons insiden, dan audit keamanan.

2.3.2.1 Integrasi Cybersecurity dalam Proses Audit Pajak

A. Penggunaan Perangkat Lunak Audit dengan Fitur Keamanan Siber

Penggunaan perangkat lunak audit dalam proses audit pajak yang dilengkapi dengan fitur keamanan siber merupakan langkah esensial dalam mengamankan data keuangan dan informasi sensitif lainnya. Berdasarkan standar dan praktik terbaik keamanan siber yang direkomendasikan oleh OECD, terdapat beberapa fitur dan praktik keamanan yang harus diterapkan, termasuk:

1) Enkripsi Data. Sebagai fondasi keamanan siber, enkripsi data memainkan peran kritikal dalam menjaga kerahasiaan data keuangan. Johnson (2010) menekankan pentingnya enkripsi dalam melindungi informasi dari akses tidak sah, khususnya selama transmisi data atau penyimpanannya dalam basis data. Dalam konteks audit pajak, ini memastikan bahwa data keuangan sensitif terlindungi secara efektif.
2) Otentikasi Dua Faktor (2FA Menurut Singer dan Friedman (2014), 2FA menambahkan lapisan keamanan tambahan yang signifikan, melebihi sekadar penggunaan nama pengguna dan kata sandi. Dalam praktik audit pajak, di mana akses ke data keuangan

sensitif merupakan kegiatan rutin, penerapan 2FA dapat drastis mengurangi risiko akses ilegal.

3) Perlindungan Terhadap Serangan Cyber. Mitnick (2013) mendeskripsikan berbagai langkah keamanan yang dirancang untuk melawan ancaman cyber, seperti malware dan ransomware. Perlindungan ini sangat penting dalam audit pajak, mengingat sensitivitas data pajak. Perangkat lunak audit harus memiliki protokol keamanan yang kuat untuk mendeteksi dan merespons ancaman cyber secara efektif..
4) Pembaruan dan Patch Keamanan Reguler. Memastikan perangkat lunak audit selalu terupdate sangat penting untuk mengatasi kerentanan baru. Hal ini membutuhkan desain yang memungkinkan instalasi pembaruan keamanan secara otomatis dan teratur.
5) Menerapkan kontrol akses memastikan bahwa hanya staff yang berwenang yang dapat mengakses data tertentu, vital untuk mencegah kebocoran dan pelanggaran data dalam proses audit pajak.
6) Pencatatan Akses Data. Menyimpan log detil tentang akses data membantu dalam kepatuhan dan keamanan. Log ini menjadi sangat berharga dalam investigasi pelanggaran keamanan.
7) Kepatuhan terhadap Standar Perlindungan Data Internasional. Mengingat banyak bisnis beroperasi secara global, kepatuhan terhadap standar seperti GDPR menjadi krusial dalam audit pajak untuk menangani masalah perpajakan lintas negara.

Integrasi fitur keamanan siber dalam perangkat lunak audit tidak hanya meningkatkan keamanan data keuangan tetapi juga memperkuat kepercayaan stakeholder dalam proses audit pajak. Studi-studi terkait menunjukkan bahwa

penerapan secara konsisten dari praktik keamanan ini dapat mengurangi risiko kebocoran data dan serangan cyber, sementara juga memastikan kepatuhan terhadap regulasi perlindungan data yang berlaku. Implikasinya terhadap praktik audit pajak mencakup peningkatan efisiensi proses audit, pengurangan potensi hambatan regulasi, dan peningkatan reputasi institusi audit.

B. Pemeriksaan Keamanan Data Pajak

Dalam era digital saat ini, keamanan data pajak memegang peranan penting dalam memastikan integritas dan kepercayaan terhadap sistem administrasi pajak. Program International Compliance Assurance Programme (ICAP) yang dirilis oleh OECD Forum on Tax Administration menawarkan kerangka kerja untuk penilaian risiko pajak dan jaminan secara multilateral. ICAP mendorong keterlibatan antara perusahaan multinasional dan administrasi pajak di berbagai yurisdiksi, memfokuskan pada risiko transfer pricing, pendirian tetap, dan isu pajak internasional lainnya (OECD, 2020).

Pentingnya pemeriksaan keamanan data terletak pada kemampuannya untuk memastikan bahwa data disimpan dalam lingkungan yang aman dan terlindungi dari akses tidak sah. Menyelaraskan praktik keamanan data dengan standar ICAP dapat memberikan kepastian dan jaminan pajak lebih dini bagi perusahaan multinasional, sekaligus mengurangi risiko keamanan data. Penelitian oleh Chan et al. (2022) menunjukkan bahwa penggunaan teknologi canggih seperti jaringan saraf tiruan untuk data mining dapat meningkatkan efektivitas pemilihan audit dengan berbasis pada data historis pajak.

Publikasi Cybersecurity in Tax Administration oleh OECD menyediakan panduan komprehensif tentang integrasi keamanan siber dalam administrasi pajak, menekankan pada strategi, teknologi, pelatihan, dan kerjasama internasional. Dokumen ini menggarisbawahi pentingnya mengadopsi pendekatan yang holistik terhadap keamanan siber, mencakup tidak hanya aspek teknis tapi juga manajemen risiko dan pelatihan kesadaran (OECD, 2019).

American Institute of Certified Public Accountants (AICPA) dalam dokumen Integrating Cybersecurity and Enterprise Risk Management (ERM) in Financial Audits menyoroti bagaimana keamanan siber dapat diintegrasikan ke dalam manajemen risiko perusahaan dan audit keuangan. Hal ini termasuk identifikasi, penilaian, dan pengelolaan risiko siber secara efektif serta pemahaman terhadap dampak risiko siber pada laporan keuangan dan proses audit (AICPA, 2021).

Dengan demikian, integrasi cybersecurity dalam pemeriksaan keamanan data pajak bukan hanya tentang mengadopsi teknologi terbaru atau memenuhi standar internasional; ini tentang membangun ekosistem yang resilien yang melibatkan pelatihan, kesadaran, kerjasama, dan manajemen risiko untuk melindungi data pajak dari ancaman siber yang terus berkembang. Pendekatan ini memungkinkan administrasi pajak untuk tidak hanya memastikan keamanan data tapi juga meningkatkan efisiensi dan keadilan dalam proses audit pajak.

C. Pelatihan Kesadaran Keamanan Siber

Kesadaran dan pelatihan keamanan siber bagi auditor pajak telah menjadi aspek kritikal dalam mengelola risiko keamanan informasi dan menjaga integritas data fiskal. Dalam laporan OnRisk 2022 oleh The Institute of Internal Auditors (IIA), diidentifikasi bahwa keamanan siber merupakan salah satu risiko utama yang dihadapi organisasi, dengan ancaman siber yang semakin canggih dan beragam mempengaruhi reputasi dan stabilitas finansial organisasi (IIA, 2022).

Pendidikan dasar dan pelatihan lanjutan dalam keamanan siber menjadi penting bagi auditor dalam era otomatisasi, komputasi awan, dan penggunaan perangkat mobile yang luas. Hal ini termasuk memahami konsep kunci keamanan siber dan bagaimana konsep-konsep ini diterapkan dalam konteks audit pajak untuk memperkuat upaya audit dan meminimalisir risiko keamanan.

Pelatihan yang efektif mencakup berbagai aspek, mulai dari definisi keamanan siber dalam konteks audit internal, pemahaman tentang ruang lingkup, tujuan, dan batasan keamanan siber, hingga pengenalan dan penerapan kontrol keamanan siber yang beragam. Kontrol ini mencakup tindakan pencegahan, deteksi, koreksi, dan mitigasi, serta pentingnya tata kelola keamanan informasi dan penilaian risiko terhadap vendor dan pihak ketiga.

Kursus pelatihan untuk auditor pajak sebaiknya dirancang untuk memberikan pemahaman mendalam tentang keamanan siber dan eksploitasi umum, dengan fokus pada bagaimana menilai keefektifan kontrol keamanan dalam menghadapi peristiwa keamanan siber dan dampaknya terhadap risiko organisasi. Hal ini melibatkan

pengenalan kepada aktivitas audit yang dapat menilai ketahanan siber dalam program audit yang ada dan bagaimana penilaian risiko keamanan siber dapat diintegrasikan dalam audit operasional.

Studi Kaspersky Lab (2019) menunjukkan bahwa pelatihan kesadaran keamanan siber yang efektif dapat mengurangi insiden keamanan hingga 70%. Hasil studi ini menekankan pentingnya pelatihan yang berkelanjutan dan adaptasi terhadap ancaman siber yang terus berkembang. Integrasi pelatihan ini dalam kurikulum audit pajak memungkinkan auditor untuk lebih siap menghadapi ancaman siber, memastikan keamanan data pajak, dan mendukung integritas keseluruhan sistem pajak.

Dengan demikian, pelatihan kesadaran keamanan siber untuk auditor pajak bukan hanya tentang memenuhi persyaratan kompetensi, tetapi juga investasi dalam resiliensi organisasi dan kepercayaan publik terhadap sistem pajak. Memperkuat pelatihan ini dengan kasus nyata, simulasi, dan penilaian keamanan siber yang hands-on akan lebih meningkatkan kemampuan auditor dalam mengidentifikasi, menanggapi, dan mencegah ancaman siber dalam lingkup audit pajak.

D. Kebijakan dan Prosedur Keamanan yang Kuat dalam Audit Pajak

Kebijakan dan prosedur keamanan yang kuat merupakan tulang punggung dari upaya cybersecurity dalam setiap organisasi, termasuk dalam konteks audit pajak. Pengaturan akses yang terkontrol ke data pajak, penggunaan kata sandi yang kuat, dan penerapan standar keamanan yang ketat adalah langkah-langkah esensial dalam menjaga keamanan informasi.

Panduan oleh Landoll (2017) menawarkan kerangka kerja komprehensif untuk mengembangkan kebijakan dan prosedur keamanan informasi yang efektif, dengan menyarankan penggunaan standar seperti NIST 800-53, ISO 27001, dan COBIT. Standar-standar ini menyediakan kerangka kerja untuk manajemen risiko keamanan informasi, pengendalian akses, dan tata kelola IT, yang semuanya krusial dalam melindungi data pajak dari ancaman siber.

Selain standar industri, regulasi seperti HIPAA untuk sektor kesehatan dan PCI DSS untuk industri kartu pembayaran juga memberikan wawasan tentang keamanan data dan privasi yang dapat diterapkan dalam konteks data pajak. Implementasi kebijakan dan prosedur yang sesuai dengan standar dan regulasi ini memastikan bahwa organisasi tidak hanya melindungi data pajak secara efektif tetapi juga mematuhi persyaratan hukum dan industri yang relevan.

Integrasi cybersecurity dalam proses audit pajak memerlukan pemahaman yang mendalam tentang terminologi kunci dan konsep pengembangan kebijakan. Hal ini mencakup identifikasi aset informasi kritikal, penilaian risiko keamanan informasi, dan pengembangan strategi untuk mitigasi risiko tersebut. Kebijakan dan prosedur keamanan yang efektif harus disertai dengan pedoman implementasi, contoh praktik terbaik, dan daftar periksa untuk memastikan penerapan yang konsisten dan efektif.

Referensi seperti panduan Landoll (2017) menjadi sangat berharga dalam proses ini, menawarkan struktur dokumen yang disarankan, sinopsis standar keamanan informasi yang berlaku, dan pedoman praktis untuk pengembangan kebijakan dan prosedur. Dengan mengadopsi pendekatan yang berbasis standar dan regulasi,

organisasi dapat membangun kerangka kerja keamanan informasi yang robust, yang tidak hanya melindungi data pajak tetapi juga mendukung integritas dan kepercayaan dalam sistem audit pajak.

Dengan demikian, kebijakan dan prosedur keamanan yang kuat tidak hanya menjadi kunci dalam menjaga keamanan data pajak tetapi juga memainkan peran penting dalam meningkatkan efektivitas audit pajak, menjamin kepatuhan, dan memperkuat posisi keamanan siber secara keseluruhan. Hal ini menuntut komitmen berkelanjutan terhadap pembaruan dan penyesuaian kebijakan sesuai dengan perkembangan teknologi dan ancaman siber yang terus berubah.

2.3.2.2 Benchmark Implementasi Global

A. Internal Revenue Service (IRS), Amerika Serikat

IRS telah mengadopsi pendekatan multi-faset terhadap keamanan siber yang mencakup kolaborasi strategis dengan sektor swasta dan lembaga keuangan, peningkatan prosedur otentikasi, dan penerapan program kepatuhan untuk penyedia layanan pajak.

1) Kolaborasi IRS dengan sektor swasta, khususnya lembaga keuangan, merupakan inisiatif penting dalam mengidentifikasi dan menerapkan praktik keamanan siber terbaik. Kemitraan ini memungkinkan pertukaran informasi tentang ancaman siber dan strategi penipuan yang berkembang, yang sangat penting dalam membangun pertahanan yang lebih kuat terhadap serangan siber.

2) IRS telah memperkuat prosedur otentikasi untuk mencegah akses tidak sah, termasuk penerapan otentikasi dua faktor, pertanyaan keamanan yang lebih kompleks, dan teknologi biometrik. Langkah-langkah ini bertujuan untuk memastikan bahwa hanya individu yang berwenang yang dapat mengakses data pajak sensitif.
3) Program kepatuhan IRS memastikan bahwa penyedia layanan pajak mengikuti standar keamanan yang ketat, termasuk kebijakan dan prosedur untuk melindungi data pelanggan, audit keamanan reguler, dan pelatihan keamanan siber untuk staf.

Studi kasus IRS menyoroti pentingnya pendekatan holistik terhadap keamanan siber dalam konteks audit pajak, yang mencakup penguatan keamanan internal dan kolaborasi eksternal. Implementasi strategi ini oleh IRS berfungsi sebagai benchmark bagi administrasi pajak lainnya di seluruh dunia dalam memerangi ancaman siber yang berkembang. Kunci dari keberhasilan ini adalah adaptasi terhadap ancaman yang terus berubah, kolaborasi antar-sektor, dan komitmen terhadap kepatuhan dan pelatihan yang berkelanjutan.

B. HM Revenue & Customs (HMRC), Inggris

HMRC telah menetapkan keamanan data sebagai prioritas utama dalam pengelolaan informasi pajak, mengimplementasikan langkah-langkah keamanan yang ketat untuk melindungi data yang disimpan dan diproses. Hal ini mencakup penerapan solusi teknologi informasi dan prosedur operasional yang dirancang untuk mengamankan

data dari akses tidak sah dan ancaman siber. Keamanan data di HMRC mencerminkan pengakuan bahwa integritas dan kerahasiaan data pajak adalah fundamental untuk menjaga kepercayaan publik dalam sistem perpajakan.

HMRC menerapkan berbagai teknologi keamanan canggih, termasuk enkripsi data, firewall, dan sistem deteksi intrusi, serta otentikasi kuat. Penerapan teknologi ini menunjukkan komitmen HMRC untuk menggunakan solusi keamanan terdepan dalam melindungi informasi sensitif dan infrastruktur TI dari serangan siber.

Pentingnya pelatihan dan kesadaran keamanan siber diakui oleh HMRC sebagai komponen kunci dalam strategi keamanan. Dengan menyediakan pelatihan reguler dan memperbarui kebijakan keamanan, HMRC bertujuan untuk meminimalkan risiko pelanggaran data yang disebabkan oleh faktor manusia. Hal ini mencerminkan pemahaman bahwa teknologi keamanan saja tidak cukup tanpa penggunaan yang tepat oleh karyawan yang terinformasi.

HMRC berkolaborasi dengan lembaga lain di sektor publik dan swasta untuk berbagi pengetahuan dan strategi terbaik dalam melawan ancaman siber. Kolaborasi ini memungkinkan pertukaran informasi tentang ancaman terkini dan pengembangan solusi keamanan bersama, menunjukkan pentingnya kerja sama dan koordinasi dalam menghadapi ancaman siber yang kompleks.

HMRC menunjukkan bahwa integrasi cybersecurity dalam proses audit pajak memerlukan pendekatan komprehensif yang mencakup penggunaan teknologi keamanan terdepan, pengembangan kesadaran dan pelatihan keamanan siber, serta kerjasama antar lembaga.

Langkah-langkah yang diambil oleh HMRC menekankan pentingnya menjaga keamanan data pajak sebagai bagian dari upaya lebih luas untuk menjaga kepercayaan publik dalam sistem perpajakan.

Implementasi strategi keamanan oleh HMRC dapat dijadikan benchmark bagi badan pajak lain di seluruh dunia dalam upaya menghadapi tantangan keamanan siber. Mempelajari dan mengadaptasi praktik terbaik dari HMRC dapat membantu administrasi pajak lain meningkatkan keamanan data pajak dan menghadapi ancaman siber dengan lebih efektif, memastikan integritas dan kepercayaan dalam sistem pajak nasional.

C. BSI Jerman hingga ACSC Australia

1) Bundesamt für Sicherheit in der Informationstechnik (BSI), Jerman
   BSI Jerman berperan sebagai otoritas keamanan siber nasional, mengimplementasikan langkah-langkah komprehensif untuk mengamankan infrastruktur kritis dan data pemerintah. Fokus BSI pada identifikasi dan mitigasi ancaman siber, pengembangan standar keamanan TI, dan kerjasama internasional menunjukkan pendekatan proaktif dan kolaboratif dalam menghadapi ancaman siber. Kunci keberhasilan BSI terletak pada kemampuannya untuk menggabungkan teknologi canggih, kebijakan yang ketat, dan kerjasama lintas batas untuk memperkuat keamanan siber nasional.
2) Australian Cyber Security Centre (ACSC), Australia
   ACSC Australia berfungsi sebagai hub kolaborasi untuk meningkatkan keamanan siber, menggabungkan

sumber daya dan keahlian dari sektor publik dan swasta. Dengan menyediakan panduan keamanan, dukungan respons insiden, dan layanan informasi ancaman, ACSC mempromosikan pendekatan yang inklusif dan adaptif terhadap keamanan siber. Inisiatif ACSC dalam meningkatkan kesadaran dan mengembangkan kerangka kerja keamanan yang kuat memperlihatkan pentingnya kolaborasi dan pendidikan dalam membangun ketahanan siber.

3) Inovasi Global dalam Audit Pajak dan Keamanan Siber
Berbagai negara telah mengadopsi pendekatan inovatif untuk mengintegrasikan keamanan siber ke dalam audit pajak, dengan teknologi dan data analytics.

- Australia.
  Pengembangan alat pencocokan data keuangan yang memungkinkan analisis transaksi yang akurat dan efisien, menyoroti pentingnya teknologi dalam mendeteksi dan mengurangi kesenjangan pajak.
- Austria
  Adopsi inovasi digital untuk penilaian risiko dan audit real-time, menunjukkan bagaimana digitalisasi dapat meningkatkan responsivitas otoritas pajak terhadap dinamika perubahan.
- Kanada
  Penerapan alat investigasi forensik digital dan peningkatan layanan melalui analisis data lanjutan, menyoroti pentingnya keahlian forensik dalam mengungkap penipuan dan penghindaran pajak.
- Italia
  Implementasi metodologi yang dibantu oleh machine learning untuk mengestimasi kesenjangan

VAT, menggambarkan bagaimana AI dapat meningkatkan akurasi dan efisiensi dalam administrasi pajak.

- Argentina hingga Spanyol
  Dari penggunaan Buku Pajak Digital VAT untuk mempermudah pengembalian pajak hingga analisis umpan balik untuk meningkatkan kepatuhan sukarela, berbagai strategi menunjukkan pentingnya inovasi dan adaptasi teknologi dalam memperkuat sistem pajak.

BAB III

Eksplorasi Literatur Big Data Analytic (BDA) dan Business Inteligence (BI) dan Integrasinya dengan Audit Pajak

3.1 Konsep Big Data Analytic

3.1.1 Pengertian dan Tujuan Big Data Analytic

Dalam era digital saat ini, analisis data telah berkembang menjadi proses yang secara signifikan otomatis atau mekanis, memungkinkan identifikasi informasi berharga dari sekumpulan data yang beragam dan kompleks.

A. Pengertian Big Data Analytic

Analisis data melibatkan integrasi dari berbagai ilmu dan teknologi untuk meningkatkan efisiensi operasional dan kinerja bisnis. Meskipun istilah analisis data dan ilmu data sering kali digunakan secara bergantian, keduanya memiliki fokus yang berbeda. Analisis data lebih terfokus pada proses dan fungsi pengolahan data, khususnya dalam hal ekstraksi informasi dan pembuatan laporan yang bermanfaat. Sementara itu, ilmu data mencakup spektrum yang lebih luas, termasuk pembersihan data sebagai langkah awal yang penting untuk penyelidikan data lebih lanjut. Dengan

demikian, kedua disiplin ilmu tersebut saling melengkapi dalam menerapkan data untuk solusi bisnis yang lebih efektif dan inovatif (Lu, 2019; Ahmed, 2017). Melalui pendekatan yang terstruktur dan metodologi yang canggih, analisis dan ilmu data bersama-sama memfasilitasi organisasi dalam menggali wawasan dari data besar, membantu dalam pengambilan keputusan strategis yang berbasis data, dan mengoptimalkan proses bisnis.

Konsep analitik data besar merujuk pada serangkaian mekanisme untuk menggali wawasan dan informasi yang bernilai dari kumpulan data yang masif. Proses ini mencakup tahapan pengumpulan, organisasi, dan analisis atas volume data yang ekstensif, dengan tujuan untuk mengidentifikasi pola-pola dan informasi yang tidak hanya berguna tetapi juga memiliki makna signifikan. Analitik data besar memanfaatkan kumpulan teknologi dan metodologi yang beragam, memerlukan integrasi teknik baru untuk menyingkap nilai yang tersembunyi dalam data kompleks tersebut. Fokus utama dari analitik data besar adalah pada penyelesaian masalah, baik yang bersifat baru maupun yang telah lama ada, dengan pendekatan yang lebih efisien. Hal ini menuntut sebuah paradigma yang inovatif dalam melihat dan mengolah data, di mana efisiensi dan efektivitas menjadi kunci dalam mendekripsi makna dari data tersebut (Verma et al., 2016).

B. Proses Analisis Data

Proses analisis data, seperti yang diuraikan oleh Arora dan Malik (2015), melibatkan beberapa langkah kritis yang dimulai dari penentuan kebutuhan data hingga analisis data itu sendiri. Langkah-langkah tersebut adalah sebagai berikut:

1) menentukan persyaratan data, yang meliputi pengelompokan data berdasarkan variabel tertentu seperti usia, jenis kelamin, atau pendapatan. Pengelompokan ini memudahkan identifikasi dan analisis pola dalam data.
2) mengidentifikasi dan mengakses sumber data yang relevan. Data bisa berasal dari berbagai sumber, termasuk komputer, media, platform online, dan sumber personel. Setelah data terkumpul, penting untuk mengorganisir data tersebut sesuai dengan kebutuhan analisis.
3) fokus pada pembersihan data. Pada tahap ini, data yang duplikat, hilang, atau tidak lengkap diidentifikasi dan dikoreksi. Pembersihan data adalah langkah penting untuk memastikan keakuratan dan keandalan analisis.
4) setelah data berada dalam kondisi yang tepat, proses analisis data dapat dilakukan. Analisis ini dapat mencakup berbagai teknik statistik atau pemodelan data untuk mengungkap wawasan dan pola yang tersembunyi dalam data.

Proses analisis data ini mencerminkan pendekatan sistematis dalam mengelola dan memanfaatkan data untuk pengambilan keputusan yang berbasis bukti. Melalui langkah-langkah yang dijelaskan oleh Arora dan Malik (2015), organisasi dapat memperoleh pemahaman yang lebih dalam tentang data, yang pada gilirannya dapat membantu dalam strategi dan operasi bisnis.

C. Tujuan Big Data Analytic (BDA)

Tujuan utama dari Big Data Analytics (BDA) adalah untuk mengubah data besar dan kompleks menjadi wawasan yang dapat ditindaklanjuti, memungkinkan organisasi untuk membuat keputusan yang lebih tepat dan meningkatkan efisiensi operasional. BDA membantu dalam mengidentifikasi tren, pola, dan hubungan dalam data yang sebelumnya tidak terlihat, yang dapat digunakan untuk mengoptimalkan strategi bisnis, meningkatkan pengalaman pelanggan, dan memperkuat keunggulan kompetitif.

Menurut Schönberger & Cukier (2014), Provost & Fawcett (2013) Tujuan dari Analitik Data Besar (BDA):

1) Pengambilan Keputusan yang Lebih Baik
   Pengambilan keputusan yang lebih baik dengan menyediakan wawasan yang diperoleh dari analisis jumlah data yang sangat besar. Hal ini memungkinkan organisasi untuk lebih efektif memahami tren pasar, perilaku pelanggan, dan ketidakefisienan operasional.
2) Meningkatkan Pengalaman Pelanggan
   BDA membantu bisnis memahami kebutuhan, preferensi, dan perilaku pelanggan secara mendalam, memungkinkan untuk menawarkan pengalaman, produk, dan layanan yang dipersonalisasi. Personalisasi ini dapat menyebabkan peningkatan kepuasan dan loyalitas pelanggan.
3) Efisiensi Operasional
   Dengan menganalisis set data yang besar, organisasi dapat mengidentifikasi hambatan dan ketidakefisienan dalam operasi. BDA memungkinkan untuk merampingkan proses, mengurangi biaya, dan meningkatkan efisiensi keseluruhan.

4) Inovasi dan Pengembangan Produk Baru
   Wawasan yang diperoleh dari BDA dapat menginformasikan pengembangan produk dan layanan baru. Dengan memahami tren yang muncul dan kebutuhan pelanggan, perusahaan dapat berinovasi untuk tetap unggul dari kompetisi.

D. Dukungan BDA terhadap Bisnis

Penggunaan metode analisis data yang canggih seperti pembelajaran mesin (Machine Learning, ML), analisis teks, pemrosesan bahasa alami (Natural Language Processing, NLP), analisis prediktif, dan statistik memainkan peran kunci dalam memanfaatkan data yang belum terpakai untuk menghasilkan wawasan baru (Verma et al., 2016). Metode ini secara teknis mendukung pengambilan keputusan yang lebih baik dan lebih cepat dengan cara berikut:

1) Pembelajaran Mesin (ML)
   Machine Learning menurut Provost & Fawcett (2013), memungkinkan komputer untuk belajar dari data tanpa diprogram secara eksplisit. Dalam konteks BDA, ML digunakan untuk mengidentifikasi pola dan membuat prediksi berdasarkan data historis. Algoritme ML dapat diterapkan untuk berbagai tugas, seperti klasifikasi, regresi, dan clustering.
2) Analisis Teks
   Teknik ini melibatkan pengolahan dan analisis data teks untuk menggali informasi berguna. Analisis teks dapat digunakan untuk sentiment analysis, ekstraksi entitas bernama, dan kategorisasi teks, membantu organisasi memahami opini dan preferensi pelanggan.
3) Pemrosesan Bahasa Alami (NLP)

NLP menurut Provost & Fawcett (2013), memungkinkan mesin untuk memahami dan menginterpretasikan bahasa manusia. Dalam BDA, NLP digunakan untuk menganalisis data teks besar, seperti ulasan pelanggan atau postingan media sosial, untuk mengidentifikasi tren dan sentimen.

4) Analisis Prediktif
   Metode ini menggunakan data historis dan algoritme statistik untuk membuat prediksi tentang masa depan. Analisis prediktif dapat membantu perusahaan dalam perencanaan sumber daya, manajemen risiko, dan pengembangan strategi pemasaran yang ditargetkan.
5) Statistik
   Teknik statistik tradisional tetap relevan dalam BDA untuk menganalisis data dan menyimpulkan pola. Analisis regresi, analisis varians (ANOVA), dan uji hipotesis adalah beberapa contoh bagaimana statistik diterapkan dalam BDA.

Penggunaan metode analisis canggih ini dalam BDA memungkinkan organisasi untuk lebih efektif dalam mengungkap pola tersembunyi, memahami preferensi pelanggan, dan mengikuti tren pasar, yang pada akhirnya dapat mengarah pada pemasaran yang lebih berhasil dan peningkatan layanan pelanggan.

3.1.2 Pentingnya Analisis Big Data

Analisis Big Data memiliki peran penting dalam berbagai aspek kehidupan dan bisnis, mengubah data menjadi aset perusahaan yang berharga dan menjadi dasar bagi model bisnis baru, seperti yang diungkapkan oleh Hirsch (2013).

Big Data Analytics (BDA) dalam konteks bisnis merupakan faktor penting yang mengubah cara perusahaan beroperasi, membuat keputusan, dan berinteraksi dengan pelanggan. Berikut ini adalah beberapa poin kunci yang menekankan pentingnya BDA dalam bisnis, disertai dengan sumber referensi untuk penjelasan yang lebih mendalam:

1) BDA memungkinkan perusahaan untuk membuat keputusan strategis berdasarkan analisis data yang komprehensif, bukan hanya intuisi atau pengalaman masa lalu. Hal ini meningkatkan akurasi dan efektivitas keputusan yang diambil (Provost & Fawcett, 2013).
2) Dengan menganalisis data pelanggan secara besar-besaran, perusahaan dapat menawarkan layanan yang lebih personalisasi, meningkatkan kepuasan dan loyalitas pelanggan. BDA membantu dalam mengidentifikasi preferensi pelanggan dan perilaku pembelian, memungkinkan perusahaan untuk menyesuaikan penawaran (Mayer-Schönberger & Cukier, 2014).
3) BDA dapat mengidentifikasi inefficiencies dan bottleneck dalam operasional perusahaan. Dengan ini, perusahaan dapat merampingkan proses, mengurangi biaya, dan meningkatkan produktivitas (Provost & Fawcett, 2013).

4) Analisis tren pasar dan feedback pelanggan melalui BDA dapat mendorong inovasi dan membantu dalam pengembangan produk atau layanan baru yang sesuai dengan kebutuhan pasar (Mayer-Schönberger & Cukier, 2014.

Pentingnya Big Data Analytics (BDA) dalam konteks pemerintahan terutama terletak pada kemampuannya untuk meningkatkan pengambilan keputusan, efisiensi operasional, dan pelayanan publik. Beberapa poin utama yang menggambarkan peranan vital BDA di sektor pemerintahan (SGS. 2023):

1) BDA memungkinkan pemerintah untuk mengidentifikasi tren dan wawasan yang memfasilitasi pengambilan keputusan yang lebih cepat dan tepat. Analisis data yang akurat memungkinkan pemerintah untuk mengklasifikasikan populasi berdasarkan berbagai faktor seperti tingkat pendapatan, kesehatan, jenis kelamin, dan usia dalam hitungan detik, yang secara langsung mendukung penerapan kebijakan dan strategi pemerintah yang spesifik.
2) BDA membantu mengatasi tantangan penyimpanan data yang dihadapi oleh lembaga pemerintah. Dengan menggunakan platform big data, data yang sama tidak perlu dikumpulkan berkali-kali untuk setiap kebutuhan lembaga, mengurangi biaya, waktu, dan potensi kesalahan. Selain itu, penyimpanan data terpusat memudahkan akses lintas lembaga.
3) Big Data berperan penting dalam mengungkap kejahatan dan aktivitas ilegal lainnya yang mengancam keamanan masyarakat. Analisis data yang teliti dapat membantu mengidentifikasi pola aktivitas

mencurigakan yang menunjukkan penipuan atau kejahatan, sehingga memungkinkan tindakan pencegahan atau penindakan yang cepat.

4) Analisis big data dapat digunakan untuk mengidentifikasi dan merespons bencana alam atau masalah kesehatan, seperti pandemi, sebelum terjadi. Data dari berbagai sumber, termasuk organisasi kesehatan dan catatan kota, dapat digunakan untuk mengidentifikasi penyebaran penyakit dan memberikan bantuan segera kepada bagian masyarakat yang membutuhkan.
5) Pengembangan platform big data dan penerapan analitik big data memungkinkan semua lembaga pemerintah mengakses data dari sumber tunggal dan bekerja dalam arah yang sama. Hal ini meminimalisir keterlambatan dalam berbagi informasi antar departemen dan meningkatkan akurasi data.

BDA menawarkan berbagai manfaat bagi sektor pemerintahan, termasuk peningkatan dalam pengambilan keputusan, efisiensi operasional, dan kualitas layanan publik. Implementasi dan pemanfaatan teknologi analitik data besar di sektor pemerintahan tidak hanya mendukung pengelolaan sumber daya yang lebih efektif tetapi juga membantu dalam memperkuat keamanan masyarakat dan meningkatkan kesejahteraan warga.

3.2 Teknik Analitik yang Digunakan BDA

Penggunaan teknik analitik dalam konteks Big Data Analytics (BDA) yang beragam memainkan peran krusial dalam mengolah dan memaknai volume data yang besar dan kompleks. Menurut Provost & Fawcett (2013), berikut adalah teknik analitik utama yang digunakan dalam BDA:

1) Data Mining
   Merupakan inti dari BDA, di mana proses ekstraksi pola dan hubungan yang signifikan dari kumpulan data besar dilakukan. Melalui teknik seperti klasterisasi, klasifikasi, dan asosiasi, data mining memungkinkan identifikasi struktur dalam data yang sebelumnya tidak diketahui.
2) Machine Learning (ML)
   ML memperkenalkan kemampuan bagi sistem untuk 'belajar' dan mengembangkan prediksi atau keputusan dari dataset, dengan membedakan antara pembelajaran terawasi dan tidak terawasi. ML mendorong otomatisasi analisis data dan memfasilitasi model yang dapat beradaptasi dengan data baru.
3) Analisis Statistik
   Menggunakan teknik statistik untuk menguji hipotesis dan memvalidasi asumsi tentang data. Analisis statistik, baik deskriptif maupun inferensial, menyediakan dasar untuk pemahaman kuantitatif tentang fenomena yang diamati dalam dataset.
4) Visualisasi Data
   Dengan memanfaatkan alat visualisasi, data disajikan secara intuitif, memudahkan identifikasi pola dan tren. Visualisasi data adalah sarana komunikasi yang efektif antara analis data dengan pemangku kepentingan.

5) Tekstual dan Analisis Sentimen
   Teknik ini menganalisis data teks untuk ekstraksi informasi, klasifikasi sentimen, dan identifikasi tren dalam komunikasi teksual, seperti media sosial atau ulasan produk.
6) Deep Learning
   Sebagai evolusi dari ML, deep learning menggunakan jaringan saraf tiruan untuk menganalisis data yang sangat kompleks. Efektivitasnya terutama terlihat dalam pengenalan pola, seperti pengenalan gambar dan pengolahan bahasa alami.
7) Analisis Waktu Seri
   Teknik ini khusus digunakan untuk menganalisis data yang dikumpulkan dalam interval waktu yang teratur, memungkinkan pengamatan tren, siklus, dan fluktuasi seiring waktu.
8) Pengolahan Bahasa Alami (NLP)
   NLP memungkinkan mesin untuk memahami dan memproses bahasa manusia, memfasilitasi interaksi antara manusia dan komputer dan memungkinkan analisis konten teks skala besar.

Penggabungan berbagai teknik analitik ini dalam BDA menyediakan landasan untuk menggali wawasan mendalam dari data, mendukung pengambilan keputusan yang berbasis bukti, dan memungkinkan inovasi berkelanjutan dalam lingkungan bisnis dan penelitian. Melalui aplikasi teknik-teknik ini, organisasi dapat memanfaatkan potensi penuh dari big data, mengarah pada peningkatan efisiensi operasional, pengembangan produk, dan strategi bisnis yang lebih dinamis.

3.3 Peran BDA dalam Audit Pajak

3.3.1 Peran BDA dalam Pengembangan Inovatif Audit Pajak

Pendekatan berbasis data memanfaatkan volume data pajak yang besar dan beragam dari berbagai sumber, termasuk laporan keuangan, transaksi elektronik, dan komunikasi digital. Analitik data besar memungkinkan identifikasi pola dan tren yang tidak dapat ditemukan dengan metode tradisional.

Pentingnya teknologi informasi, peralatan teknis, dan kualifikasi pejabat pajak dalam pengembangan ekonomi yang inovatif dijelaskan Madina et al., 2020 dari beberapa aspek teknis:

1) Penggunaan teknologi informasi dalam audit pajak memungkinkan analisis data besar secara lebih efisien dan akurat. Teknologi seperti analitik data besar (Big Data Analytics - BDA) memungkinkan otoritas pajak untuk mengidentifikasi pola, anomali, dan potensi penghindaran pajak dengan memproses volume data yang sangat besar dengan cepat. Teknologi ini secara signifikan mengurangi waktu yang dibutuhkan untuk audit dan meningkatkan akurasi hasil audit.
2) Teknologi informasi memungkinkan automasi proses-proses audit pajak, yang mengurangi beban kerja manual dan mempercepat proses audit. Automasi ini meliputi pengumpulan data, klasifikasi, dan analisis transaksi yang dilaporkan oleh wajib pajak. Dengan demikian, memungkinkan pejabat pajak untuk fokus pada aspek yang lebih strategis dari audit pajak, seperti investigasi kasus penghindaran pajak yang kompleks.

3) Implementasi teknologi informasi dalam sistem pajak meningkatkan transparansi dan memudahkan kepatuhan pajak. Sistem elektronik memungkinkan wajib pajak untuk mengakses informasi tentang kewajiban pajak secara real-time, mengajukan pajak secara online, dan menerima pembaruan status audit. Hal ini memudahkan wajib pajak untuk mematuhi peraturan pajak dan mengurangi risiko kesalahan atau ketidakpatuhan.
4) Penggunaan teknologi informasi yang maju dalam audit pajak memerlukan pejabat pajak yang memiliki kualifikasi khusus, termasuk pengetahuan tentang analitik data, keamanan siber, dan hukum pajak. Pelatihan dan pengembangan kompetensi terus-menerus bagi pejabat pajak sangat penting untuk memastikan bahwa pejabat pajak dapat menggunakan teknologi informasi secara efektif dalam audit pajak dan pengembangan ekonomi yang inovatif.

3.3.2 Peran BDA dalam Pengolahan Data Audit Pajak

Analitik Data Besar (Big Data Analytics - BDA) memiliki potensi yang signifikan dalam meningkatkan efisiensi audit pajak, seperti yang dijelaskan dalam dokumen oleh Madina et al. (2020). Penggunaan BDA dalam audit pajak memungkinkan otoritas pajak untuk mengolah dan menganalisis volume data yang besar dengan cepat dan akurat, yang bisa meningkatkan efektivitas pengumpulan pajak dan mengidentifikasi penghindaran pajak dengan lebih efisien.

BDA memungkinkan analisis korelasi antara tingkat beban pajak dan intensitas aktivitas inovatif di berbagai sektor ekonomi. Dengan menggunakan metode statistik dan algoritma machine learning, peneliti dapat mengidentifikasi apakah beban pajak yang tinggi berkontribusi pada penurunan investasi dalam R&D dan inovasi.

Metode dalam BDA untuk Penilaian Efisiensi Audit Pajak:

1) Menggunakan teknik analitik prediktif, seperti machine learning dan data mining, untuk mengidentifikasi pola dan anomali yang menunjukkan potensi penghindaran pajak. Hal ini memungkinkan otoritas pajak untuk memprioritaskan sumber daya audit lebih efektif.
2) Analisis sentiment dan tekstual pada komunikasi elektronik dan media sosial dapat memberikan wawasan tentang perilaku wajib pajak dan persepsi terhadap sistem pajak. Teknik ini bisa membantu dalam mengidentifikasi area risiko dan meningkatkan kepatuhan pajak.
3) Penerapan visualisasi data dalam BDA memungkinkan auditor untuk memahami kompleksitas data pajak dengan lebih baik dan mengidentifikasi tren atau pola yang tidak jelas melalui metode tradisional.

3.3.3 Peran BDA dalam Transformasi Interaksi Entitas Publik

Transformasi interaksi antara entitas sektor publik dan wajib pajak melalui penerapan analitik data besar (Big Data Analytics - BDA) dan data terbuka (open data) merupakan proses yang kompleks dan multifaset, yang mencakup aspek

politik, legislatif, dan teknologi. Seperti yang dijelaskan dalam dokumen oleh Madina et al. (2020), aspek yang melingkupi peran BDA meliputi:

1) Aspek Politik
    a) Penerapan BDA dalam audit pajak memerlukan dukungan kebijakan publik yang kuat, termasuk investasi dalam teknologi informasi dan infrastruktur data. Hal ini juga melibatkan pembuatan kebijakan yang mendorong transparansi dan penggunaan data terbuka oleh pemerintah.
    b) Transformasi ini mendorong pengambilan keputusan berbasis data dalam pemerintahan, di mana kebijakan dan praktik audit pajak didasarkan pada analisis data komprehensif, bukan hanya intuisi atau proses tradisional.
2) Aspek Legislatif
    a) Transformasi ini memerlukan pengembangan dan pembaruan regulasi yang mengatur pengumpulan, pengolahan, dan pembagian data, termasuk aspek privasi dan keamanan data pribadi wajib pajak.
    b) Pengembangan kerangka hukum yang mendukung inisiatif data terbuka sangat penting, memungkinkan akses dan penggunaan dataset oleh publik dan meningkatkan transparansi pemerintah.
3) Aspek Teknologi
    a) Pembangunan dan peningkatan infrastruktur TI yang memadai adalah dasar implementasi BDA dan data terbuka. Hal ini termasuk penyimpanan

data, komputasi awan, dan teknologi keamanan data.

b) Transformasi melibatkan integrasi antara berbagai sistem TI di sektor publik, termasuk sistem administrasi pajak, keuangan, dan lainnya, untuk memudahkan pertukaran dan analisis data.
c) Penerapan teknologi BDA memungkinkan analisis volume data yang besar dan beragam dari berbagai sumber dalam waktu nyata atau hampir nyata, meningkatkan efektivitas audit pajak dan kepatuhan pajak.
d) Publikasi dataset oleh pemerintah sebagai bagian dari inisiatif data terbuka memungkinkan peneliti, pengembang, dan masyarakat umum untuk mengakses dan menggunakan data untuk berbagai tujuan, termasuk pengembangan aplikasi, analisis, dan inovasi sosial.

Transformasi interaksi antara entitas sektor publik dan wajib pajak melalui BDA dan data terbuka berdampak luas terhadap peningkatan transparansi, efisiensi, dan akuntabilitas dalam administrasi pajak. Hal ini dapat mempromosikan partisipasi masyarakat dan inovasi berbasis data, yang pada gilirannya dapat meningkatkan kepercayaan publik terhadap pemerintah dan sistem pajak.

3.3.4 Peran BDA dalam Pergeseran Audit Pajak

Penggunaan sumber data internal dan eksternal melalui teknologi data besar (Big Data Analytics - BDA) dan data terbuka dalam audit pajak menandai pergeseran signifikan dalam cara audit dilaksanakan, menawarkan pendekatan yang lebih komprehensif dan akurat.

A. Sumber Data Internal dan Eksternal

Peran Big Data Analytics (BDA) dalam memanfaatkan sumber data internal dan eksternal telah mengubah paradigma tradisional menjadi pendekatan yang lebih inovatif dan efektif. Sumber data internal, yang terdiri dari informasi yang dikumpulkan langsung oleh otoritas pajak dari wajib pajak, seperti laporan tahunan, deklarasi pajak, dan berbagai dokumen keuangan lainnya, tetap menjadi tulang punggung audit pajak. Data ini memberikan dasar yang solid untuk menilai kewajiban pajak dan kepatuhan wajib pajak dengan ketentuan yang berlaku.

Data eksternal membuka jendela baru untuk memperkaya analisis dan pengawasan pajak dengan perspektif yang lebih luas, termasuk data transaksi elektronik dari bank dan lembaga keuangan, yang bisa mengungkap pola transaksi yang tidak dilaporkan atau tidak konsisten dengan laporan keuangan yang disampaikan. Informasi dari media sosial dan database publik, menawarkan wawasan tentang aktivitas ekonomi wajib pajak yang tidak tercermin dalam data internal. Data pasar dapat menyediakan informasi tentang standar industri dan benchmarking, yang membantu dalam menilai kepatuhan dan risiko pajak dengan lebih akurat.

Integrasi dan analisis dari kedua sumber data ini melalui teknologi BDA memungkinkan otoritas pajak untuk mendapatkan pemahaman yang lebih mendalam dan komprehensif tentang perilaku wajib pajak. Dengan memanfaatkan algoritma canggih dan kapasitas pemrosesan data besar, BDA membantu dalam mengidentifikasi anomali, pola transaksi yang mencurigakan, dan potensi kasus

penghindaran pajak dengan kecepatan dan akurasi yang belum pernah ada sebelumnya.

B. Teknologi Data Besar dan Data Terbuka

Teknologi Data Besar (Big Data Analytics) dan Data Terbuka memainkan peran kunci dalam merevolusi praktik audit pajak, membawa kapasitas analitis yang belum pernah terjadi sebelumnya untuk meningkatkan efisiensi dan akurasi audit. Teknologi Data Besar memanfaatkan algoritma dan teknik analitik canggih untuk mengolah dan menganalisis volume data yang besar, beragam, dan berkecepatan tinggi. Alat seperti Hadoop dan Spark memungkinkan pengolahan data terdistribusi secara efisien, sedangkan sistem manajemen basis data NoSQL menawarkan fleksibilitas dalam mengelola data yang tidak terstruktur (semi-terstruktur), seperti teks atau log transaksi, yang seringkali merupakan bagian dari audit pajak.

Data Terbuka berkontribusi terhadap transparansi dan kepatuhan pajak dengan menyediakan akses terhadap set data yang dapat digunakan dan dibagikan oleh publik. Dalam konteks audit pajak, ini berarti otoritas pajak dapat memanfaatkan informasi publik, seperti data registrasi bisnis, properti, dan informasi lainnya yang relevan, untuk memperkaya analisis. Integrasi antara Data Besar dan Data Terbuka memungkinkan pembentukan gambaran yang lebih komprehensif tentang aktivitas ekonomi subjek pajak, memfasilitasi identifikasi potensi penghindaran pajak dan memperkuat kepatuhan pajak secara keseluruhan.

C. Implementasi Teknis

Implementasi teknis dalam konteks Big Data Analytics (BDA) untuk audit pajak melibatkan serangkaian proses yang canggih dan terintegrasi, dimulai dengan pengumpulan dan integrasi data. Dalam tahap ini, data dari berbagai sumber, baik internal seperti laporan keuangan, deklarasi pajak, maupun eksternal seperti transaksi elektronik, media sosial, dan database public, dikumpulkan dan diintegrasikan menggunakan teknologi ETL (Extract, Transform, Load). Proses ETL memungkinkan data yang beragam dan tersebar untuk diekstraksi dari sumbernya, ditransformasi ke format yang seragam dan konsisten, serta dimuat ke dalam sistem manajemen data terpusat untuk analisis lebih lanjut. Hal ini memastikan bahwa data siap untuk dianalisis secara efektif dan efisien.

Pada tahap analisis data, teknik analitik canggih seperti machine learning, data mining, dan analisis prediktif digunakan (Osama, 2021). Machine learning memungkinkan sistem untuk belajar dari data dan mengidentifikasi pola tanpa diprogram secara eksplisit, sedangkan data mining menggali informasi berharga dari kumpulan data besar, dan analisis prediktif menggunakan data historis dan tren saat ini untuk memprediksi perilaku di masa depan. Dalam konteks audit pajak, teknik-teknik ini dapat mengungkap pola transaksi yang tidak biasa, anomali, dan indikasi potensi penghindaran pajak atau kesalahan dalam pelaporan, memungkinkan otoritas pajak untuk fokus pada kasus-kasus yang paling berisiko.

Visualisasi data memainkan peran penting dalam menyajikan hasil analisis. Dengan menggunakan alat visualisasi data, temuan audit disajikan dalam format yang

mudah dipahami, memungkinkan auditor untuk dengan cepat dan intuitif mengidentifikasi area yang memerlukan investigasi lebih lanjut. Visualisasi dapat berupa grafik, peta panas, atau diagram yang mengilustrasikan pola, tren, dan hubungan dalam data, menjadikannya alat yang tak ternilai untuk menganalisis informasi kompleks dan membuat keputusan berbasis bukti. Proses implementasi teknis ini, dari pengumpulan data hingga visualisasi, mengoptimalkan kapasitas audit pajak, mengarah pada audit yang lebih akurat, komprehensif, dan efisien.

D. Manfaat

Penerapan Big Data Analytics (BDA) dalam audit pajak memberikan sejumlah manfaat signifikan yang mengubah landskap administrasi pajak. Pertama, integrasi sumber data internal dan eksternal secara substansial memperkaya basis data yang tersedia untuk analisis, yang secara langsung meningkatkan keakuratan dan efisiensi audit. Dengan akses ke dataset yang lebih luas dan lebih beragam, auditor pajak dapat dengan lebih cepat mengidentifikasi risiko, anomali, dan ketidaksesuaian, memungkinkan alokasi sumber daya yang lebih tepat sasaran dan pengurangan waktu yang diperlukan untuk audit. Berarti bahwa audit dapat dilakukan dengan lebih cepat, mengurangi beban baik bagi otoritas pajak maupun wajib pajak.

Kemampuan untuk menganalisis data secara komprehensif dengan teknik BDA memungkinkan otoritas pajak untuk beralih dari pendekatan reaktif menjadi lebih proaktif dan prediktif. Melalui pemanfaatan analisis prediktif dan machine learning, otoritas pajak dapat mengidentifikasi potensi masalah pajak sebelum berkembang menjadi pelanggaran yang lebih serius,

memungkinkan intervensi dini dan mitigasi risiko. Pendekatan ini tidak hanya mengoptimalkan sumber daya tetapi juga mempromosikan lingkungan kepatuhan yang lebih baik dengan mengurangi peluang untuk penghindaran pajak.

Peningkatan dalam proses audit dan administrasi pajak melalui BDA mendorong transparansi yang lebih besar dalam sistem pajak. Dengan data dan proses analitik yang lebih terbuka, wajib pajak dapat memiliki pemahaman yang lebih baik tentang bagaimana kewajiban pajak ditentukan dan apa yang diharapkan dari wajib pajak, memperkuat kepercayaan dalam sistem pajak. Hal ini memungkinkan untuk dialog yang lebih konstruktif antara otoritas pajak dan wajib pajak, yang dapat menyebabkan peningkatan kepatuhan pajak secara keseluruhan. Kemampuan analitik yang ditingkatkan dan proses audit yang lebih transparan memberikan insentif bagi wajib pajak untuk mematuhi hukum pajak, mengurangi litigasi dan meningkatkan efisiensi pengumpulan pajak.

3.4 Aplikasi BDA dalam Audit Pajak

Big Data Analytics memainkan peran penting dalam memodernisasi dan meningkatkan proses audit pajak. Dengan menganalisis kumpulan data yang besar dan kompleks, Big Data Analytics membantu otoritas pajak dan auditor dalam mengidentifikasi risiko kepatuhan, menemukan pola yang tidak biasa, dan membuat keputusan berdasarkan bukti yang lebih akurat.

Big Data Analytics dalam audit pajak menyediakan sarana yang lebih efisien dan efektif untuk mengelola dan memproses data pajak yang besar. Hal ini tidak hanya

meningkatkan kemampuan auditor untuk mengidentifikasi risiko dan kekurangan kepatuhan tetapi juga memungkinkan pengalokasian sumber daya yang lebih baik dan pengambilan keputusan yang berdasarkan data. Seiring waktu, penerapan teknologi ini diharapkan menjadi lebih luas, membawa perubahan signifikan dalam cara otoritas pajak beroperasi dan mengaudit.

3.4.1 Aplikasi BDA dalam Identifikasi Risiko Kepatuhan Dalam Audit Pajak

Dengan memanfaatkan volume data transaksi yang besar, Big Data Analytics memungkinkan analisis data secara real-time atau hampir real-time, membuka jalan baru dalam mengidentifikasi perilaku yang mencurigakan atau tidak sesuai yang mungkin menunjukkan penghindaran pajak atau kesalahan pelaporan.

A. Identifikasi penggunaan BDA

Identifikasi Risiko Kepatuhan Menggunakan Big Data Analytics:

1) Teknologi ini memproses data transaksi yang terjadi secara real-time, memungkinkan deteksi dini aktivitas yang mencurigakan. Hal ini sangat penting dalam lingkungan bisnis saat ini di mana volume transaksi digital terus meningkat.
2) Algoritma canggih dan teknik machine learning digunakan untuk menganalisis dan membandingkan deklarasi pajak dan transaksi lainnya terhadap pola umum atau yang diharapkan. Teknologi ini mampu mengidentifikasi penyimpangan dari norma, yang mungkin menunjukkan upaya penghindaran pajak atau kesalahan dalam pelaporan.

3) Dengan memahami di mana risiko kepatuhan terbesar berada, auditor dapat menargetkan sumber daya dan inspeksi dengan lebih efisien. Hal ini meminimalkan gangguan terhadap bisnis yang patuh sementara meningkatkan tekanan pada entitas yang berisiko.

B. Aplikasi Praktis

1) Pembandingan Deklarasi Pajak
   Dengan menggunakan Big Data Analytics, auditor dapat membandingkan deklarasi pajak dari sebuah perusahaan dengan tren industri yang relevan atau dengan data historis perusahaan tersebut. Penyimpangan signifikan tanpa penjelasan yang memadai dapat memicu audit lebih lanjut.
2) Analisis Transaksi Lintas Batas
   Analisis data besar juga sangat berguna dalam mengidentifikasi transaksi lintas batas yang mencurigakan, yang sering kali rumit dan sulit untuk dilacak. Dengan memanfaatkan data dari berbagai sumber, auditor dapat mendeteksi skema penghindaran pajak seperti transfer pricing yang tidak sesuai.
3) Penggunaan Data Eksternal
   Integrasi data eksternal, seperti informasi dari database publik atau data transaksi elektronik dari lembaga keuangan, memperkaya analisis dan memberikan konteks tambahan untuk evaluasi risiko kepatuhan.

C. Manfaat Aplikasi BDA

Manfaat Aplikasi BDA dalam Identifikasi Risiko Kepatuhan Pajak:

1) Meningkatkan keakuratan deteksi risiko kepatuhan dengan mengurangi ketergantungan pada sampling dan pendekatan manual.
2) Memungkinkan otoritas pajak untuk bertindak secara proaktif dan responsif terhadap isu kepatuhan.
3) Mengoptimalkan alokasi sumber daya dengan memfokuskan upaya audit pada area dengan risiko tinggi.

Big Data Analytics tidak hanya memperkuat kemampuan auditor dalam mengidentifikasi dan mengelola risiko kepatuhan tetapi juga mendorong lingkungan kepatuhan yang lebih baik di kalangan wajib pajak, secara keseluruhan meningkatkan integritas dan efektivitas sistem pajak.

3.4.2 Aplikasi BDA dalam Segmentasi Wajib Pajak

Segmentasi wajib pajak merupakan aplikasi kritis dari Big Data Analytics (BDA) dalam audit pajak, yang secara teknis melibatkan pengolahan dan analisis data pajak yang luas dan kompleks untuk mengkategorikan wajib pajak ke dalam berbagai segmen. Proses ini didasarkan pada sejumlah variabel, termasuk perilaku kepatuhan, ukuran bisnis, jenis industri, dan karakteristik keuangan lainnya. Tujuannya adalah untuk memfasilitasi pendekatan audit yang lebih disesuaikan dan efektif, dengan mengarahkan sumber daya

audit ke segmen yang paling berisiko atau memerlukan perhatian lebih.

Proses dan aplikasi segmentasi wajib pajak melalui BDA:

1) Proses pengumpulan data dari berbagai sumber, termasuk laporan pajak, catatan keuangan, transaksi elektronik, dan data eksternal seperti informasi pasar atau data ekonomi makro. Data ini sering kali beragam dalam format dan struktur, memerlukan penggunaan teknologi ETL (Extract, Transform, Load) untuk mengekstrak data, mentransformasikannya ke dalam format yang konsisten, dan memuatnya ke dalam basis data terpusat untuk analisis lebih lanjut.
2) Setelah data terkumpul, teknik analitik canggih seperti machine learning dan algoritma klasifikasi digunakan untuk menganalisis dan mengelompokkan wajib pajak ke dalam segmen berdasarkan kriteria yang ditentukan. Algoritma ini dapat mengidentifikasi pola dan hubungan dalam data yang mungkin tidak terlihat melalui analisis manual, seperti korelasi antara jenis transaksi tertentu dan risiko penghindaran pajak.
3) Segmentasi memungkinkan otoritas pajak untuk mengidentifikasi grup wajib pajak yang memiliki karakteristik serupa dan menerapkan strategi audit yang disesuaikan untuk masing-masing segmen. Misalnya, wajib pajak dengan volume transaksi tinggi dan kompleksitas bisnis yang lebih besar mungkin memerlukan pendekatan audit yang lebih detail dan teknis, sedangkan wajib pajak kecil dengan transaksi yang lebih sederhana mungkin memerlukan audit yang lebih ringkas dan langsung.

Manfaat Segmentasi dengan menggunakan aplikasi BDA adalah

1) Memungkinkan auditor untuk mengalokasikan sumber daya lebih efisien, dengan memfokuskan upaya pada segmen yang paling mungkin menunjukkan risiko kepatuhan yang tinggi.
2) Strategi audit yang disesuaikan meningkatkan relevansi dan efektivitas audit, memungkinkan auditor untuk mengatasi masalah kepatuhan spesifik yang mungkin ada dalam segmen tertentu.
3) Dengan menyasar area berisiko tinggi dan menyediakan panduan yang lebih spesifik untuk segmen tertentu, otoritas pajak dapat meningkatkan kesadaran kepatuhan dan mendorong perilaku kepatuhan yang lebih baik di kalangan wajib pajak.

Proses segmentasi wajib pajak melalui penggunaan BDA mencerminkan evolusi dalam praktik audit pajak, memanfaatkan teknologi untuk meningkatkan akurasi, efisiensi, dan efektivitas dalam mengelola kepatuhan pajak.

3.4.3 Aplikasi BDA dalam Prediksi dan Pemodelan

Teknik prediksi dan pemodelan memanfaatkan data historis dan saat ini untuk menghasilkan estimasi atau prediksi mengenai kejadian di masa depan, khususnya terkait dengan hasil pajak dan area risiko. Pendekatan ini menggunakan algoritma statistik, machine learning, dan data mining untuk mengidentifikasi tren, pola, dan hubungan dalam data pajak yang besar dan kompleks, memungkinkan auditor dan otoritas pajak untuk membuat keputusan yang lebih informasi dan strategis.

1) Perencanaan Sumber Daya Audit.
   Dengan memperkirakan hasil pajak masa depan dan area risiko, otoritas pajak dapat mengalokasikan sumber daya audit secara lebih efektif, memprioritaskan audit pada area dengan risiko kepatuhan tertinggi atau potensi penghindaran pajak terbesar.
2) Identifikasi Potensi Area Risiko
   Prediksi dan pemodelan memungkinkan deteksi dini area yang mungkin menjadi fokus penghindaran pajak di masa depan, memungkinkan otoritas pajak untuk mengambil tindakan proaktif sebelum masalah kepatuhan muncul.

Prediksi dan pemodelan dalam BDA memberikan otoritas pajak alat yang kuat untuk memperkirakan hasil pajak masa depan dan mengidentifikasi area risiko potensial, memungkinkan pengambilan keputusan yang lebih cerdas dan alokasi sumber daya yang lebih strategis. Meskipun aplikasi ini sangat teknis dan memerlukan keahlian dalam statistik dan analisis data, penggunaannya dapat meningkatkan signifikan efektivitas audit pajak.

3.5 Potensi BDA dalam Audit Pajak

3.5.1 Potensi BDA dalam Efektivitas Audit Pajak

Big Data Analytics (BDA) dalam audit pajak menawarkan potensi signifikan untuk meningkatkan efektivitas dan efisiensi dalam pengawasan dan pelaksanaan kewajiban pajak.

BDA menyediakan infrastruktur teknologi yang memungkinkan pelacakan transaksi keuangan secara real-time dan komprehensif. Dengan mengintegrasikan data dari berbagai sumber, organisasi dapat memastikan bahwa setiap elemen pendapatan dan pengeluaran tercatat secara akurat, mengurangi potensi kesalahan dalam laporan keuangan yang dapat mempengaruhi perhitungan pajak.

Kemampuan BDA untuk menganalisis volume data yang besar dan kompleks memungkinkan organisasi untuk memahami dengan lebih baik pola pengeluaran dan pendapatan. Analisis ini tidak hanya menjamin klasifikasi yang tepat dari transaksi untuk tujuan pajak tetapi juga membantu dalam mengidentifikasi potensi area penghematan pajak.

Aplikasi algoritma dan teknik machine learning dalam BDA memperkuat kemampuan organisasi dalam mengidentifikasi transaksi yang tidak biasa atau mencurigakan yang mungkin menunjukkan kecurangan atau kesalahan pelaporan. Identifikasi ini secara signifikan meningkatkan integritas dan keandalan laporan keuangan.

Dengan data yang lebih lengkap dan akurat, BDA memfasilitasi perhitungan kewajiban pajak yang lebih

presisi, meminimalkan risiko kesalahan perhitungan dan potensi sanksi dari otoritas pajak.

Integrasi BDA dalam audit pajak memungkinkan pengambilan keputusan yang didasarkan pada analisis data yang mendalam, membantu organisasi dalam memenuhi kewajiban pajak sambil memaksimalkan efisiensi operasional.

3.5.2 Potensi BDA dalam Memperkuat Kepatuhan Pajak

Pemanfaatan teknologi BDA dalam audit pajak menandai pergeseran paradigma menuju pendekatan yang lebih data-driven, memungkinkan organisasi tidak hanya untuk memenuhi kewajiban pajak dengan lebih efisien tetapi juga untuk mendapatkan wawasan strategis dari data keuangan. Hal ini menekankan pentingnya investasi dalam kapabilitas analitik untuk memperkuat kepatuhan dan strategi pajak organisasi.

Dalam konteks peningkatan efektivitas audit pajak, Big Data Analytics (BDA) memegang peranan vital dalam mendukung kepatuhan proaktif terhadap regulasi pajak melalui analisis data keuangan secara real-time. Penggunaan BDA memungkinkan organisasi untuk tidak hanya mengidentifikasi tapi juga mengatasi potensi masalah kepatuhan sebelum berkembang menjadi isu yang lebih serius. Mekanisme teknis BDA menurut KPMG (2023) dalam meningkatkan kepatuhan pajak meliputi:

1) Analisis Data Real-Time
   BDA memanfaatkan teknologi canggih untuk mengolah dan menganalisis data transaksi keuangan secara real-time. Hal ini memungkinkan deteksi dini

indikator-indikator yang mungkin menunjukkan ketidaksesuaian dengan ketentuan pajak yang berlaku.

2) Deteksi dan Koreksi Proaktif
   Dengan kemampuan untuk memonitor aliran data keuangan secara terus-menerus, BDA membantu organisasi mengidentifikasi dan mengoreksi kesalahan atau ketidakakuratan dalam pelaporan pajak secara proaktif. Kemampuan ini berkontribusi pada pemeliharaan kepatuhan yang lebih baik terhadap peraturan pajak.
3) Peran Chief Data Officer (CDO) untuk Pajak
   Seperti yang disarankan oleh KPMG, CDO memainkan peran penting dalam memastikan integritas data, mengelola akses dan retensi data, serta memfasilitasi kolaborasi lintas departemen untuk memenuhi kebutuhan dan regulasi pajak. CDO bertanggung jawab atas pengelolaan strategis data yang menjadi kunci dalam analisis BDA, memastikan bahwa data yang dianalisis akurat dan relevan dengan kebutuhan audit pajak.
4) Optimisasi Proses Pajak
   Big Data Analytic (BDA) memberikan kemampuan untuk mengotomatisasi proses pengumpulan dan analisis data, meminimalkan kesalahan manusia, dan meningkatkan efisiensi proses audit pajak. Penggunaan alat analitik canggih memungkinkan organisasi untuk melakukan segmentasi data dan analisis prediktif, yang secara langsung mendukung pengambilan keputusan yang lebih tepat dan berbasis bukti dalam konteks pajak.
5) Kepatuhan dan Strategi Pajak yang Berbasis Data

Kemampuan BDA untuk menghasilkan wawasan yang mendalam dari data keuangan mendukung pengembangan strategi pajak yang lebih efektif dan berorientasi pada kepatuhan. Organisasi dapat menggunakan wawasan ini untuk menyusun rencana pajak yang mengoptimalkan kewajiban pajak sambil mematuhi peraturan yang berlaku.

3.6 Penggunaan BDA dalam Efektivitas Audit Pajak

3.6.1 BDA dalam Efisiensi Audit Pajak

Big Data Analytics (BDA) memainkan peran kunci dalam meningkatkan efisiensi audit pajak dengan memungkinkan auditor untuk meninjau volume data yang besar dengan cepat, mengurangi waktu dan usaha yang dihabiskan untuk ulasan manual (bdo.insight, 2023). Poin kunci bagaimana BDA mencapai efisiensi audit pajak (Europeanbusinessreview, 2023):

1) Dengan kemampuan menganalisis dataset besar dengan cepat, BDA memungkinkan auditor untuk mengurangi waktu yang dibutuhkan dalam melakukan audit. Hal ini berarti bahwa proses audit yang biasanya memakan waktu lama sekarang dapat diselesaikan dalam jangka waktu yang lebih singkat.
2) BDA menyediakan kapasitas untuk menganalisis seluruh populasi data, bukan hanya sampel. Hal ini memungkinkan auditor untuk mendapatkan gambaran yang lebih lengkap dan akurat mengenai keadaan keuangan entitas yang diaudit.
3) BDA dapat mengidentifikasi pola atau tren yang tidak biasa dalam data keuangan, yang mungkin

menunjukkan potensi risiko atau ketidaksesuaian. Dengan ini, auditor dapat fokus pada area-area yang lebih berisiko atau memerlukan perhatian lebih lanjut.

4) Dengan BDA, kualitas bukti audit yang diperoleh meningkat, karena data yang dianalisis lebih luas dan lebih mendalam. Hal ini mengarah pada peningkatan keandalan hasil audit.
5) BDA memungkinkan auditor untuk menyesuaikan pendekatan audit berdasarkan temuan yang diperoleh dari analisis data. Hal ini membuat proses audit lebih responsif terhadap kebutuhan khusus dari setiap entitas yang diaudit.

3.6.2 BDA dalam Efektivitas Audit Pajak

Big Data Analytics (BDA) meningkatkan efektivitas audit pajak dengan memungkinkan pemahaman holistik terhadap kesehatan keuangan organisasi (euronews, 2023). BDA memfasilitasi evaluasi yang lebih komprehensif dengan cara berikut:

1) BDA memungkinkan auditor untuk menganalisis keseluruhan data keuangan organisasi, bukan hanya sampel terpilih. Hal ini memberi gambaran lengkap tentang operasi keuangan, termasuk area yang mungkin sebelumnya tidak terdeteksi dalam audit tradisional.
2) BDA dapat mengidentifikasi pola dan tren dalam data keuangan yang besar dan kompleks. Hal ini membantu dalam mengungkap hubungan dan interaksi yang mungkin tidak langsung terlihat, memberikan pemahaman yang lebih dalam tentang kinerja keuangan organisasi.

3) Dengan analisis data yang lebih mendalam dan luas, BDA meningkatkan kualitas bukti audit. Hal ini mengarah pada kesimpulan audit yang lebih kuat dan andal.
4) BDA memungkinkan auditor untuk lebih efektif mengidentifikasi area risiko keuangan, seperti potensi penipuan atau kelemahan dalam kontrol internal. Hal ini memungkinkan tindakan korektif sebelum masalah berkembang lebih lanjut.
5) Melalui analisis data besar, auditor dapat menyesuaikan strategi audit berdasarkan kebutuhan spesifik organisasi, memastikan bahwa area yang memerlukan perhatian lebih diberikan prioritas yang sesuai.

Big Data Analytics (BDA) memperkuat efektivitas audit pajak dengan meningkatkan kemampuan deteksi risiko. Kemampuan ini dilakukan dengan mengidentifikasi pola atau tren yang tidak biasa dalam data keuangan, yang membantu auditor dalam mendeteksi area risiko potensial (bdo.insight, 2023). Berikut adalah beberapa aspek penting BDA membantu dalam deteksi risiko:

1) BDA memungkinkan auditor untuk mengidentifikasi pola yang tidak biasa atau anomali dalam data keuangan yang mungkin menunjukkan risiko atau ketidakpatuhan. Hal ini bisa berupa transaksi yang tidak sesuai, fluktuasi yang tidak dijelaskan dalam angka-angka keuangan, atau inkonsistensi dalam data yang terkait dengan praktik akuntansi.
2) BDA menyediakan kemampuan untuk menganalisis data secara lebih mendalam, membantu auditor menggali lebih jauh ke dalam data untuk

mengungkapkan masalah yang mungkin tidak terlihat dalam audit tradisional.

3) Dengan menganalisis tren dan pola dalam data, BDA membantu auditor mendapatkan kesadaran yang lebih baik tentang risiko yang dihadapi suatu organisasi. Hal ini membantu dalam menetapkan prioritas audit dan fokus pada area yang paling berisiko.
4) BDA tidak hanya membantu dalam mendeteksi risiko kepatuhan pajak, tetapi juga risiko operasional dan finansial lainnya yang mungkin mempengaruhi kesehatan keuangan organisasi.
5) Setelah risiko teridentifikasi, auditor dapat bekerja sama dengan organisasi untuk mengembangkan strategi mitigasi risiko dan tindakan pencegahan.

3.6.3 Integrasi BDA dalam Audit Pajak

Integrasi Big Data Analytics (BDA) dalam proses audit menyajikan perubahan paradigmatis dari metodologi audit konvensional menuju pendekatan yang lebih dinamis dan analitis. Berbeda dengan audit tradisional yang cenderung mengandalkan teknik sampling untuk evaluasi data keuangan, BDA memungkinkan analisis yang menyeluruh atas keseluruhan dataset. Hal ini secara signifikan meningkatkan kemampuan auditor dalam mengidentifikasi ketidakakuratan pelaporan keuangan, potensi penipuan, serta risiko operasional.

Dengan menggunakan teknologi BDA, auditor mampu mengolah dan menganalisis volume data yang besar dengan kecepatan dan akurasi yang tinggi. Pendekatan ini memungkinkan pengujian data keuangan secara komprehensif, melampaui batasan pengujian berbasis

sampel yang mungkin hanya mencakup sebagian kecil dari data yang tersedia. Oleh karena itu, auditor dapat menghasilkan wawasan yang lebih mendalam dan validitas audit yang lebih tinggi.

Namun, transformasi ini menyertakan tantangan yang harus diatasi, termasuk kebutuhan untuk pengambilan data yang efisien dan isu terkait privasi data. Pengelolaan data yang efektif membutuhkan infrastruktur teknologi yang kuat serta kebijakan privasi yang ketat untuk melindungi kerahasiaan informasi. Hal ini menuntut peningkatan kapasitas teknologi informasi serta kerangka kerja hukum dan etika yang solid untuk mengatur penggunaan BDA dalam audit. Perkembangan ini menandai sebuah kemajuan signifikan dalam bidang audit, memberikan potensi untuk audit yang lebih akurat, efisien, dan berbasis bukti. Namun, untuk merealisasikan sepenuhnya potensi ini, organisasi audit harus mengatasi hambatan teknis dan etis yang terkait dengan penggunaan BDA.

Teknologi ini memungkinkan pendekatan proaktif dan prediktif dalam menentukan subjek audit. Berbeda dengan metode audit tradisional yang umumnya mengandalkan sampling acak, BDA memberikan kemampuan untuk menganalisis dataset secara keseluruhan, memungkinkan otoritas pajak untuk secara efektif mengidentifikasi transaksi berisiko tinggi dan perilaku yang menyimpang dari norma.

Proses ini menurut KPMG (2023) dilakukan melalui tahapan teknis berikut:

1) Profil Risiko Berbasis Data
   Otoritas pajak dapat memanfaatkan algoritma BDA untuk mengolah dan menganalisis volume data

transaksi yang besar, memungkinkan identifikasi pola-pola atau transaksi yang menunjukkan risiko tinggi terhadap ketidakpatuhan pajak.

2) Prediksi dan Prioritas Audit
   Dengan menganalisis data secara komprehensif, BDA memungkinkan otoritas pajak untuk memprioritaskan audit berdasarkan risiko ketidakpatuhan yang. Hal ini memungkinkan alokasi sumber daya audit secara lebih efisien, meningkatkan kemungkinan deteksi dan koreksi ketidakpatuhan pajak.
3) Pengambilan Keputusan yang Didukung Data. Integrasi BDA dalam proses audit memungkinkan pengambilan keputusan yang lebih informasi dan tepat. Otoritas pajak dapat membuat keputusan berbasis data mengenai subjek audit yang potensial tanpa harus menunggu periode audit berikutnya.
4) Efisiensi Operasional
   Melalui pemanfaatan teknologi BDA, proses audit menjadi lebih dinamis dan responsif terhadap tren dan perilaku ketidakpatuhan pajak terkini. Hal ini secara signifikan meningkatkan efisiensi operasional audit pajak, mengurangi waktu dan biaya yang terkait dengan prosedur audit tradisional.

3.7 Urgensi Keamanan Siber dalam BDA

Dalam era digital saat ini, big data analytics (BDA) memainkan peran penting dalam berbagai aspek bisnis dan keamanan siber. Kemampuan untuk mengolah dan menganalisis volume data yang besar dengan kecepatan tinggi tidak hanya membuka peluang baru tetapi juga menghadirkan tantangan keamanan yang signifikan. Seperti yang dikutip dari Alvin Toffler, 'Seiring dengan

meningkatnya kekuatan teknologi kita, efek samping dan potensi bahaya juga meningkat'. Kekuatan dari big data ini, jika tidak dilindungi dengan benar, bisa menjadi sasaran empuk bagi penyerang yang ingin mengeksploitasi kerentanan untuk tujuan yang tidak sah (Rawat et al., 2019).

Keamanan siber dalam konteks BDA menjadi sangat penting karena adanya kebutuhan untuk melindungi data yang tidak hanya besar tetapi juga seringkali sensitif. Tantangan keamanan siber dalam big data meliputi, tetapi tidak terbatas pada, aspek kerahasiaan, integritas, dan ketersediaan data. Kejahatan siber yang menggunakan teknik canggih dapat mengekspos data pribadi, merusak integritas data, atau bahkan menyebabkan layanan menjadi tidak tersedia. Untuk mengatasi risiko ini, pendekatan keamanan siber harus berevolusi dari hanya berfokus pada pencegahan menjadi strategi yang lebih inklusif yang mencakup deteksi dan respons terhadap insiden keamanan. Big data dapat memainkan peran kunci dalam pendekatan baru ini dengan menyediakan kemampuan untuk menganalisis pola lalu lintas data secara real-time, mengidentifikasi perilaku mencurigakan, dan merespons secara otomatis terhadap ancaman yang terdeteksi. Dengan demikian, penggunaan algoritma dan model yang canggih untuk memproses dan menganalisis big data menjadi penting untuk memperkuat keamanan siber (Rawat et al., 2019).

Dengan pertumbuhan eksponensial data yang dihasilkan melalui Internet, penting untuk mengembangkan model dan algoritma baru yang tidak hanya dapat mengakomodasi volume data yang besar tapi juga menjamin keamanan dan privasi data. Keamanan siber dalam konteks

BDA, oleh karena itu, menjadi urgensi yang tidak bisa diabaikan dalam upaya melindungi infrastruktur digital dan data dari serangan siber yang semakin canggih (Rawat et al., 2019).

3.7.1 Memperkuat BDA dalam menghadapi Serangan Siber

3.7.1.1. Pendekatan Inovatif BDA dalam Mendeteksi Ancaman Siber

Big Data Analytics (BDA) sebagai alat yang kuat dalam memerangi serangan siber, menawarkan solusi canggih untuk mengatasi berbagai bentuk ancaman digital. Dengan kemampuan untuk menyiapkan, membersihkan, dan menanyakan data heterogen dengan efisiensi tinggi, BDA mampu mengatasi kompleksitas data yang tidak lengkap atau bermasalah, sesuatu yang sulit dilakukan oleh manusia (Raja & Rabbani, 2014). Pendekatan yang menggabungkan analisis data besar dengan metode semantik, seperti yang dibahas oleh Yao et al. (2016), memungkinkan pengumpulan wawasan mendalam tentang data heterogen, menjadikan BDA alat penting dalam keamanan siber.

Serangan siber hadir dalam berbagai bentuk, mulai dari peretasan, malware, serangan sosial, hingga Advanced Persistent Threats (APT) yang merupakan serangan canggih dan terencana (Cardenas, 2013). APT khususnya, sangat sulit dideteksi, tetapi penggunaan analisis data besar dapat membantu mendeteksi ancaman ini pada tahap awal. Teknik analisis pola yang canggih, yang bekerja pada berbagai sumber data heterogen, adalah kunci untuk mendeteksi ancaman tersebut.

Dalam mengurangi serangan botnet, Crespo & Gaarwood (2014) mengeksplorasi penggunaan analisis data besar. Sementara itu, Advanced Cyber Defense Center

(ACDC) berfokus pada pembagian informasi keamanan siber yang dikumpulkan mengenai serangan botnet untuk mempertahankan diri melalui botnet. Le et al. (2016) mengusulkan arsitektur untuk deteksi botnet menggunakan Peta Pengorganisasian Mandiri, menawarkan pendekatan pembelajaran tanpa pengawasan untuk mengklasifikasikan lalu lintas yang tidak diketahui.

Di sektor keuangan, analisis data besar digunakan untuk mencegah tindakan jahat atau serangan siber. Fatima et al. (2017) menyoroti penggunaan teknik fusi data dan visualisasi dalam Analisis Forensik Jaringan. Asuransi Keamanan Siber (CI) juga mendapatkan popularitas sebagai sarana mitigasi kerugian akibat insiden siber bagi perusahaan keuangan, dengan penelitian Kai et al. (2016) mengusulkan kerangka kerja yang menggunakan pendekatan data besar dalam CI.

Kerangka kerja keamanan siber berbasis Virtualisasi Fungsi Jaringan (NFV) yang dikembangkan oleh Gardikis et al. (2017), dikenal sebagai SHIELD, memanfaatkan BDA untuk mendeteksi dan memitigasi ancaman secara real-time. Saenko et al. (2017) membahas pembangunan sistem pemantauan keamanan untuk Internet of Things, yang menggunakan pemrosesan data paralel melalui platform Hadoop, memperkuat keandalan dan efisiensi dalam menghadapi serangan.

Penelitian lain menunjukkan peningkatan Manajemen Informasi Keamanan (SIM) melalui BDA, dengan desain cetak biru untuk SIM yang ditingkatkan (Gottwalt & Karduck, 2015). SIM menggunakan Sistem File Terdistribusi Hadoop untuk pengumpulan dan penyimpanan data, sambil menerapkan algoritme pembelajaran mesin untuk deteksi serangan. Alat yang dikembangkan oleh Puri & Dukatz

(2015) menyoroti pentingnya analisis grafik dalam deteksi anomali, menawarkan wawasan baru ke dalam ancaman keamanan melalui data besar.

Menghadapi serangan yang beragam dan kompleks, BDA telah menunjukkan kapasitasnya sebagai alat keamanan siber yang vital, memberikan strategi yang diperlukan untuk memitigasi serangan tersebut. Melalui penggunaan analisis data besar, pendekatan inovatif dalam deteksi, dan strategi mitigasi ancaman, BDA terbukti sebagai pilar penting dalam upaya keamanan siber modern.

3.7.1.2 Inovasi dan Tantangan dalam BDA untuk Keamanan Siber

Dalam konteks keamanan siber, inovasi melalui Big Data Analytics (BDA) menjadi katalis penting dalam memperkuat keamanan dan privasi data. Riset yang dilakukan oleh Miloslavskaya et al., (2016), Cui (2016), Miloslavskaya (2017), dan Mengke (2016) telah memberikan kontribusi signifikan terhadap pengembangan strategi dan kerangka kerja baru yang memanfaatkan kekuatan big data untuk meningkatkan keamanan siber.

A. Kerangka Kerja untuk Pemrosesan Data Besar yang Tidak Aman

Miloslavskaya et al., (2016) menawarkan sebuah taksonomi untuk pemrosesan data besar yang tidak aman dalam Security Operations Centers (SOC). Kerangka kerja ini dirancang untuk mengidentifikasi dan mengklasifikasikan berbagai jenis ancaman dan kerentanan yang mungkin dihadapi dalam pemrosesan data besar. Taksonomi ini memungkinkan SOC untuk lebih efektif dalam merencanakan dan menerapkan strategi keamanan yang

sesuai dengan spesifikasi ancaman yang diidentifikasi dalam lingkungan big data.

B. Model Big Data untuk Keamanan di Lingkungan Cloud

Penelitian oleh Cui (2016) berfokus pada pengembangan model big data yang melayani keamanan dalam lingkungan cloud. Model ini bertujuan untuk mengintegrasikan teknologi big data dengan infrastruktur cloud untuk menciptakan solusi keamanan yang lebih dinamis dan adaptif. Pendekatan ini memungkinkan penggunaan big data untuk analisis keamanan yang lebih mendalam, memanfaatkan kemampuan komputasi dan penyimpanan cloud untuk meningkatkan deteksi ancaman dan respons keamanan.

C. Pusat Intelijen Keamanan untuk Pemrosesan Big Data

Miloslavskaya (2017) mengembangkan konsep Security Intelligence Centers (SIC) yang difokuskan pada pemrosesan big data. SIC bertujuan untuk mengumpulkan, menganalisis, dan memproses volume data yang besar untuk mengidentifikasi pola-pola yang menunjukkan adanya ancaman keamanan. Dengan memanfaatkan teknologi big data, SIC dapat meningkatkan kemampuan organisasi dalam memahami dan merespons ancaman siber dengan lebih cepat dan akurat.

Analisis big data menyediakan wawasan penting yang bisa mengidentifikasi ancaman siber melalui pengenalan pola. Studi yang dilakukan oleh Gahi et al., (2016) dan Nelson & Olovsson (2016) menyoroti bagaimana teknologi seperti Hadoop, MapReduce, dan Hadoop Distributed File System (HDFS) memainkan peran krusial dalam mengelola dan menganalisis volume data yang besar. Namun, peningkatan keamanan siber di lingkungan big data menimbulkan

serangkaian tantangan yang signifikan, yang membutuhkan pendekatan inovatif untuk diatasi.

Mengke et al., (2016) mengeksplorasi tantangan dan solusi keamanan informasi yang muncul di era big data. Penelitian ini menyoroti bagaimana pertumbuhan eksponensial data menciptakan kerentanan baru dan menuntut pendekatan keamanan yang inovatif. Penulis mengusulkan solusi yang mencakup pengembangan algoritme keamanan yang lebih canggih, kebijakan privasi yang diperkuat, dan peningkatan kesadaran keamanan di antara pengguna.

Tantangan keamanan dalam big data mencakup masalah distribusi acak data dan keamanan dalam komputasi big data. Gahi et al., (2016) menekankan bahwa privasi dan keamanan merupakan dua tantangan utama dalam analisis big data. Sifat dari big data yang heterogen dan terdistribusi menambah kompleksitas dalam mengimplementasikan solusi keamanan yang efektif. Nelson & Olovsson (2016) dalam tinjauan literatur sistematis, mengidentifikasi kebutuhan untuk menangani aspek-aspek privasi dan keamanan sebagai bagian integral dari pengelolaan big data.

Solusi untuk tantangan keamanan ini termasuk penerapan teknologi canggih dan inovasi dalam kriptografi. Hadoop, MapReduce, dan HDFS, sebagai alat utama dalam pengelolaan big data, menawarkan kerangka kerja yang dapat diperluas untuk implementasi fitur keamanan. Misalnya, kerangka kerja Hadoop dapat dikonfigurasi dengan fitur keamanan seperti Kerberos untuk autentikasi yang aman. Selain itu, teknik kriptografi lanjutan seperti enkripsi homomorfik dan teknik pengawasan privasi dapat diterapkan untuk melindungi data saat proses analisis

berlangsung, memastikan bahwa data sensitif tetap terenkripsi bahkan selama pemrosesan.

Gahi et al., (2016) dan Nelson & Olovsson (2016) sama-sama menunjukkan bahwa ada kebutuhan untuk penelitian dan pengembangan lebih lanjut dalam teknologi keamanan yang dapat diintegrasikan dengan sistem big data. Hal ini mencakup pengembangan algoritma yang lebih efisien untuk enkripsi dan dekripsi data dalam volume besar, serta pengembangan kerangka kerja yang lebih aman untuk pemrosesan dan analisis data.

Mengatasi tantangan keamanan dalam big data membutuhkan pendekatan multi-faset yang menggabungkan teknologi inovatif, kriptografi lanjutan, dan praktik pengelolaan data yang baik. Penelitian oleh Gahi et al., (2016) dan Nelson & Olovsson (2016) menekankan pada kebutuhan untuk inovasi yang berkelanjutan dalam teknologi keamanan untuk menghadapi ancaman siber yang kompleks dan dinamis. Dengan mengadopsi solusi teknologi canggih, kita dapat memperkuat keamanan dan privasi dalam ekosistem big data, memastikan perlindungan data yang efektif di era digital.

3.7.2 Strategi Serangan Siber dalam BDA

3.7.2.1 Mengamankan Data Besar

Keamanan data besar mencakup tiga aspek utama kerahasiaan, integritas, dan ketersediaan Kaur et al. (2017). Kerahasiaan adalah tentang melindungi data dari akses tidak sah, menjadikannya prioritas utama dalam mengamankan data besar. Teknik seperti kontrol akses dan enkripsi memainkan peran penting dalam menjaga kerahasiaan data. Dengan meningkatnya volume dan keragaman data, menjaga kerahasiaan menjadi lebih menantang namun

sangat penting. Integritas menyangkut pencegahan modifikasi data yang tidak sah. Hal ini esensial untuk memastikan bahwa data yang disimpan dan diproses di cloud tetap akurat dan tidak terkorupsi, menghindari manipulasi yang dapat merusak keputusan bisnis dan operasional. Ketersediaan berkaitan dengan pemulihan data setelah gangguan perangkat keras, perangkat lunak, atau sistem, serta menghindari penolakan akses data. Hal ini memastikan bahwa data selalu dapat diakses saat diperlukan, yang krusial untuk kelancaran operasi bisnis.

Kaur et al. (2017) menyoroti pentingnya mengidentifikasi dan mengatasi kerentanan keamanan dalam cloud untuk melindungi data besar. Menginformasikan vendor tentang kerentanan terkini adalah langkah kritis dalam strategi ini, memungkinkan pengembangan solusi keamanan yang lebih efektif. Dalam konteks strategi serangan siber, pendekatan multi-lapis untuk keamanan data besar adalah penting. Memastikan hanya pengguna yang berwenang yang dapat mengakses data sensitif. Menggunakan teknologi enkripsi canggih untuk melindungi data baik saat disimpan maupun saat ditransmisikan. Menggunakan alat keamanan canggih untuk memantau aktivitas mencurigakan dan mencegah serangan sebelum terjadi. Dengan memahami dan menerapkan strategi serangan siber dalam konteks BDA, organisasi dapat lebih efektif dalam melindungi aset data yang berharga dari ancaman keamanan yang terus berkembang.

3.7.2.2 Teknik dalam Big Data Analytics (BDA) untuk Menghadapi Serangan Siber

Dalam konteks Big Data Analytics (BDA), strategi serangan siber melibatkan penggunaan teknik canggih untuk melawan ancaman yang terus berkembang terhadap integritas, kerahasiaan, dan ketersediaan data besar. Enkripsi dan kontrol akses merupakan dua pilar utama dalam strategi ini, masing-masing menyediakan lapisan perlindungan yang krusial melawan serangan siber.

A. Enkripsi sebagai Benteng Pertahanan Utama

Enkripsi memainkan peran kritikal dalam melindungi data dalam BDA, menyediakan metode yang kuat untuk memastikan bahwa hanya entitas yang berwenang yang dapat mengakses informasi sensitif. Dengan kemajuan dalam teknik enkripsi seperti FHE, FPE, dan ABE, bersama dengan penelitian yang berfokus pada peningkatan efisiensi dan skalabilitas, benteng pertahanan untuk kerahasiaan data menjadi semakin tangguh. Inovasi dalam enkripsi tidak hanya memperkuat keamanan tetapi juga memungkinkan analisis data yang aman dalam lingkungan yang semakin berbasis cloud. Dalam konteks Big Data Analytics (BDA), enkripsi berperan sebagai benteng pertahanan utama dalam melindungi kerahasiaan data. Hal ini penting terutama dalam skenario di mana data dipindahkan atau disimpan di cloud, memperbesar risiko akses tidak sah. Penelitian oleh Kepner et al., (2014) dan Xu et al., (2017) menunjukkan kemajuan signifikan dalam teknik enkripsi untuk meningkatkan keamanan data besar.

Enkripsi Homomorfik Sepenuhnya (FHE), memungkinkan operasi komputasi dilakukan pada data terenkripsi tanpa perlu mendekripsinya terlebih dahulu, menjaga kerahasiaan data tetap terlindung selama proses analitik. Hal ini penting dalam BDA, memungkinkan penggunaan data sensitif dalam penghitungan tanpa mengorbankan privasi. Kepner et al., (2014) mengeksplorasi metode untuk meningkatkan verifikasi data besar dengan menghitung pada data yang "dimasker," yang berpotensi memanfaatkan prinsip FHE untuk meningkatkan kepercayaan pada kebenaran data.

Format-Preserving Encryption (FPE), memungkinkan enkripsi data sedemikian rupa sehingga output enkripsi mempertahankan format asli dari data plaintext. Hal ini berguna dalam aplikasi yang memerlukan data untuk mempertahankan format tertentu bahkan setelah enkripsi, seperti nomor identifikasi yang harus memenuhi standar format tertentu. FPE menyediakan keseimbangan antara keamanan dan utilitas data, memungkinkan penggunaan data yang aman dalam aplikasi sensitif terhadap format data.

Enkripsi Berbasis Atribut (ABE), memungkinkan enkripsi data berdasarkan atribut, dengan kunci dekripsi yang hanya diberikan kepada pengguna yang atributnya cocok dengan kebijakan enkripsi. Hal ini sangat relevan untuk BDA, di mana akses ke data sensitif perlu dikontrol dengan ketat berdasarkan peran atau atribut pengguna. Xu et al., (2017) menyoroti implementasi MongoDB yang terenkripsi, menunjukkan bagaimana teknologi enkripsi dapat diintegrasikan dalam sistem manajemen database untuk mengamankan data besar.

Salah satu tantangan utama dalam penerapan teknik enkripsi untuk big data adalah masalah skalabilitas dan efisiensi. Enkripsi tradisional dapat sangat membebani dari segi komputasi, terutama ketika diterapkan pada volume data yang besar. Kepner et al., dan Xu et al., melalui riset, menunjukkan upaya berkelanjutan dalam mengembangkan solusi yang tidak hanya aman tetapi juga praktis untuk skala data besar. Peningkatan dalam algoritma enkripsi dan implementasi sistem yang efisien penting untuk memastikan bahwa keamanan data tidak menghambat kemampuan untuk melakukan analitik big data secara efektif.

B. Kontrol Akses

Kontrol akses merupakan salah satu pilar utama dalam memastikan keamanan dan privasi data dalam Big Data Analytics (BDA). Berbeda dengan enkripsi yang berfokus pada perlindungan kerahasiaan data, kontrol akses mengatur siapa yang dapat mengakses data berdasarkan kebijakan yang ditetapkan. Hal ini mencakup mekanisme untuk membatasi akses kepada pengguna yang terverifikasi dan berhak, sehingga mengurangi risiko kebocoran data dan penyalahgunaan. Pengembangan dan implementasi teknik kontrol akses yang efisien dan fleksibel adalah kunci untuk memastikan keamanan dan privasi dalam BDA. Dengan menerapkan kerangka kerja berbasis atribut dan teknologi perlindungan privasi, organisasi dapat memperkuat pertahanan terhadap serangan siber, memastikan bahwa data sensitif dilindungi dari akses tidak sah sambil tetap memenuhi kebutuhan akses yang sah. Penelitian oleh AlMamun et al., dan Islam et al., menawarkan wawasan berharga dalam arah yang harus diambil untuk mencapai tujuan ini dalam era big data.

Penelitian yang dilakukan oleh AlMamun et al., (2017) dan Islam et al., (2017) menunjukkan kemajuan signifikan dalam pengembangan model kontrol akses yang lebih canggih dan efisien. Model-model ini dirancang untuk tidak hanya menyaring akses tidak sah tetapi juga untuk mendukung kebijakan privasi yang kompleks dan dinamis. Hal ini sangat penting dalam lingkungan BDA, di mana volume data yang besar dan sifatnya yang sensitif memerlukan perlindungan yang kuat dan fleksibel.

Salah satu pendekatan inovatif dalam kontrol akses adalah penggunaan kerangka kerja berbasis atribut. Teknik ini memungkinkan kebijakan akses yang lebih granular, di mana akses diberikan berdasarkan atribut tertentu dari pengguna atau data itu sendiri. Hal ini memfasilitasi pengelolaan akses yang lebih dinamis dan adaptif, yang dapat menyesuaikan dengan perubahan kebijakan atau kondisi lingkungan. Selain itu, teknologi perlindungan privasi, seperti yang dijelaskan dalam karya Islam et al., (2017), memainkan peran penting dalam menjaga keamanan data pribadi, khususnya dalam konteks data medis besar. Kerangka kerja ini menawarkan solusi untuk melindungi rekam medis dan informasi sensitif lainnya dari akses tidak sah, seraya memastikan bahwa data dapat diakses oleh pihak-pihak yang berwenang untuk tujuan yang sah.

Implementasi model kontrol akses yang canggih ini memerlukan pertimbangan yang teliti terhadap kebutuhan pengguna dan persyaratan keamanan. Dalam praktiknya, ini dapat melibatkan pengembangan algoritma yang efisien untuk evaluasi kebijakan akses, serta mekanisme untuk audit dan pemantauan akses yang efektif. Selain itu, penting untuk memastikan bahwa sistem kontrol akses dapat berintegrasi

dengan baik dengan infrastruktur BDA yang ada, termasuk dukungan untuk teknologi cloud dan big data seperti Hadoop.

C. Menghadapi Serangan Siber dengan Teknologi Hybrid

Pendekatan hybrid dalam keamanan BDA, yang menggabungkan enkripsi dan kontrol akses, menawarkan solusi yang efektif dan efisien untuk melindungi data besar dari ancaman siber. Integrasi kriptografi simetris dan ABE, bersama dengan pengembangan teknik komputasi pada data yang disamarkan, menunjukkan inovasi yang signifikan dalam mengatasi tantangan keamanan yang kompleks dan dinamis. Kajian ini menggarisbawahi pentingnya adaptasi dan inovasi dalam strategi keamanan, memastikan bahwa data besar dapat dilindungi secara efektif dalam lingkungan yang terus berkembang.

Pendekatan hybrid dalam keamanan siber, yang menggabungkan teknik enkripsi dan kontrol akses, merupakan strategi yang kuat dan adaptif untuk melindungi data besar dalam konteks Big Data Analytics (BDA). Penelitian oleh Li et al., (2010) dan Soceanu et al., (2015), serta kerja oleh Kepner et al., (2014) dan Lee & Wu, (2017), menyajikan wawasan penting tentang bagaimana pendekatan ini dapat meningkatkan keamanan data besar.

Li et al., (2010) mengeksplorasi bagaimana kriptografi simetris dan ABE dapat digabungkan untuk mengamankan catatan kesehatan pribadi dalam cloud computing. Pendekatan ini memungkinkan kontrol akses yang pasien-sentris dan granular dalam pengaturan dengan banyak pemilik, meningkatkan baik efisiensi maupun fleksibilitas dalam pengamanan data. Dengan demikian, hanya

pengguna yang memenuhi atribut tertentu yang dapat mengakses data, memastikan bahwa data sensitif dilindungi secara efektif dari akses tidak sah.

Soceanu et al., (2015) membahas pengelolaan privasi dan keamanan data e-health, menyoroti pentingnya pendekatan yang mengintegrasikan privasi dan mekanisme kontrol akses untuk mengelola data sensitif secara efektif. Pendekatan ini membantu dalam memastikan bahwa data kesehatan pribadi dilindungi sesuai dengan kebijakan privasi yang ketat dan dapat diakses hanya oleh pihak-pihak yang berwenang.

Kepner et al., (2014) mengusulkan metode komputasi pada data yang disamarkan sebagai cara untuk meningkatkan kebenaran data besar. Teknik ini memungkinkan pemrosesan data sensitif tanpa mengungkapkan isi sebenarnya dari data tersebut, menawarkan lapisan keamanan tambahan sambil mempertahankan kemampuan analisis data.

Lee & Wu, (2017) mengeksplorasi teknologi perlindungan privasi dan mekanisme kontrol akses untuk data medis besar, menunjukkan bagaimana pendekatan hybrid dapat mengamankan data sensitif dalam industri layanan kesehatan. Pendekatan hybrid ini menekankan pada pentingnya melindungi privasi pasien sambil memastikan akses data yang aman dan terkontrol.

3.7.2.3 Pemanfaatan Big Data dalam Peningkatan Keamanan Siber

Bertino (2015) menggarisbawahi pentingnya menggabungkan dan menerapkan kebijakan kontrol akses yang ketat dalam pengelolaan big data untuk menjaga kerahasiaan dan privasi data. Kebijakan kontrol akses yang dirancang dengan baik memungkinkan organisasi untuk membatasi akses terhadap data sensitif hanya kepada pengguna yang berhak, sehingga mengurangi potensi risiko kebocoran data dan penyalahgunaan informasi. Pendekatan ini memerlukan penerapan mekanisme otentikasi dan otorisasi yang canggih, memastikan bahwa setiap akses terhadap data diawasi dan direkam untuk tujuan audit dan kepatuhan.

Mishra dan Singh (2016) mengeksplorasi tantangan keamanan yang muncul dari penyimpanan dan pengelolaan database besar serta file log transaksi dalam kerangka kerja terdistribusi. Kerangka kerja menekankan pentingnya memastikan keamanan pada setiap titik dalam siklus hidup data, dari pengumpulan, penyimpanan, hingga analisis data. Hal ini mencakup perlindungan terhadap serangan siber, seperti akses tidak sah, modifikasi data, dan denial of service (DoS), melalui penerapan teknologi keamanan terbaru seperti enkripsi data, pemantauan keamanan real-time, dan sistem deteksi intrusi.

Kedua studi tersebut menunjukkan bagaimana big data, dengan volume, kecepatan, dan variasi datanya, dapat digunakan sebagai alat untuk meningkatkan deteksi dan respons terhadap ancaman siber. Analisis big data memungkinkan identifikasi pola-pola yang menunjukkan adanya ancaman atau aktivitas mencurigakan, memfasilitasi

tindakan pencegahan atau respons yang lebih cepat terhadap insiden keamanan. Teknologi big data seperti Hadoop, sistem basis data NoSQL, dan alat analitik canggih dapat digunakan untuk memproses dan menganalisis data dalam skala besar, menyediakan wawasan yang diperlukan untuk menginformasikan strategi keamanan siber.

Bertino (2015) dan Mishra dan Singh (2016) secara efektif menggambarkan bagaimana big data dapat menjadi kunci dalam menghadapi tantangan keamanan siber di era digital. Pemanfaatan big data dalam keamanan siber menandai revolusi dalam bagaimana organisasi melindungi infrastruktur dan informasi digital. Dengan mengadopsi solusi berbasis big data yang inovatif, organisasi dapat lebih proaktif dan adaptif dalam menghadapi ancaman siber, memastikan integritas, kerahasiaan, dan ketersediaan data dalam lingkungan yang semakin terhubung dan digital.

BAB IV

Eksplorasi Literatur Business Inteligence (BI) dan Integrasinya dengan Audit Pajak

4.1 Pemanfaatan Business Intelligence (BI)

4.1.1 Memaksimalkan Efisiensi dengan Business Intelligence

Dalam era data yang semakin kompleks, Business Intelligence (BI) berperan kunci dalam membantu organisasi mengatasi tantangan manajemen risiko dan meningkatkan efisiensi operasional. Chang (2019) menyoroti bagaimana analisis data canggih dan BI dapat memperkuat proses manajemen dalam mengidentifikasi dan menangani risiko bisnis. Proses analitis yang mendalam pada kumpulan data besar (Big Data) melalui Data Analytics atau BI menawarkan peluang signifikan untuk meningkatkan pengelolaan risiko di berbagai sektor bisnis dan organisasi publik.

Namun, Grzegorek (2017) mengidentifikasi bahwa tantangan utama dalam analisis bisnis saat ini adalah sifat prosesnya yang memakan waktu. Kebutuhan manajemen perusahaan untuk melakukan analisis berkala—untuk memverifikasi hasil secara berkelanjutan terhadap dinamika lingkungan ekonomi dan kondisi pasar—seringkali

memerlukan investasi waktu yang signifikan dari sumber daya manusia departemen analitik dan manajemen. Hal ini menciptakan kebutuhan akan solusi yang dapat meningkatkan efisiensi dan mengurangi beban kerja.

Dalam konteks ini, penggunaan platform analitis terkomputerisasi yang mengadopsi prinsip-prinsip Industri Keuangan 4.0 menawarkan solusi yang sangat efektif. Teknik analitis yang diintegrasikan ke dalam formula BI, seperti yang dijelaskan oleh Gendron (2014), secara signifikan meningkatkan efisiensi proses analitis. Dengan mengotomatisasi dan mempercepat analisis, BI mengurangi jumlah jam kerja yang diperlukan untuk proses analitis, memungkinkan manajemen untuk lebih cepat menerapkan koreksi terhadap laporan dan rencana operasional.

Tujuan utama dari BI adalah untuk memberikan wawasan yang tepat waktu dan relevan yang mendukung pengambilan keputusan yang informasi. Melalui pengumpulan, pengolahan, dan analisis data, BI membantu organisasi.

A. Mengidentifikasi dan mengelola risiko bisnis secara proaktif

BI memungkinkan organisasi untuk mengidentifikasi risiko bisnis melalui analisis data historis dan real-time. Teknik seperti analisis prediktif dan pemodelan risiko digunakan untuk mengantisipasi potensi masalah sebelum berdampak pada operasi bisnis. Alat BI dapat mengintegrasikan data dari berbagai sumber, memberikan pandangan holistik yang memungkinkan deteksi pola atau tren yang mungkin menunjukkan risiko. Dengan menggunakan teknologi seperti machine learning, sistem BI dapat secara otomatis menyesuaikan model risiko

berdasarkan data baru, memungkinkan respons yang lebih cepat dan lebih informasi terhadap ancaman potensial (Han et al., 2011).

B. Memantau dan menyesuaikan dengan perubahan lingkungan ekonomi dan kondisi pasar

BI memfasilitasi pemantauan lingkungan ekonomi dan kondisi pasar secara berkelanjutan dengan mengagregasi dan menganalisis data dari berbagai sumber, termasuk berita pasar, laporan industri, dan indikator ekonomi. Dashboard dan visualisasi data yang dinamis memungkinkan pemangku kepentingan untuk memahami perubahan pasar secara intuitif dan membuat keputusan yang cepat. Alat analitik canggih, seperti analisis sentimen dan analisis tren, memungkinkan organisasi untuk memprediksi perubahan pasar dan menyesuaikan strategi secara proaktif (Chaudhuri et al., 2011).

C. Meningkatkan keputusan strategis dan operasional

Dengan menyediakan akses ke data yang komprehensif dan analisis mendalam, BI mendukung pengambilan keputusan strategis dan operasional. Penggunaan alat analitik, seperti analisis SWOT (Strengths, Weaknesses, Opportunities, Threats) dan analisis kompetitif, membantu organisasi dalam merumuskan strategi bisnis. Pada tingkat operasional, BI mendukung optimisasi proses, dari logistik hingga manajemen rantai pasok, dengan menyediakan insight yang diperlukan untuk meningkatkan efisiensi dan mengurangi biaya (Laudon & Laudon, 2016).

D. Mengoptimalkan alokasi sumber daya dan efisiensi operasional

Alat BI memungkinkan analisis sumber daya dan kinerja operasional secara real-time, memungkinkan organisasi untuk mengidentifikasi pemborosan, bottleneck, dan peluang penghematan biaya. Dengan mengintegrasikan data dari seluruh organisasi, BI menyediakan pandangan menyeluruh tentang kinerja operasional, memungkinkan manajemen untuk membuat keputusan yang didasarkan pada data untuk alokasi sumber daya yang optimal. Analisis data historis dan prediktif juga mendukung perencanaan sumber daya yang lebih akurat, memastikan bahwa organisasi memiliki sumber daya yang diperlukan untuk memenuhi permintaan masa depan tanpa kelebihan kapasitas (Davenport, 2013).

Penerapan BI, dengan demikian, tidak hanya merupakan strategi untuk mengatasi tantangan analitis tetapi juga merupakan investasi dalam keberlanjutan dan pertumbuhan organisasi. Dengan mengurangi kompleksitas dan waktu yang dibutuhkan untuk analisis, BI memungkinkan organisasi untuk lebih responsif dan adaptif dalam lingkungan bisnis yang dinamis.

4.1.2 Memperkuat Keunggulan Kompetitif melalui Business Intelligence

Dalam lanskap bisnis yang kompetitif saat ini, keunggulan kompetitif suatu perusahaan sering kali ditentukan oleh kemampuan untuk membuat keputusan yang cepat dan tepat. Prokopowicz (2017) menekankan bahwa keberhasilan dalam mencapai keunggulan ini sangat

bergantung pada pengumpulan, organisasi, dan analisis data yang efektif, yang dapat dicapai melalui penerapan laporan analitis Business Intelligence (BI) secara berkelanjutan. BI memungkinkan perusahaan untuk mengolah informasi yang diperlukan untuk pengambilan keputusan manajemen yang cerdas, dengan cara yang terorganisir dan sistematis.

Fan (2015) mendefinisikan proses analitis BI sebagai transformasi data multi-kriteria menjadi pengetahuan esensial untuk manajemen perusahaan yang efektif dan efisien. Proses ini melibatkan pengorganisasian dan pemrosesan data yang tersimpan dalam sistem TI perusahaan, serta penyajian hasilnya dalam bentuk laporan ekstensif. Dengan demikian, BI memungkinkan analisis multi-kriteria secara real-time, memberikan gambaran menyeluruh tentang situasi perusahaan.

Tomczak (2019) menambahkan bahwa analisis yang dilakukan melalui rumus BI membuka kemungkinan baru bagi manajemen untuk menganalisis kumpulan data besar secara real-time. Dengan demikian, solusi yang didasarkan pada teknologi informasi untuk proses analitis dan pengambilan keputusan menjadi semakin penting bagi para pengusaha. Penerapan BI tidak hanya mempercepat proses pengambilan keputusan tetapi juga meningkatkan kualitasnya, memastikan bahwa keputusan didasarkan pada data yang akurat dan relevan.

BI dimanfaatkan untuk mendukung pengambilan keputusan yang efektif melalui:

1) Mengumpulkan data yang relevan dari berbagai sumber untuk analisis.
2) Menyusun data yang terkumpul dalam format yang terstruktur untuk memudahkan analisis.
3) Menggunakan metode analitis untuk menginterpretasikan data dan mengidentifikasi tren, pola, dan wawasan.
4) Menyajikan hasil analisis dalam format laporan yang mudah dipahami, memungkinkan pengambilan keputusan yang informasi.

Dengan demikian, BI memainkan peran kunci dalam mengoptimalkan proses pengambilan keputusan, memungkinkan perusahaan untuk merespons dengan cepat terhadap perubahan pasar, mengidentifikasi peluang baru, dan mengelola risiko dengan lebih efektif. Melalui pemanfaatan BI, perusahaan dapat meningkatkan operasional, mencapai efisiensi yang lebih tinggi, dan memperkuat posisi kompetitif di pasar.

4.2 Integrasi Analitik Data dan Bisnis dalam Business Intelligence

Business Intelligence (BI) berperan krusial dalam mengubah data mentah menjadi informasi penting yang mendukung pengambilan keputusan strategis dalam bisnis. Inti dari BI terletak pada integrasinya yang mulus antara analitik data dan fungsi bisnis, memungkinkan organisasi untuk mengoptimalkan operasi, meningkatkan efisiensi, dan memperkuat keputusan strategis. Aspek ini menyoroti

bagaimana arsitektur, teknologi, dan proses BI secara kolektif memfasilitasi transisi dari pengumpulan data menjadi analisis yang dapat ditindaklanjuti dan wawasan bisnis yang berharga (Matthew Urwin, 2023).

Dalam era digital saat ini, teknologi seperti Big Data, Machine Learning (ML), dan Artificial Intelligence (AI) telah menjadi bagian integral dari BI. Penerapan teknologi ini memungkinkan organisasi untuk mengolah volume data yang besar dengan kecepatan dan ketepatan yang lebih tinggi, menghasilkan analisis prediktif dan preskriptif yang mendalam (Chen et al., 2012). Big Data menyediakan kemampuan untuk mengelola dataset yang sangat besar dan kompleks, yang tidak dapat diolah menggunakan metode pengolahan data tradisional. Integrasi Big Data dalam BI memungkinkan organisasi untuk mendapatkan wawasan yang lebih luas dari berbagai sumber data, termasuk data tidak terstruktur seperti teks, gambar, dan video. ML memungkinkan sistem BI untuk belajar dari data masa lalu dan membuat prediksi tentang masa depan. Dengan menggunakan algoritma ML, BI dapat mengidentifikasi pola dan tren tersembunyi dalam data, memfasilitasi pengambilan keputusan yang lebih informasi dan proaktif (Provost & Fawcet, 2013).

Metode Analisis Data dalam BI seperti Data Mining, merupakan Teknik data mining, seperti clustering, classification, dan association rules, digunakan untuk mengeksplorasi dan menganalisis data dalam BI. Metode ini membantu mengidentifikasi hubungan, pola, dan insight yang tidak jelas dari dataset besar (Han et al., 2011). Visualisasi data memainkan peran kunci dalam BI, memungkinkan pengguna untuk memahami wawasan

kompleks melalui grafik, diagram, dan peta interaktif. Dashboard yang disesuaikan membantu berbagai pengguna dari eksekutif hingga analis untuk memonitor KPI dan tren real-time Few, S. (2009).

4.2.1 Elemen Kunci dalam Integrasi Analitik Data dan Bisnis

Integrasi antara analitik data dan proses bisnis merupakan fondasi untuk mendapatkan wawasan yang mendalam dan mengambil keputusan berbasis data. Elemen kunci dalam BI, seperti agregasi multidimensi, denormalisasi, dan pelaporan real-time, memainkan peran vital dalam memanfaatkan potensi data tidak terstruktur atau semi-terstruktur.

A. Agregasi Multidimensi

Agregasi multidimensi memungkinkan organisasi untuk menganalisis data dari berbagai perspektif dan dimensi, seperti waktu, geografi, dan demografi. Teknik ini sangat berguna dalam model data warehousing, di mana data dikumpulkan dari berbagai sumber dan disusun dalam struktur yang memudahkan analisis dan pelaporan (Kimball & Ross, 2013).

B. Denormalisasi

Denormalisasi adalah proses yang digunakan dalam desain database untuk meningkatkan kinerja query dengan mengurangi kompleksitas join antartabel. Dalam konteks BI, denormalisasi memungkinkan akses data yang lebih cepat dan efisien, yang sangat penting untuk analisis real-time dan pengambilan keputusan (Inmon, 2005).

C. Pelaporan Real-Time

Pelaporan real-time mengubah cara organisasi mengakses dan menggunakan data. Dengan menyediakan wawasan instan ke dalam operasi bisnis, pelaporan real-time memungkinkan manajemen untuk membuat keputusan yang cepat dan tepat berdasarkan informasi terkini. Teknologi seperti aliran data (stream processing) dan database in-memory memainkan peran penting dalam memungkinkan pelaporan real-time (Plattner & Zeier, 2011).

D. Visualisasi Data

Kemampuan untuk mengubah data kompleks menjadi representasi visual yang intuitif merupakan aspek penting dari BI. Visualisasi data memudahkan pemahaman dan interpretasi analisis data, memungkinkan pengguna dari berbagai latar belakang untuk mengambil wawasan yang relevan. Alat visualisasi seperti dashboard dan infografis meningkatkan kemampuan organisasi untuk berkomunikasi dan bertindak berdasarkan data (Few, S., 2009).

Integrasi elemen-elemen kunci ini dalam BI memungkinkan organisasi untuk mengatasi tantangan yang berkaitan dengan pengolahan data besar yang kompleks dan memanfaatkan potensi penuh dari data. Dengan menggabungkan teknologi canggih dan metode analitis, BI memberdayakan organisasi untuk mengidentifikasi pola, tren, dan peluang yang sebelumnya tidak terlihat, mendorong keputusan yang lebih tepat dan strategi bisnis yang lebih efektif.

4.2.2 Mendorong Analisis Prediktif dan Pencarian Pola

Integrasi analitik data dan bisnis memanfaatkan statistik lanjutan dan analitik prediktif, memungkinkan ahli data untuk tidak hanya mengeksplorasi data tetapi juga memprediksi tren masa depan. Hal ini menciptakan landasan untuk keputusan bisnis yang proaktif dan berbasis bukti, dimana model dan algoritma analitik diterjemahkan menjadi strategi bisnis yang dapat ditindaklanjuti.

A. Analisis Prediktif

Analisis prediktif menggunakan data historis, algoritma pembelajaran mesin, dan teknik statistik untuk memprediksi hasil masa depan. Aplikasinya meliputi segala hal dari peramalan penjualan dan analisis perilaku pelanggan hingga deteksi penipuan dan manajemen risiko. Model prediktif secara proaktif mengidentifikasi peluang dan tantangan, memungkinkan organisasi untuk merencanakan strategi dengan lebih efektif (Siegel, E. 2016).

B. Pencarian Pola

Pencarian pola adalah proses mengidentifikasi pola berulang dalam data, yang dapat mengungkapkan insight yang berharga mengenai perilaku pelanggan, tren pasar, dan anomali operasional. Teknik seperti clustering dan association rule learning sangat berguna dalam mengungkap hubungan tersembunyi dalam data (Han et al., 2011).

C. Implementasi dalam Strategi Bisnis

Penerapan analisis prediktif dan pencarian pola dalam strategi bisnis memungkinkan organisasi untuk mengambil langkah-langkah yang dapat ditindaklanjuti berdasarkan prediksi yang akurat dan analisis mendalam dari pola data. Hal ini membuka jalan untuk optimisasi sumber daya, peningkatan pengalaman pelanggan, dan pengembangan produk atau layanan baru (Davenport & Harris, 2007).

D. Peran Teknologi Modern

Kemajuan dalam teknologi komputasi, seperti cloud computing dan big data platforms, telah meningkatkan kemampuan organisasi untuk menyimpan, memproses, dan menganalisis volume data yang besar dengan kecepatan dan efisiensi yang lebih tinggi. Teknologi ini, bersama dengan alat visualisasi data yang canggih, memastikan bahwa insight yang diperoleh dari analisis prediktif dan pencarian pola dapat dengan mudah dibagikan dan dipahami oleh pemangku kepentingan di seluruh organisasi. (Marr, 2015).

Dengan mengintegrasikan analisis prediktif dan pencarian pola ke dalam proses pengambilan keputusan, organisasi dapat meraih keunggulan kompetitif dengan menjadi lebih responsif terhadap perubahan pasar dan kebutuhan pelanggan. Hal ini menciptakan landasan untuk pertumbuhan yang berkelanjutan dan keberhasilan jangka panjang dalam lingkungan bisnis yang semakin didorong oleh data.

4.2.3 Evolusi ke BI Modern

Perkembangan Business Intelligence (BI) dari paradigma tradisional ke model modern telah merevolusi cara organisasi mengakses, menganalisis, dan memanfaatkan data. Transformasi ini menggeser fokus dari sistem BI yang kaku dan top-down, yang sangat bergantung pada departemen IT, ke solusi yang lebih fleksibel, interaktif, dan user-friendly, memungkinkan pengguna bisnis untuk melakukan eksplorasi data dan analitik secara mandiri.

A. Dari BI Tradisional ke Modern

BI tradisional sering kali dibatasi oleh kebutuhan akan pemrograman kompleks dan intervensi IT untuk menghasilkan laporan dan analisis, yang mengakibatkan keterlambatan dan penghalang dalam pengambilan keputusan bisnis. Sebaliknya, BI modern memanfaatkan teknologi canggih untuk memberikan kemampuan drag-and-drop, interaktivitas, dan analisis real-time yang dapat diakses langsung oleh pengguna akhir tanpa ketergantungan yang signifikan pada dukungan IT (Davenport & Harris, 2017).

B. Analitik Mandiri dan Kecepatan

Salah satu karakteristik utama BI modern adalah penekanan pada analitik mandiri, yang memberdayakan pengguna akhir untuk menggali insight dari data dengan sedikit hingga tanpa bantuan dari ahli data atau IT. Platform seperti Tableau, Qlik, dan Power BI telah memimpin dalam aspek ini, menawarkan antarmuka pengguna yang intuitif dan kemampuan visualisasi data yang kuat. Kemampuan untuk dengan cepat menyesuaikan dashboard dan menghasilkan laporan secara real-time sangat meningkatkan

kecepatan di mana organisasi dapat merespons dinamika pasar dan membuat keputusan yang informasi (Evelson, 2020).

C. Memperkuat Integrasi antara Analitik Data dan Keputusan Bisnis

BI modern tidak hanya memfasilitasi akses cepat ke data dan analisis tetapi juga memperkuat integrasi antara analitik data dan keputusan bisnis. Dengan menurunkan hambatan untuk analisis data, BI modern memungkinkan berbagai tingkat pengguna dalam organisasi, dari eksekutif hingga analis data, untuk berkolaborasi lebih efektif dan memanfaatkan data dalam strategi dan operasi sehari-hari. Hal ini mendorong budaya pengambilan keputusan berbasis data di seluruh organisasi (Bean & Davenport, 2019).

4.3 Integrasi Business Intelligence dalam Audit Pajak

Era digital telah merevolusi banyak aspek dalam dunia bisnis, termasuk audit pajak. Business Intelligence (BI), sebagai alat yang kuat, telah menunjukkan potensinya dalam mendukung fungsi audit pajak selama dua dekade terakhir. Dengan kemampuan untuk mendukung sistem akuntansi manajemen lanjutan, sistem kontrol, kepatuhan regulasi, dan manajemen risiko, BI telah menjadi kunci dalam mengoptimalkan proses audit pajak. Investasi yang signifikan dalam BI oleh berbagai organisasi bertujuan untuk memanfaatkan data warehouse besar, dengan tujuan akhir untuk mengakumulasi manfaat substansial dari analisis data yang komprehensif (Edger & Smith, 2021).

Dalam konteks pencegahan dan deteksi penipuan, aplikasi BI dalam audit pajak berperan penting dalam pengembangan model prediksi penipuan. Model ini membantu auditor dalam meningkatkan manajemen portofolio, memperbaiki keputusan perencanaan audit, dan secara proaktif mengidentifikasi entitas untuk penyelidikan penipuan potensial. Penggunaan BI dalam deteksi penipuan tidak hanya meningkatkan efektivitas audit tapi juga efisiensi, dengan memungkinkan auditor untuk memprioritaskan sumber daya pada area risiko yang lebih tinggi (Edger & Smith, 2021).

Perkembangan tren Big Data telah memberikan dampak signifikan terhadap berbagai sektor, termasuk audit pajak, dimana Business Intelligence and Analytics (BIA) telah digunakan untuk meningkatkan kontrol dan pemantauan. Pergeseran menuju otomasi maksimum dalam pengolahan data telah mengubah cara transaksi bisnis dipantau, menyediakan keuntungan strategis dalam mengurangi biaya deteksi anomali. Pendekatan ini, yang membandingkan dengan pengumpulan dan pemrosesan data terstruktur tradisional, menawarkan efisiensi yang signifikan dalam pemantauan kepatuhan pajak (Edger & Smith, 2021).

Dalam laporan Tax Administration OECD Tahun 2022, dinyatakan bahwa banyak administrasi pajak telah mengadopsi teknik data science dan alat analitik untuk mendukung proses kepatuhan. Sebagai ilustrasi, Administrasi Pajak Australia (ATO) telah mengembangkan alat yang mampu memproses data transaksi keuangan dengan kecepatan dan akurasi yang sangat meningkat dibandingkan analisis manusia. Di Austria, penilaian risiko

waktu nyata untuk deklarasi pajak individu telah diimplementasikan, memanfaatkan teknik pembelajaran mesin untuk pemilihan kasus. Sementara itu, Administrasi Pajak Kanada telah mengintegrasikan alat forensik digital untuk investigasi yang kompleks, yang secara substansial menghemat waktu dan biaya (Edger & Smith, 2021).

Penerapan Business Intelligence (BI) dalam audit pajak merepresentasikan sebuah revolusi dalam cara administrasi pajak mengelola data, risiko kepatuhan, dan intervensi kepatuhan. Teknologi BI, dengan memanfaatkan big data dan pembelajaran mesin, memungkinkan administrasi pajak untuk mendeteksi penipuan dan menilai risiko dengan presisi yang belum pernah terjadi sebelumnya. Hal ini dijelaskan dalam laporan OECD "Tax Administration 2022", yang menyoroti bagaimana teknik-teknik canggih ini mengasah manajemen risiko dan memfasilitasi pengembangan tindakan intervensi yang lebih tepat, termasuk otomatisasi proses yang kompleks (OECD, 2022).

Dalam era digital yang terus berkembang, pemahaman akan pentingnya adopsi teknologi dalam audit pajak menjadi semakin mendalam. Kecerdasan teknologi, kesadaran lingkungan, pendekatan berbasis data, dan kemampuan prediktif menjadi fondasi bagi organisasi untuk mengajukan pengembalian pajak yang akurat, melacak perubahan regulasi, dan bahkan memprediksi kewajiban pajak dengan lebih efektif. Penggunaan otomatisasi proses robotik tidak hanya meningkatkan akurasi dalam pengajuan dan pelaporan pajak tetapi juga mendukung pengambilan keputusan yang informasi dan pengembangan strategi kepatuhan pajak yang proaktif (OECD, 2022).

4.3.1 Business Intelligence Memaksimalkan Efisiensi Audit Pajak

Dalam konteks yang semakin kompleks dan data-driven, integrasi Business Intelligence (BI) dalam audit pajak menawarkan sebuah pendekatan revolusioner untuk meningkatkan efisiensi, akurasi, dan keandalan proses audit. BI, sebagai kumpulan solusi perangkat lunak yang memungkinkan organisasi untuk mengumpulkan, mengintegrasikan, dan mengevaluasi data besar, berperan penting dalam mengidentifikasi kemampuan dan kerentanan sebuah organisasi (Harrison et al., 2015). Dalam audit pajak, penerapan BI dapat secara signifikan mengubah cara auditor memperoleh, menganalisis, dan menilai bukti audit untuk memastikan kepatuhan terhadap Prinsip Akuntansi yang Berlaku Umum (GAAP).

A. Memperkuat Proses Audit dengan BI

Integrasi BI dalam audit pajak mengubah paradigma tradisional audit dengan memanfaatkan analitik data untuk mendukung prosedur audit yang lebih sistematis, objektif, dan tercatat (Popa & Toma, 2009). Dengan algoritma canggih dan model prediktif, BI memungkinkan auditor untuk secara otomatis mengidentifikasi pola atau ketidaksesuaian dalam data pajak. Hal ini tidak hanya mempercepat proses audit tetapi juga meningkatkan objektivitas dan keakuratan hasil audit, menjadikannya lebih efektif dalam mengidentifikasi risiko dan pelanggaran.

B. Mendukung Keputusan Audit dengan Data

Laporan auditor, sebagai konfirmasi atas laporan keuangan perusahaan, memainkan peran kunci dalam membantu pemangku kepentingan membuat keputusan

yang berdasarkan informasi (Chen et al., 2014). Dengan BI, laporan audit dapat diperkaya dengan insight yang lebih mendalam dan berbasis data, memberikan kepercayaan tambahan kepada kreditor, investor, dan pihak berkepentingan lainnya. Integrasi BI dalam audit pajak tidak hanya memungkinkan auditor untuk menyajikan temuan yang lebih akurat dan terpercaya tetapi juga memberikan dasar yang lebih kuat untuk rekomendasi dan keputusan audit.

C. Meningkatkan Efisiensi dan Kepercayaan

Audit yang dilakukan secara rutin dengan dukungan BI tidak hanya mempercepat proses verifikasi keuangan tetapi juga meningkatkan kepercayaan dalam laporan keuangan (Rezaee et al., 2001). Kemampuan BI untuk menyediakan analisis real-time dan online mengubah cara auditor menilai kepatuhan terhadap GAAP, memungkinkan penyesuaian yang lebih cepat terhadap perubahan kondisi pasar atau regulasi. Selain itu, kemajuan dalam teknologi audit seperti RPA dan pembelajaran mesin menawarkan potensi untuk meningkatkan audit berdasarkan Standar Data Audit, meskipun masih memerlukan keterampilan dan penilaian profesional auditor manusia (Cohen dkk., 2019; Huang & Vasarhelyi, 2019).

Dengan evolusi teknologi informasi dan analitik, termasuk BI, menjadi semakin penting dalam audit pajak, pengetahuan tentang keterampilan baru menjadi esensial bagi tim audit (Brender & Gauthier, 2018). Integrasi BI dalam audit pajak bukan hanya tentang pemanfaatan teknologi terkini tetapi juga tentang mendorong pendekatan audit yang lebih efisien, akurat, dan dapat diandalkan,

membentuk landasan kuat untuk keputusan bisnis dan investasi yang berbasis data.

4.3.2 Business Intelligence Memaksimalkan Akurasi Audit Pajak

Dalam era digital yang terus berkembang, sistem akuntansi dan manajemen data menjadi semakin kompleks. Hal ini mendorong pergeseran dari teknik audit tradisional ke penggunaan Perangkat Lunak Audit atau Computer Assisted Audit Tools (CAAT), yang secara signifikan meningkatkan efektivitas pekerjaan audit. Menurut Stanciu et al. (2009), implementasi CAAT telah menggantikan metode verifikasi laporan keuangan dan dokumentasi tradisional, memberikan banyak manfaat bagi auditor. Zuca & Tinta (2018) menekankan bahwa penggunaan alat Business Intelligence (BI) untuk audit berkelanjutan memberikan pengaruh yang signifikan terhadap organisasi dengan menawarkan peluang untuk menggantikan audit berkala/tahunan dengan prosedur audit berkelanjutan yang lebih efisien.

Davis dan Woratschek (2015) menunjukkan bagaimana alat BI dapat memfasilitasi audit berkelanjutan, didukung oleh serangkaian KPI (Key Performance Indicators) yang mencakup rasio keuangan tradisional dan metrik kinerja keuangan seperti estimasi aliran kas dan rasio perputaran utang usaha. Ali (2020) menambahkan bahwa struktur alat BI dapat membantu dalam audit berkelanjutan, memungkinkan auditor untuk lebih efektif dalam pekerjaan.

Penggunaan alat BI tidak hanya mempercepat proses audit tetapi juga meningkatkan kualitas dan akurasi laporan. Berberich (2005) menyatakan bahwa alat BI secara dramatis mengurangi waktu yang dibutuhkan untuk memperoleh bukti audit, memungkinkan akses cepat dan tepat waktu ke data yang diaudit. Zuca & Tinta (2018) menyoroti bagaimana metode ini mempercepat identifikasi anomali dan pengecualian, memudahkan penyederhanaan pekerjaan audit dan produksi laporan secara otomatis. Zraqat (2020) menekankan bahwa perangkat lunak BI, sebagai alat inti ekonomi modern, dapat secara spesifik mencatat detail aktivitas keuangan dan ekonomi korporasi, meningkatkan kecepatan produksi dan verifikasi pencatatan.

Kualitas laporan yang dihasilkan oleh alat BI sangat penting dan bergantung pada validitas sumber data. Ali (2019) menggarisbawahi bahwa alat BI dapat diatur sedemikian rupa untuk memastikan kualitas dan integritas data yang dimasukkan ke dalam sistem organisasi, serta memberikan peringatan jika data baru tidak memenuhi standar kualitas yang diharapkan. Chaudhuri et al. (2011) menambahkan bahwa alat BI dapat menerima berbagai jenis data (real-time, tidak terstruktur, dan terstruktur) dan mengubahnya menjadi informasi yang berguna.

Dalam konteks audit pajak, integrasi BI menawarkan potensi besar untuk mengoptimalkan dan menstandardisasi laporan keuangan. Duan dan Xu (2012) serta Zraqat (2020) menunjukkan bahwa metode BI berkontribusi signifikan terhadap efisiensi laporan keuangan, mendukung fungsi pengambilan keputusan bagi sekelompok besar pengguna. Dengan demikian, alat BI harus difokuskan untuk memanfaatkan sepenuhnya dalam audit pajak, menjanjikan

transformasi menuju efisiensi, akurasi, dan keputusan yang lebih informatif.

4.3.3 Business Intelligence Memaksimalkan Aksesibilitas Audit Pajak

Audit pajak yang terus berkembang, integrasi teknologi Business Intelligence (BI) telah membuka jalan baru untuk efisiensi, aksesibilitas, dan akurasi. Alat BI, seperti yang diungkapkan oleh Webb (2012), memungkinkan auditor untuk berinteraksi dengan berbagai unit bisnis dalam suatu organisasi secara mendalam. Ini memberikan keuntungan signifikan dalam menetapkan analisis risiko, memvalidasi metrik keberhasilan, mempelajari strategi manajemen risiko, dan menunjukkan integrasi peran bisnis dalam kerangka tata kelola perusahaan. Kemampuan untuk mengakses informasi audit melalui perangkat seluler apa pun, tanpa memandang waktu dan lokasi, seperti yang dijelaskan oleh Kamordzhanova & Selezneva (2019), menambahkan lapisan fleksibilitas yang belum pernah terjadi sebelumnya dalam audit pajak.

Penggunaan dasbor seluler dan digital, bersama dengan fitur seperti KPI utama, kartu skor keseimbangan, analisis komparatif, dan keamanan berlapis, memungkinkan auditor untuk menghasilkan dan mempresentasikan temuan secara efisien (Chaudhuri et al., 2011). Komponen visualisasi dari suite BI menyediakan cara intuitif dan canggih untuk melacak dan membandingkan pola operasi dan peran organisasi (Trigo et al., 2014). Ini memperkuat kemampuan

auditor dalam mengidentifikasi area risiko dan peluang peningkatan dalam tata kelola pajak.

Lebih lanjut, penelitian oleh Wong dan Venkatraman (2015) menyoroti bagaimana metode akuntansi forensik modern, yang diperkuat oleh BI, dapat melakukan analisis pola keuangan dari data keuangan yang dipalsukan dengan efektif. Adopsi pendekatan BI dalam audit pajak tidak hanya meningkatkan akurasi dalam mendeteksi penipuan akuntansi tetapi juga mengurangi waktu dan sumber daya yang dibutuhkan untuk melakukan audit. Teknologi ini, seperti yang disebutkan oleh Ali (2020), memanfaatkan Hukum Benford dan teori serupa untuk mengidentifikasi aktivitas mencurigakan melalui pemantauan pola digit dalam catatan keuangan. Ini memungkinkan auditor untuk secara proaktif menandai dan memeriksa ulang transaksi yang meragukan untuk mendeteksi penipuan.

Integrasi BI dalam audit pajak tidak hanya mengoptimalkan proses audit melalui aksesibilitas dan analisis data yang lebih baik tetapi juga memberikan alat yang kuat untuk deteksi penipuan. Dengan menyediakan wawasan yang lebih dalam dan akurat tentang operasi pajak dan tata kelola perusahaan, BI membantu auditor dan akuntan forensik dalam menghadapi tantangan audit di era digital. Kemampuan untuk mengakses, menganalisis, dan mengevaluasi data pajak secara real-time dan dari jarak jauh menawarkan keuntungan signifikan dalam mengidentifikasi dan mengatasi masalah sebelum mereka berkembang menjadi risiko yang lebih besar. Ini menandai era baru dalam audit pajak, di mana teknologi BI berperan sebagai katalis untuk transparansi, kepatuhan, dan integritas dalam praktik pajak.

4.4 Strategi Pengembangan BI dalam Audit Pajak yang Efektif

Mengembangkan strategi BI yang sukses memerlukan pemahaman yang mendalam tentang tujuan bisnis, identifikasi pemangku kepentingan utama, dan definisi tanggung jawab. Hal ini menekankan pentingnya integrasi analitik data dan bisnis dalam perencanaan dan implementasi strategi BI.

4.4.1 Optimasi Audit Pajak Melalui Penerapan BI

Dalam era digital, Business Intelligence (BI) telah menjadi alat penting dalam mendukung pengambilan keputusan, pemantauan, dan pelaporan dalam audit pajak, memberikan kemampuan untuk mengubah data pajak menjadi wawasan bisnis yang berharga. Penggunaan teknologi digital, termasuk AI dan machine learning, memungkinkan perusahaan dan otoritas pajak untuk menganalisis dan meramalkan tren pajak dengan presisi yang belum pernah terjadi sebelumnya, mendukung keputusan strategis dan operasional yang efektif (Murillo, 2024).

BI memungkinkan analisis komprehensif data perusahaan untuk mendukung fungsi pajak, menyederhanakan proses, mengurangi risiko, dan menyediakan insight berharga terkait dengan pendapatan, arus kas, dan biaya. Implementasi kerangka kerja strategis yang mencakup tujuan transformasi, data pendukung, serta proses bisnis dan pajak yang terpengaruh, menjamin

integrasi efektif antara alat data perusahaan dan alat data pajak (Murillo, 2024).

Otoritas pajak juga meningkatkan pemanfaatan analitik data untuk efisiensi pengumpulan pajak dan kepatuhan, mengumpulkan informasi dari berbagai sumber untuk membangun profil pajak perusahaan yang akurat. Penggunaan analitik data real-time atau hampir real-time memungkinkan validasi faktur, verifikasi deklarasi, dan perbandingan data lintas yurisdiksi dengan efektif.

Penerapan BI dalam audit pajak tidak hanya meningkatkan transparansi dan efisiensi bagi perusahaan dalam menghadapi perubahan kebijakan pajak dan kepatuhan tetapi juga memfasilitasi otoritas pajak dalam mengumpulkan dan menganalisis data untuk peningkatan administrasi pajak dan identifikasi area audit potensial.

Business Intelligence (BI) telah menjadi tulang punggung dalam mendukung pengambilan keputusan yang cerdas, pemantauan yang efektif, dan pelaporan yang akurat dalam lingkup audit pajak. Melalui pemanfaatan alat dan teknik canggih, BI menyediakan kemampuan analitik yang mendalam untuk mengolah dan menganalisis data, yang sangat meningkatkan kualitas dan efisiensi proses audit. Berikut ini adalah beberapa aspek kunci di mana BI memberikan kontribusi signifikan:

A. Pengambilan Keputusan Berbasis Data

BI memperkaya auditor dengan alat yang memungkinkan analisis data keuangan dan operasional yang komprehensif. Dengan mengidentifikasi tren dan pola dalam data, auditor dapat membuat keputusan yang berinformasi dan tepat, menilai risiko dengan lebih akurat, dan menargetkan area untuk pemeriksaan lebih lanjut secara efektif.

B. Pemantauan Real-time

Alat BI memfasilitasi pemantauan data keuangan yang berkelanjutan, memperkenalkan kemampuan untuk mengamati perubahan dan perkembangan data secara real-time. Visualisasi data dan dashboard yang intuitif memungkinkan auditor untuk menjaga pengawasan yang ketat terhadap variabel penting seperti fluktuasi transaksi, pendapatan, dan biaya.

C. Pelaporan yang Dinamis dan Akurat

Melalui otomatisasi yang disediakan oleh BI, proses pembuatan laporan menjadi lebih cepat dan lebih akurat. Alat-alat ini memungkinkan generasi laporan yang menyajikan analisis tren, komparasi, dan insight penting lainnya yang mendukung kebutuhan audit pajak, sembari mengurangi kemungkinan kesalahan manusia.

D. Analisis Prediktif untuk Antisipasi Risiko

BI sering kali dilengkapi dengan kemampuan analisis prediktif, memanfaatkan data historis untuk memproyeksikan tren masa depan. Dalam audit pajak, hal ini memungkinkan prediksi area berisiko tinggi untuk non-kepatuhan atau penipuan, membantu auditor dalam mengalokasikan sumber daya secara lebih strategis.

E. Pengelolaan Data Besar

Dalam era data yang terus berkembang, kemampuan untuk mengelola dan menganalisis dataset yang luas menjadi kritikal. BI menyediakan solusi untuk mengatasi volume data yang besar, membuka wawasan yang sebelumnya tersembunyi dan mendukung keputusan yang lebih informasi.

Pemanfaatan Business Intelligence dalam audit pajak tidak hanya memperkuat akurasi dan efisiensi audit tetapi juga memberikan landasan bagi pengambilan keputusan yang proaktif dan strategis. Dengan teknologi BI, auditor dapat menavigasi kompleksitas audit pajak dengan lebih mudah, memastikan kepatuhan yang lebih baik, dan mengurangi risiko secara signifikan.

4.4.2 Mengatasi Tantangan Implementasi

Tantangan dalam implementasi BI, seperti manajemen data yang tidak terstruktur dan kebutuhan akan talenta analitik, menyoroti pentingnya pendekatan yang terintegrasi. Mengatasi tantangan ini memerlukan solusi yang tidak hanya teknis tetapi juga mempertimbangkan aspek bisnis dari analitik data.

Penggunaan Business Intelligence (BI) dalam audit pajak menawarkan berbagai keuntungan, termasuk peningkatan efisiensi dan akurasi dalam pengumpulan data dan analisis. Namun, penerapan dan integrasi teknologi BI ini tidak tanpa tantangan. Studi oleh Kascelan (2011) mengungkapkan bahwa implementasi alat BI dapat memakan waktu yang lama, dari enam bulan hingga beberapa tahun, yang mungkin berdampak negatif terutama pada bisnis dengan aset keuangan yang terbatas. Lebih lanjut, Gartner menemukan bahwa dari 2.000 proyek gudang data yang dianalisis, hanya 20% yang berhasil, menyoroti tingginya tingkat kegagalan dalam penerapan proyek BI.

Komitmen finansial yang signifikan diperlukan untuk menerapkan sistem BI, dan kesalahan dalam pemilihan alat BI dapat mengakibatkan konsekuensi finansial dan strategis yang serius (Ali, 2019). Selain itu, banyak alat BI tidak dirancang untuk menangani atau menyesuaikan kembali data yang sering digunakan di kantor keuangan, seperti berbagai skema laba dan rugi dan persyaratan pelaporan yang berbeda. Hal ini menimbulkan kesulitan dalam mempertahankan fleksibilitas untuk penelusuran berdasarkan produk, geografi, saluran, atau dimensi terkait

lainnya. Selain itu, sistem BI sering kali tidak memiliki kemampuan untuk melacak langsung ke data tingkat transaksional, yang penting untuk menjelaskan asal-usul data (Board International).

Kekurangan lain dari penerapan BI dalam audit adalah seringkali auditor tidak terlibat dalam pembangunan gudang data, yang penting untuk melihat transaksi yang dilaporkan dalam sistem sumber (Murali, 2010). Ini menciptakan kesenjangan antara kebutuhan auditor dan kemampuan sistem BI yang sudah terimplementasi. Webb (2012) menekankan bahwa tantangan dalam penerapan dan pemeliharaan alat BI juga termasuk pembatasan layanan untuk analisis data, yang sangat diminati.

4.5 Cybersecurity dalam Business Intelligence

4.5.1 Keamanan Siber dalam Business Intelligence, Menuju Keamanan Data yang Berkelanjutan

Di tengah revolusi teknologi keempat dan kemajuan Industri 4.0, keamanan data menjadi semakin penting, terutama dalam konteks Business Intelligence (BI) dan cloud computing. Teknologi seperti Big Data, komputasi awan, pembelajaran mesin, Internet of Things, kecerdasan buatan, dan BI sendiri, telah mendorong evolusi dalam cara data dikumpulkan, diproses, dan dianalisis (Gwoździewicz, 2010). Namun, kemajuan ini juga membawa tantangan baru dalam hal keamanan dan privasi data.

Mengadopsi kerangka kerja keamanan yang proaktif dan preventif, seperti yang diusulkan oleh Cavoukian (2021) dalam "Privacy by Design", menjadi krusial. Paradigma ini

menekankan bahwa privasi harus diintegrasikan ke dalam desain dan operasi organisasi sebagai mode operasi default, melampaui sekedar kepatuhan terhadap undang-undang dan peraturan. Hal ini mengakui bahwa di era Big Data, keamanan dan privasi data harus ditanamkan dari awal dan diperkuat melalui berbagai lapisan pertahanan.

Gołębiowska et al., (2021) menguraikan prinsip-prinsip keamanan yang dapat diadaptasi untuk Big Data, yang juga relevan untuk lingkungan BI dan cloud computing:

1) Mengantisipasi dan mencegah serangan sebelum terjadi.
2) Mengimplementasikan hak akses minimal untuk membatasi akses hanya kepada yang membutuhkan.
3) Memasukkan keamanan sebagai bagian integral dari desain sistem dan proses operasional.
4) Menggunakan lapisan keamanan berganda untuk melindungi data.
5) Menjamin keamanan data dari titik asal hingga destinasi akhir.
6) Membuat sistem keamanan dapat diverifikasi dan dipercaya.
7) Menempatkan privasi dan keamanan pengguna sebagai prioritas.
8) Mengawasi sistem secara terus-menerus untuk deteksi ancaman sejak dini.
9) Memastikan tindakan dan akses ke data dapat dilacak dan dipertanggungjawabkan.

Dalam lingkungan BI dan cloud computing, menerapkan prinsip-prinsip ini memungkinkan organisasi untuk tidak hanya melindungi aset data tetapi juga

membangun kepercayaan dengan pengguna dan pemangku kepentingan. Keamanan data yang efektif dan berkelanjutan adalah kunci untuk memanfaatkan sepenuhnya potensi BI dalam mendorong keputusan bisnis yang informasi dan strategis.

Dalam lingkungan Business Intelligence (BI) yang data-driven, keamanan siber tidak hanya menjadi prioritas tetapi juga sebuah keharusan. Tang (2015) menekankan bahwa sistem manajemen keamanan big data harus menyertakan serangkaian tindakan dan subsistem perlindungan yang komprehensif, meliputi pencegahan, penghindaran, mitigasi, deteksi, respons, pemulihan, dan koreksi. Hal ini mencerminkan pendekatan holistik terhadap keamanan yang diperlukan untuk melindungi data besar dari ancaman siber yang semakin canggih.

Menurut Association for Data-driven Marketing & Advertising (ADMA, 2013), ada beberapa praktik terbaik dalam keamanan data besar yang harus diadopsi oleh organisasi untuk memastikan integritas dan keamanan data:

1) Memastikan bahwa data dilindungi dari titik asal hingga titik akhir, menjamin keamanan data selama transmisi dan saat disimpan.
2) Menggunakan enkripsi data untuk melindungi data sensitif dan memastikan bahwa kunci enkripsi dikelola dengan sistem manajemen kunci yang aman.
3) Mengadopsi pendekatan pertahanan dalam kedalaman, dengan lapisan keamanan berganda untuk melindungi terhadap serangan siber yang berbeda.
4) Melakukan penilaian keamanan secara berkala dan pengujian penetrasi untuk mengidentifikasi dan

mengatasi kerentanan sebelum dapat dimanfaatkan oleh penyerang.

5) Memastikan bahwa semua pemangku kepentingan memahami kebijakan keamanan organisasi dan konsekuensi dari tidak mematuhi standar tersebut.

4.5.2 Meningkatkan Keamanan Siber dalam BI

Dalam era digital yang didominasi oleh Big Data dan teknologi cloud, keamanan siber menjadi aspek kritis dalam pengelolaan dan analisis data bisnis. Untuk menilai dan meningkatkan kesiapan organisasi dalam menghadapi tantangan keamanan big data, model kematangan keamanan big data, yang berakar pada Capability Maturity Model oleh Software Engineering Institute (SEI) di Carnegie Mellon University (Paulk, 1995), menawarkan kerangka kerja yang komprehensif. Model ini membagi kesiapan keamanan big data ke dalam lima level kematangan: awal, dapat diulang, ditentukan, dikelola, dan optimalisasi, yang masing-masing menandakan peningkatan dalam prediktabilitas, efektivitas, dan pengelolaan keamanan data.

1) Tingkat Tidak Ada
   Pada level ini, organisasi belum menyadari risiko dan tantangan keamanan yang terkait dengan big data.
2) Tahap Awal
   Organisasi mulai mengakui pentingnya manajemen keamanan big data dan menerapkan proses yang belum terdokumentasi, sering kali secara ad hoc, yang menghasilkan keluaran yang tidak terprediksi.
3) Tahap Pengembangan
   Dilakukan penilaian risiko keamanan big data yang kompleks, mengidentifikasi area utama yang

memerlukan perhatian, dan mendokumentasikan proses keamanan big data.

4) Tingkat Ditentukan
   Proses keamanan big data telah distandarisasi dan menjadi bagian dari operasi bisnis sehari-hari.
5) Tingkat Dikelola
   Organisasi menetapkan metrik kinerja untuk menilai efektivitas proses keamanan big data, memungkinkan perbaikan berkelanjutan.
6) Tingkat Optimalisasi
   Proses keamanan big data disesuaikan untuk mencapai efisiensi maksimal, mewakili tingkat keamanan yang paling canggih.

Dengan kemajuan teknologi informasi dan komunikasi (TIK) serta Industri 4.0, termasuk Big Data dan cloud computing, pentingnya membangun keamanan siber yang tangguh menjadi semakin penting. Gołębiowska et al., (2021) menggarisbawahi bahwa perkembangan teknologi ini sangat bergantung pada teknik dan perangkat yang memungkinkan akses ke internet, yang pada gilirannya, mempengaruhi cara organisasi mengamankan data dan infrastruktur TI.

4.5.3 Penguatan Cyber Security dalam BI

Dalam era digital yang ditandai dengan perkembangan pesat teknologi informasi dan komunikasi (TIK), keamanan siber menjadi aspek fundamental dalam pengelolaan dan analisis data bisnis. Gołębiowska et al., (2021) menekankan pentingnya kesadaran akan keamanan siber, terutama dalam menghadapi risiko yang terus

berkembang terhadap infrastruktur penting di internet. Pendekatan yang komprehensif terhadap keamanan siber, yang mencakup aspek legislatif eksternal dan tindakan internal entitas, menjadi krusial untuk menanggapi tantangan ini secara efektif.

Dengan meningkatnya penerapan teknologi Big Data, cloud computing, Internet of Things, machine learning, dan kecerdasan buatan, pentingnya dan kemungkinan aplikasi Business Intelligence (BI) dalam analisis ekonomi perusahaan, lembaga keuangan, dan entitas publik menjadi semakin signifikan. Model analitik kompleks multifaktorial dalam BI, seperti yang diuraikan oleh Prokopowicz (2017), memungkinkan analisis hasil kuantitatif penelitian ilmiah yang dilakukan dengan metode ekonometrik, menjamin objektivitas dan validitas temuan penelitian.

Penggunaan TIK dalam analisis ekonometrik dan statistik, seperti yang dijelaskan oleh Opolska-Bielańska (2019), memungkinkan otomatisasi dan standardisasi dalam verifikasi data kuantitatif, mengurangi biaya analisis dan meningkatkan efisiensi proses. Kemajuan teknologi Industri 4.0 mendukung pengembangan analitik berbasis data canggih, memfasilitasi analisis dan pelaporan multi-kriteria yang tidak mungkin dilakukan tanpa penggunaan model ekonometrik yang kompleks (Chang, 2018).

Dalam konteks ini, keamanan siber menjadi aspek penting yang harus diperhatikan oleh entitas bisnis yang menggunakan platform analitis terkomputerisasi seperti BI, Data Science, dan Big Data Analytics. Mengadopsi prinsip "Privacy by Design" dan praktik terbaik keamanan big data, serta menerapkan model kematangan keamanan big data

yang dibangun berdasarkan Capability Maturity Model, merupakan langkah strategis untuk memastikan keamanan data dalam proses analitis.

Sebagai respons terhadap peningkatan digitalisasi dan internasionalisasi proses ekonomi, terutama selama pandemi SARS-CoV-2 (Covid-19), Golczak (2020) menyoroti peningkatan legitimasi penggunaan BI dan Analisis Big Data dalam entitas bisnis. Integrasi strategi keamanan siber yang kuat dalam penggunaan BI dan teknologi terkait menjadi kunci untuk memastikan bahwa data bisnis dilindungi secara efektif dari ancaman siber, sambil memanfaatkan potensi penuh dari analisis data untuk mendukung pengambilan keputusan dan meningkatkan efektivitas kegiatan bisnis.

BAB V

Eksplorasi Literatur Compliance Risk Management (CRM) dan Integrasinya dengan Audit Pajak

Peran utama administrasi perpajakan adalah mengumpulkan pendapatan negara untuk membiayai berbagai program sosial dan ekonomi. Kepatuhan wajib pajak menjadi kunci dalam mencapai tujuan ini. Penggunaan *Compliance Risk Management* (CRM) dalam administrasi perpajakan (Betts, 2022) dapat membantu mengidentifikasi dan memfokuskan sumber daya pada wajib pajak dengan risiko ketidakpatuhan tinggi, sehingga meningkatkan efisiensi dan efektivitas penagihan pajak. Penerapan CRM juga mampu mendorong budaya kepatuhan pajak dengan menciptakan kepastian hukum dan keadilan bagi semua wajib pajak.

5.1 Konsep Compliance Risk Management (CRM) dan Audit Pajak

Dalam administrasi pajak, pendekatan terhadap manajemen risiko kepatuhan (CRM) dan audit pajak telah mengalami transformasi signifikan, mendorong ke efektivitas dan keadilan yang lebih besar dalam sistem perpajakan. OECD (2017) dan studi oleh Advani et al., (2023), menyoroti bagaimana inovasi dalam bidang ini telah

membentuk strategi baru yang mendasari proses audit pajak dan Compliance Risk Management (CRM).

5.1.1 Manajemen Risiko Kepatuhan (CRM)

Manajemen risiko pajak adalah proses dinamis yang melibatkan identifikasi cermat dan penanganan potensi risiko kepatuhan pajak dari wajib pajak (Advani et al., 2023). Manajemen risiko ini mencakup evaluasi komprehensif terhadap risiko penghindaran pajak, pelaporan yang tidak akurat, dan kegiatan ilegal lainnya.

5.1.1.1 Definisi Manajemen Risiko

Manajemen risiko merupakan suatu strategi krusial yang diterapkan oleh organisasi untuk memastikan pencapaian tujuan bisnis mereka secara efektif. Definisi risiko, menurut COSO (2020), merujuk pada potensi terjadinya peristiwa yang dapat mempengaruhi pencapaian strategi dan tujuan bisnis. Ini mencakup risiko kepatuhan, yang berkaitan dengan potensi pelanggaran terhadap hukum, regulasi, dan standar yang dapat berujung pada konsekuensi finansial atau sanksi lainnya.

UNECE (2018) menggambarkan manajemen risiko sebagai sebuah model organisasi yang memperkuat kualitas proses manajerial dengan menganalisis potensi peristiwa yang belum terjadi. Berbeda dengan sistem manajerial lainnya, manajemen risiko menawarkan perspektif unik yang melintasi berbagai fungsi organisasi seperti perencanaan, pengendalian, evaluasi kinerja, dan audit.

Tujuan Utama Manajemen Risiko:

1) Meningkatkan Nilai dan Etika. Mendukung nilai inti dan memperkuat rasa memiliki di antara stakeholder.
2) Melindungi aset tangibel dan intangibel organisasi.
3) Mendorong pertumbuhan budaya organisasi yang positif.
4) Memperkuat kepemimpinan dan memperbaiki hubungan internal dan eksternal.
5) Meningkatkan efektivitas dan efisiensi operasional.
6) Memastikan sumber daya dialokasikan untuk prioritas strategis.
7) Meningkatkan kepuasan stakeholder melalui pengelolaan risiko yang efektif.

Manajemen risiko bukan hanya tentang menghindari risiko, tetapi juga tentang mengidentifikasi dan memanfaatkan peluang yang dapat meningkatkan nilai entitas. Proses ini, yang melibatkan semua level organisasi dari dewan direksi hingga karyawan, bertujuan untuk mengidentifikasi potensi peristiwa yang dapat mempengaruhi entitas dan mengelola risiko sesuai dengan toleransi risiko organisasi untuk memastikan pencapaian tujuan secara optimal.

Dengan demikian, manajemen risiko adalah alat esensial untuk navigasi organisasi yang sukses, memastikan bahwa setiap keputusan dibuat dengan pemahaman yang komprehensif terhadap potensi risiko dan peluang. Ini adalah pendekatan holistik yang tidak hanya mempertahankan keberlangsungan bisnis tetapi juga memandu organisasi menuju pertumbuhan dan inovasi yang berkelanjutan.

5.1.1.2 Standar Internasional Program Kepatuhan

Dalam upaya meningkatkan tata kelola dan kepatuhan organisasi, Organisasi Internasional untuk Standardisasi (ISO) memainkan peran krusial melalui pengembangan standar internasional. ISO 19600:2014, yang berfokus pada sistem manajemen kepatuhan, telah memberikan kerangka kerja komprehensif bagi organisasi untuk mengelola kepatuhan mereka secara efektif. ISO telah mengusulkan rancangan standar baru, ISO/DIS 37301 pada tahun 2020, yang bertujuan untuk menggantikan ISO 19600 dengan menguraikan lima elemen sistem manajemen kepatuhan sebagai berikut:

1) Kewajiban Kepatuhan
   Elemen ini memfokuskan pada identifikasi dan pemahaman terhadap persyaratan kepatuhan baru dan yang telah diubah. Identifikasi ini melibatkan pemantauan peraturan terkini dan relevan untuk memastikan organisasi tetap sesuai dan responsif terhadap perubahan lingkungan hukum dan regulasi.
2) Penilaian Risiko Kepatuhan
   Penilaian risiko kepatuhan ini mengacu pada proses evaluasi risiko yang terkait dengan kemungkinan pelanggaran terhadap peraturan, standar, dan kebijakan internal. Penilaian ini membantu organisasi menentukan area mana yang memerlukan perhatian khusus dan sumber daya untuk mengurangi kemungkinan ketidakpatuhan.
3) Kebijakan Kepatuhan
   Merupakan pedoman resmi organisasi yang menguraikan komitmen dan pendekatannya terhadap kepatuhan. Kebijakan ini menetapkan ekspektasi

untuk perilaku dan prosedur dalam memenuhi kewajiban hukum dan regulasi, serta standar etika organisasi.

4) Komponen ini menekankan pentingnya memberikan pelatihan yang memadai kepada karyawan mengenai kebijakan dan prosedur kepatuhan, serta memastikan bahwa informasi penting tentang kepatuhan disampaikan secara efektif ke seluruh tingkatan organisasi. Ini bertujuan untuk membangun kesadaran dan memperkuat budaya kepatuhan.
5) Evaluasi Kinerja
   Melibatkan pengukuran dan penilaian terhadap efektivitas sistem manajemen kepatuhan organisasi. Ini termasuk penggunaan audit internal, review, dan metode lain untuk menilai apakah kebijakan dan prosedur kepatuhan telah diimplementasikan dengan baik dan memberikan hasil yang diharapkan.

Standar ISO/DIS 37301 menawarkan kerangka kerja yang terstruktur dan holistik untuk membangun, mengimplementasikan, memelihara, dan meningkatkan sistem manajemen kepatuhan. Melalui penerapan lima elemen kunci ini, organisasi dapat lebih efektif dalam mengelola risiko kepatuhan, memastikan integritas operasional, dan memperkuat reputasi mereka dalam lingkungan bisnis yang semakin diatur dan berisiko.

5.1.1.3 Hubungan Kepatuhan dengan Pengendalian Internal dan Manajemen Risiko

Dalam lingkungan bisnis yang kompleks dan berubah-ubah, pemahaman tentang bagaimana kepatuhan, pengendalian internal, dan manajemen risiko berinteraksi merupakan faktor kunci dalam menjaga integritas operasional dan keberlanjutan organisasi. Framework dari Committee of Sponsoring Organizations of the Treadway Commission (COSO) memberikan panduan komprehensif dalam mengintegrasikan ketiga aspek ini untuk mencapai tujuan organisasi.

COSO mendefinisikan pengendalian internal sebagai proses yang dirancang untuk memberikan keyakinan yang wajar mengenai pencapaian tujuan organisasi dalam tiga kategori: operasi, pelaporan, dan kepatuhan. Kerangka kerja ini menekankan bahwa pengendalian internal melampaui masalah keuangan dan akuntansi untuk mencakup kepatuhan terhadap undang-undang dan regulasi sebagai salah satu tujuan utamanya.

Lima Komponen Pengendalian Internal dalam kerangka kerja COSO:

1) Pengendalian Lingkungan
   Fondasi untuk sistem pengendalian internal, mencakup integritas, nilai etika, dan lingkungan operasional.
2) Penilaian Risiko
   Proses identifikasi dan penilaian risiko yang dapat mempengaruhi pencapaian tujuan.
3) Aktivitas Pengendalian

Kebijakan dan prosedur yang membantu memastikan bahwa arahan manajemen dilaksanakan.

4) Informasi dan Komunikasi
   Sistem yang memastikan informasi penting diidentifikasi, diambil, dan dikomunikasikan dalam bentuk dan waktu yang memungkinkan orang melakukan tugasnya.
5) Kegiatan Pemantauan
   Proses untuk menilai kualitas kinerja sistem pengendalian internal dari waktu ke waktu.

Kerangka COSO ERM

ERM didefinisikan oleh COSO sebagai budaya, kapabilitas, dan praktik yang terintegrasi dengan strategi dan kinerja organisasi, yang diandalkan untuk mengelola risiko dalam menciptakan, melestarikan, dan mewujudkan nilai. Seperti kerangka pengendalian internal, kerangka COSO ERM juga terdiri dari lima komponen yang saling terkait:

1) Pemerintahan & Budaya
   Mendorong perilaku yang tepat dalam manajemen risiko, termasuk nilai-nilai organisasi dan lingkungan di mana risiko dikelola.
2) Strategi & Penetapan Tujuan
   Menyelaraskan tujuan risiko dengan strategi dan tujuan bisnis.
3) Pertunjukan
   Mengidentifikasi dan mengelola risiko dalam pencapaian tujuan.
4) Tinjau dan Revisi
   Menilai dan meningkatkan proses manajemen risiko berdasarkan perubahan internal dan eksternal.

5) Informasi, Komunikasi, dan Pelaporan
   Mempromosikan pertukaran informasi yang tepat tentang risiko di seluruh organisasi.

Kerangka kerja COSO, baik untuk pengendalian internal maupun ERM, menyediakan struktur untuk organisasi dalam mengelola risiko secara efektif, memastikan kepatuhan terhadap regulasi yang berlaku, dan mencapai tujuan strategisnya. Dengan mengintegrasikan kepatuhan ke dalam pengendalian internal dan manajemen risiko, organisasi dapat meningkatkan efektivitas operasional, efisiensi proses, dan kepuasan pemangku kepentingan sambil meminimalkan potensi kerugian atau sanksi.

5.1.1.4 CRM Perpajakan

Compliance Risk Management (CRM) dalam konteks perpajakan, sebagaimana dijelaskan oleh Betts (2022), mewakili metodologi strategis yang ditujukan untuk mengidentifikasi dan menangani risiko kepatuhan di antara wajib pajak. Pendekatan ini memungkinkan administrator pajak untuk mengambil keputusan yang informasi dalam mengatasi ketidakpatuhan dan secara efektif mendorong tingkat kepatuhan sukarela yang lebih tinggi di masa depan.

Tujuan utama dari CRM menurut Betts (2022) adalah untuk mengoptimalkan kepatuhan terhadap empat kewajiban utama wajib pajak: registrasi, pengajuan tepat waktu, pelaporan yang akurat, dan pembayaran tepat waktu. Keempat kewajiban ini, disebut sebagai pilar kepatuhan, merupakan dasar dari tanggung jawab administrasi pajak dalam mengumpulkan pendapatan negara.

CRM bertujuan untuk memastikan bahwa:

1) Registrasi
   Wajib pajak mendaftar untuk pajak sesuai kebutuhan.
2) Pengajuan Tepat Waktu
   Pernyataan pajak disampaikan dalam batas waktu yang ditentukan.
3) Pelaporan yang Benar
   Kewajiban perpajakan dilaporkan dengan akurasi.
4) Pembayaran Tepat Waktu
   Pembayaran pajak dilakukan sesuai jadwal.

Melalui analisis risiko yang komprehensif, sistem penilaian risiko CRM memastikan bahwa keempat pilar ini diperhitungkan, mengkategorikan risiko sebagai tinggi, sedang, atau rendah dalam setiap aspek kepatuhan, dan mengembangkan strategi mitigasi yang sesuai untuk menghadapi risiko yang teridentifikasi.

CRM bukanlah sekadar pemilihan kasus untuk audit. Sebaliknya, itu merupakan pendekatan end-to-end yang mencakup seluruh spektrum kepatuhan, menyesuaikan penanganan berdasarkan tingkat dan sifat ketidakpatuhan yang dihadapi. Dengan memprioritaskan intervensi dan sumber daya, CRM memungkinkan tindakan yang lebih terfokus dan ekonomis, seperti pendidikan dan komunikasi, untuk mencegah ketidakpatuhan sebelum terjadi. Audit dan investigasi, yang merupakan tindakan yang paling mahal, diperuntukkan hanya untuk kasus-kasus ketidakpatuhan yang paling serius dan berisiko.

CRM dalam perpajakan menawarkan kerangka kerja yang dinamis dan responsif untuk meningkatkan kepatuhan pajak, mengurangi risiko ketidakpatuhan, dan secara efisien

mengalokasikan sumber daya. Dengan fokus pada pemahaman dan mitigasi risiko kepatuhan melalui empat pilar kepatuhan, administrasi pajak dapat lebih efektif dalam menjalankan tugasnya, memastikan keadilan dalam sistem perpajakan, dan memperkuat kepercayaan publik terhadap proses pajak.

5.1.2 Peran Audit Pajak dalam Meningkatkan Kepatuhan

Pemeriksaan pajak merupakan instrumen penting dalam mencapai kepatuhan. Meskipun ancaman audit sendiri dapat mengubah perilaku kepatuhan, apa dampak pelaksanaan audit terhadap kepatuhan terhadap target audit di masa depan, jika ada. Prediksi mengenai efek pasca-audit rata-rata positif ini secara umum sejalan dengan literatur empiris yang berkembang mengenai efek pasca-audit, namun tidak sesuai dengan temuan eksperimental, yang justru konsisten dengan rata-rata efek pasca-audit negatif (Kasper & Rablen, 2023).

Berdasarkan evaluasi risiko dengan CRM, otoritas pajak menyesuaikan strategi auditnya, menargetkan sumber daya pada wajib pajak atau sektor yang dianggap berisiko tinggi. Hal ini memastikan alokasi sumber daya audit yang efektif dan meningkatkan kepatuhan pajak secara keseluruhan. Audit pajak, sebagai alat kunci dalam arsenal CRM, memainkan peran penting dalam mempengaruhi perilaku wajib pajak. Advani et al., (2023) mengungkapkan bahwa audit tidak hanya mengoreksi ketidakpatuhan jangka pendek tetapi juga memiliki dampak jangka panjang pada perilaku pelaporan pajak, dengan efek yang bertahan hingga lima tahun setelah audit. Hal ini menegaskan peran audit

sebagai instrumen penting dalam meningkatkan kepatuhan pajak dan memaksimalkan pendapatan pajak.

Manajemen Risiko Kepatuhan (CRM) telah menjadi alat penting bagi otoritas pajak global dalam meningkatkan efisiensi dan efektivitas Audit Pajak. Berdasarkan analisis Betts (2022), CRM memainkan beberapa peran kunci dalam proses audit pajak, sebagai berikut:

1) Seleksi Target Audit yang Lebih Tepat.
   CRM memungkinkan otoritas pajak untuk mengidentifikasi dan memprioritaskan wajib pajak untuk audit berdasarkan analisis risiko kepatuhan yang komprehensif. Faktor-faktor seperti riwayat pelaporan pajak yang bermasalah, profil keuangan yang mencurigakan, dan perilaku ketidakpatuhan adalah beberapa indikator yang digunakan. Pendekatan ini memastikan bahwa sumber daya audit dialokasikan ke wajib pajak dengan risiko tinggi, memaksimalkan potensi penemuan ketidakpatuhan dan pengumpulan pajak.
2) Perencanaan dan Pelaksanaan Audit yang Efektif.
   Menggunakan insight dari CRM, otoritas pajak dapat merencanakan audit dengan lebih strategis, menetapkan ruang lingkup audit yang tepat, membentuk tim auditor dengan keahlian yang sesuai, dan merumuskan strategi audit yang efisien. Pendekatan berbasis risiko ini memungkinkan auditor untuk fokus pada area kritis, mempercepat proses audit, dan meningkatkan kualitas hasil audit.
3) Meningkatkan Efektivitas Audit.
   CRM berkontribusi pada peningkatan efektivitas audit dengan memfokuskan upaya pada area berisiko tinggi,

yang secara signifikan meningkatkan kemungkinan deteksi pelanggaran. Hal ini tidak hanya meningkatkan jumlah pajak yang berhasil dikumpulkan dari wajib pajak yang melanggar tetapi juga berfungsi sebagai pencegah bagi ketidakpatuhan pajak. Kesadaran akan sistem seleksi audit yang berbasis risiko mendorong wajib pajak untuk mematuhi peraturan pajak, berkontribusi pada budaya kepatuhan yang lebih luas.

Manajemen Risiko Kepatuhan (CRM) telah terbukti menjadi instrumen penting dalam meningkatkan efisiensi dan efektivitas audit pajak, seperti yang dijelaskan dalam "Tax Administration Diagnostic Tool" oleh Dana Moneter Internasional (IMF, 2021). Dengan menerapkan CRM, otoritas pajak dapat secara strategis mengidentifikasi, merencanakan, dan melaksanakan audit pajak, serta meningkatkan kepatuhan pajak secara keseluruhan.

1) Identifikasi Wajib Pajak Berisiko Tinggi.
   CRM memfasilitasi otoritas pajak dalam mengidentifikasi wajib pajak yang berpotensi besar terhadap risiko ketidakpatuhan. Melalui analisis data mendalam, segmentasi wajib pajak berdasarkan risiko, dan penilaian risiko yang akurat, otoritas pajak dapat menargetkan audit pada entitas yang paling mungkin menimbulkan pelanggaran pajak, memastikan penggunaan sumber daya yang lebih terfokus dan efektif.
2) Perencanaan dan Pelaksanaan Audit yang Efisien.
   Dengan informasi dari CRM, otoritas pajak dapat mengalokasikan sumber daya dengan lebih bijak, menetapkan prioritas audit pada wajib pajak berisiko

tinggi, dan merumuskan strategi audit yang disesuaikan untuk masing-masing kasus. Pendekatan ini tidak hanya meningkatkan efisiensi proses audit tetapi juga memperkuat kemungkinan deteksi dan pemulihan pajak yang tidak patuh.

3) Meningkatkan Efektivitas Audit.
CRM berkontribusi pada peningkatan efektivitas audit dengan memperbesar peluang deteksi pelanggaran pajak dan memperkuat upaya pemulihan pajak dari wajib pajak yang tidak patuh. Selain itu, keberadaan dan penerapan CRM mendorong kepatuhan pajak lebih luas di kalangan wajib pajak, membangun budaya kepatuhan pajak yang lebih baik.

Implementasi CRM dalam audit pajak membawa berbagai manfaat, termasuk peningkatan efisiensi dalam penggunaan waktu dan sumber daya auditor, peningkatan efektivitas dalam deteksi pelanggaran dan pemulihan pajak, serta promosi kepatuhan pajak yang lebih luas di antara wajib pajak.

5.2 Integrasi Compliance Risk Management (CRM) dan Audit Pajak

5.2.1 Peningkatan Efektivitas Audit Pajak dengan CRM

Dalam menghadapi tantangan global dan kompleksitas yang meningkat dalam perekonomian dan peraturan pajak, otoritas pajak di seluruh dunia berusaha untuk meningkatkan efisiensi dan efektivitas dalam mengumpulkan pajak dan memastikan kepatuhan pajak yang lebih baik. OECD, dalam publikasi 2017, menyoroti

pentingnya Compliance Risk Management (CRM) sebagai proses terstruktur yang penting bagi otoritas pajak dalam menghadapi tantangan tersebut. CRM dalam konteks audit pajak dirancang untuk mengidentifikasi, menilai, mengurutkan, dan menangani risiko kepatuhan pajak secara sistematis, dengan tujuan akhir untuk mengoptimalkan pengumpulan pajak dan meningkatkan kepatuhan pajak.

CRM melibatkan serangkaian langkah yang didefinisikan dengan baik, yang memungkinkan otoritas pajak untuk membuat keputusan yang lebih informasi dan strategis. Karena sumber daya yang tersedia untuk otoritas pajak sering terbatas, pentingnya alokasi sumber daya yang efisien tidak bisa diabaikan. Proses ini memastikan bahwa sumber daya tersebut dialokasikan untuk mengatasi risiko kepatuhan pajak yang paling signifikan, sehingga meningkatkan efektivitas keseluruhan sistem pajak.

Salah satu instrumen kunci dalam CRM adalah audit pajak, yang digunakan sebagai sarana untuk mengatasi risiko kepatuhan pajak yang telah diidentifikasi sebelumnya. Melalui pemilihan kasus atau wajib pajak yang dianggap berisiko tinggi, audit pajak menjadi lebih terfokus dan strategis. Pendekatan ini tidak hanya memperbaiki alokasi sumber daya tetapi juga meningkatkan kemungkinan mengidentifikasi dan mengoreksi ketidakpatuhan pajak.

CRM, dalam konteks audit pajak, tidak hanya membantu dalam menargetkan sumber daya audit pajak secara lebih efektif tetapi juga mendukung otoritas pajak dalam mengembangkan strategi yang lebih proaktif dan berbasis risiko dalam mengelola kepatuhan pajak. Dengan mengadopsi pendekatan terstruktur dan sistematis ini,

otoritas pajak dapat lebih baik dalam mengidentifikasi potensi risiko kepatuhan pajak dan mengambil langkah-langkah yang diperlukan untuk mengurangi atau mengeliminasi risiko tersebut. Hal ini pada akhirnya berkontribusi pada sistem pajak yang lebih adil, transparan, dan efisien, yang menguntungkan baik otoritas pajak maupun wajib pajak.

Referensi penting dalam konteks ini adalah panduan OECD 2017 tentang Compliance Risk Management, yang menyediakan kerangka kerja dan rekomendasi bagi otoritas pajak untuk mengimplementasikan CRM secara efektif dalam konteks audit pajak. Implementasi CRM yang sukses menjanjikan peningkatan kepatuhan pajak dan pengoptimalan pengumpulan pajak, memperkuat integritas dan kepercayaan dalam sistem pajak secara keseluruhan.

5.2.2 Memperkuat Keunggulan Audit Pajak dengan CRM

5.2.2.1 Integrasi Manajemen Risiko Pajak dan Audit Pajak untuk Peningkatan Kepatuhan

Dalam era globalisasi ekonomi dan perubahan dinamis lingkungan bisnis, otoritas pajak di seluruh dunia menghadapi tantangan yang semakin kompleks dalam mengelola kepatuhan pajak. "Guidance Note on Compliance Risk Management" yang dirilis oleh OECD pada tahun 2004, menyajikan kerangka kerja komprehensif untuk manajemen risiko pajak, yang menekankan pentingnya pendekatan terstruktur dalam identifikasi, penilaian, peringkat, dan penanganan risiko kepatuhan pajak. Pendekatan ini tidak hanya mendukung pengambilan keputusan yang efektif

tetapi juga memperkuat keterkaitan antara manajemen risiko pajak dan audit pajak.

Alokasi Sumber Daya dan Penetapan Prioritas: Otoritas pajak harus menggunakan sumber daya yang terbatas secara efisien untuk mengatasi risiko kepatuhan pajak. Ini melibatkan penetapan prioritas tindakan kepatuhan berdasarkan tingkat risiko dan memutuskan strategi penanganan yang paling efektif untuk mencapai hasil yang diinginkan.

1) Faktor eksternal seperti perubahan legislatif, kebijakan pemerintah, opini publik, dan kondisi ekonomi berdampak signifikan terhadap risiko kepatuhan pajak. Memahami konteks ini penting dalam mengidentifikasi kelemahan dan ancaman yang perlu ditangani untuk meminimalisir risiko.
2) Budaya organisasi, struktur, teknologi informasi dan sistem bisnis, serta kemampuan staf merupakan aspek penting dalam manajemen risiko pajak. Keterlibatan dan komitmen organisasi terhadap strategi kepatuhan pajak baru sangat krusial.
3) Risiko kepatuhan pajak harus diidentifikasi baik pada tingkat strategis maupun operasional, mempertimbangkan faktor seperti globalisasi yang dapat mengikis basis pajak dan identifikasi wajib pajak individu yang mewakili risiko tinggi.
4) Mengelompokkan wajib pajak ke dalam segmen dengan karakteristik serupa memungkinkan identifikasi risiko kepatuhan yang lebih efektif pada level segmen, memperkuat upaya manajemen risiko.
5) Manajemen risiko pajak mencakup spektrum risiko dari strategis hingga operasional, dengan berbagai

kategori risiko perantara. Proses manajemen risiko yang efektif harus diimplementasikan pada kedua tingkat tersebut.

6) Kemampuan otoritas pajak untuk memahami lanskap risiko mereka berkembang seiring dengan pendekatan identifikasi yang berkembang, memperluas opsi strategi untuk mengatasi penyebab risiko secara proaktif.

Integrasi antara manajemen risiko pajak dan audit pajak menjadi kunci dalam mengidentifikasi, menilai, dan menangani risiko kepatuhan pajak. Melalui audit pajak yang ditargetkan, otoritas pajak dapat mengalokasikan sumber daya mereka secara efisien pada area atau wajib pajak yang memiliki risiko tinggi, meningkatkan efektivitas dan efisiensi dalam mencapai kepatuhan pajak yang lebih baik..

5.2.2.2 Optimalisasi Kepatuhan Pajak Melalui Integrasi Compliance Risk Management (CRM) dalam Audit Pajak

Dalam dunia yang terus berkembang dan semakin kompleks ini, kepatuhan pajak menjadi lebih penting dari sebelumnya bagi entitas bisnis. Untuk mengatasi tantangan ini, otoritas pajak dan entitas yang diaudit mengadopsi Compliance Risk Management (CRM) sebagai bagian integral dari proses audit pajak. Berdasarkan prinsip-prinsip yang dijabarkan oleh OECD pada tahun 2017, CRM dalam konteks audit pajak adalah sebuah metodologi terstruktur yang bertujuan untuk mengidentifikasi, menilai, mengurutkan, dan menangani risiko kepatuhan pajak. Proses ini dirancang untuk mengoptimalkan pengumpulan pajak dan memastikan kepatuhan pajak yang lebih baik,

sekaligus memanfaatkan sumber daya yang terbatas secara efisien.

A. Metodologi CRM dalam Audit Pajak

Metodologi CRM dimulai dengan identifikasi risiko kepatuhan yang mungkin dihadapi oleh entitas, meliputi risiko pelaporan yang tidak akurat, penghindaran pajak, dan penggunaan skema pajak yang meragukan. Selanjutnya, auditor menilai risiko tersebut berdasarkan kemungkinan terjadinya dan dampak potensial terhadap entitas. Penilaian ini membantu dalam penentuan strategi pengelolaan risiko, yang dapat mencakup mitigasi, transfer, penerimaan, atau penghindaran risiko.

B. Alat dan Teknik CRM

Penerapan CRM dalam audit pajak melibatkan penggunaan berbagai alat dan teknik, termasuk perangkat lunak analitik untuk mengevaluasi data pajak dan mengidentifikasi pola yang tidak biasa. Wawancara dengan karyawan, pengkajian dokumen, dan prosedur uji substansi juga merupakan bagian penting dari proses ini, memberikan pemahaman mendalam tentang bagaimana entitas mengelola kepatuhan terhadap peraturan pajak.

Rencana Peningkatan Kepatuhan (Compliance Improvement Plans - CIPs) memainkan peran kunci dalam CRM dengan tujuan meningkatkan tingkat kepatuhan pajak secara keseluruhan dan meminimalkan risiko kepatuhan. CIPs biasanya mencakup serangkaian tindakan yang dirancang untuk meningkatkan kesadaran dan pemahaman tentang undang-undang pajak, memperbaiki sistem dan

proses pelaporan pajak, serta meningkatkan transparansi dan kerja sama dengan otoritas pajak.

CRM dan CIPs berkontribusi pada efektivitas audit pajak dengan memastikan bahwa entitas memiliki proses dan kontrol yang memadai untuk mematuhi hukum pajak. Dengan mengurangi risiko kepatuhan, CIPs mengurangi kemungkinan kesalahan atau penyimpangan dalam laporan pajak, yang pada gilirannya meningkatkan keakuratan dan keandalan hasil audit. Implementasi CRM dan CIPs yang efektif tidak hanya memastikan kepatuhan terhadap hukum pajak yang berlaku tetapi juga mendorong entitas untuk proaktif dalam mengelola risiko kepatuhan.

Melalui integrasi CRM yang efektif dalam audit pajak, otoritas pajak dan entitas yang diaudit dapat membangun sistem kepatuhan pajak yang lebih kuat, meningkatkan kepercayaan publik terhadap sistem pajak, dan memastikan pengumpulan pajak yang optimal. Pendekatan ini menggambarkan pentingnya kerja sama antara otoritas pajak dan entitas yang diaudit dalam mencapai tujuan kepatuhan pajak yang lebih baik.

Dalam era administrasi pajak modern, audit pajak dan manajemen risiko kepatuhan (CRM) memegang peranan krusial dalam mengoptimalkan kepatuhan wajib pajak terhadap peraturan pajak. Sesuai dengan standar yang telah dikembangkan oleh Organisasi Kerjasama Ekonomi dan Pembangunan (OECD), administrasi pajak terdepan di dunia telah mengadopsi metodologi standar untuk mengelola risiko kepatuhan. Hal ini dilakukan dengan tujuan utama untuk memaksimalkan tingkat kepatuhan pajak, seperti dijelaskan oleh Brondolo et al (2022).

Salah satu instrumen kunci dalam mencapai tujuan ini adalah rencana peningkatan kepatuhan (Compliance Improvement Plans atau CIPs), yang menyediakan pendekatan sistematis dalam mengurangi risiko kepatuhan utama yang dihadapi oleh sistem pajak. Dengan mengadopsi metodologi standar dalam merancang dan mengimplementasikan CIPs, administrasi pajak dapat memastikan pendekatan yang kohesif, konsisten, dan dapat diulang untuk meningkatkan kepatuhan wajib pajak, sekaligus melindungi pendapatan pajak.

CIPs dikembangkan dengan fokus pada segmen wajib pajak utama, sektor industri kritikal, dan area fokus penting lainnya. Ini mencakup kategori wajib pajak dengan karakteristik umum, seperti perusahaan besar, usaha kecil dan menengah (UKM), bisnis mikro, serta individu kaya, yang semuanya membutuhkan pendekatan khusus dalam analisis dan pengobatan risiko.

Komponen utama dari CIPs internasional meliputi:

1) Merupakan ringkasan dari pendekatan yang akan diadopsi dalam mengelola kepatuhan pada segmen, sektor, atau area fokus tertentu.
2) Menyoroti karakteristik kunci dari segmen, sektor, atau area fokus tertentu.
3) Mengidentifikasi risiko kepatuhan utama dan menyediakan penilaian untuk setiap risiko.
4) Menjabarkan aksi utama yang diambil untuk mengurangi risiko yang telah diidentifikasi.
5) Mewakili jumlah dan jenis pengobatan yang akan diterapkan untuk mengatasi risiko.
6) Menetapkan kriteria untuk mengevaluasi efektivitas CIP dalam meningkatkan kepatuhan.

7) Mendeskripsikan kemampuan administrasi pajak yang perlu diperkuat untuk mendukung implementasi CIP.

Melalui penerapan CRM dan CIPs yang efektif, administrasi pajak dapat memastikan kepatuhan pajak yang lebih baik dan meningkatkan kepercayaan publik terhadap sistem pajak. Ini tidak hanya membantu dalam mengurangi risiko kepatuhan tetapi juga memastikan bahwa entitas yang diaudit memiliki proses dan kontrol yang memadai untuk mematuhi hukum pajak, memperkuat fondasi keuangan dan reputasi sistem pajak secara keseluruhan.

5.2.2.3 Penerapan Audit Pajak dan CRM untuk Optimalisasi Pendapatan Pajak

Dalam era digital dan globalisasi ekonomi saat ini, administrasi pajak menghadapi tantangan yang semakin kompleks dalam mengoptimalkan pengumpulan pendapatan dan memastikan kepatuhan pajak yang tinggi. Konsep audit pajak dan Manajemen Risiko Kepatuhan (CRM) menawarkan solusi strategis untuk mengatasi tantangan tersebut. Menurut Brondolo et al (2022), dan diperkuat oleh penelitian Betts (2022) dan Chan et al (2022), pendekatan sistematis dalam CRM memungkinkan administrasi pajak untuk secara efektif mengidentifikasi, menilai, dan mengurangi risiko kepatuhan, yang pada gilirannya meningkatkan efisiensi pengumpulan pendapatan pajak.

CRM dalam audit pajak dimulai dengan proses identifikasi risiko kepatuhan yang mungkin dihadapi oleh populasi wajib pajak. Ini melibatkan analisis terperinci

terhadap berbagai indikator kepatuhan, seperti pendaftaran wajib pajak, pengisian pengembalian pajak tepat waktu, pelaporan yang akurat, dan pembayaran pajak yang tepat waktu. Dengan memprioritaskan risiko ini, administrasi pajak dapat mengembangkan strategi yang ditargetkan untuk mengatasinya, termasuk pendidikan pajak, pengingat, pengisian pengembalian pajak terlebih dahulu, audit, dan investigasi.

Salah satu inovasi terbaru dalam metodologi audit pajak adalah penggunaan Jaringan Saraf Tiruan (ANNs) untuk meningkatkan efektivitas pemilihan kasus audit. Seperti yang diungkapkan oleh Chan et al (2022), studi ini menganalisis dataset dari bisnis restoran selama sepuluh tahun, menunjukkan bahwa ANNs dapat secara signifikan meningkatkan presisi dan recall dalam mengidentifikasi kasus audit yang potensial. Hal ini memungkinkan administrasi pajak untuk lebih efisien mengalokasikan sumber dayanya, meningkatkan keadilan dalam pemilihan kasus audit, dan akhirnya, meningkatkan pendapatan pajak.

Rencana Peningkatan Kepatuhan (CIPs) merupakan bagian integral dari strategi CRM, seperti yang dijelaskan oleh Brondolo et al (2022). CIPs menyediakan kerangka kerja sistematis untuk mengurangi risiko kepatuhan utama dan meningkatkan kepatuhan wajib pajak. Melalui pengembangan dan implementasi CIPs yang ditargetkan, administrasi pajak dapat memastikan pendekatan yang kohesif, konsisten, dan dapat diulang dalam meningkatkan kepatuhan dan melindungi pendapatan pajak.

Implementasi CRM dan audit pajak yang berbasis teknologi dan data, dikombinasikan dengan inisiatif CIPs,

menunjukkan langkah maju yang signifikan dalam upaya administrasi pajak untuk menghadapi tantangan modern dan memaksimalkan efisiensi pengumpulan pendapatan. Pendekatan ini tidak hanya memperkuat kepatuhan pajak tetapi juga membangun kepercayaan publik terhadap sistem pajak, memastikan bahwa semua wajib pajak memberikan kontribusi yang adil dan tepat terhadap pendapatan negara.

5.3 Integrasi Psikologi, Data Besar, dan CRM

5.3.1 Integrasi Psikologi dan CRM dalam Audit Pajak

Dalam era digital saat ini, penelitian dan praktik dalam audit pajak dan Manajemen Risiko Kepatuhan (CRM) telah mengalami evolusi signifikan, sebagaimana dijelaskan oleh OECD Tax Administration (2022). Studi oleh Chan & Song (2021) menyoroti pentingnya memahami psikologi wajib pajak dalam meningkatkan kepatuhan pajak. Ditemukan bahwa individu dengan tendensi untuk tidak mempertimbangkan konsekuensi masa depan, tingkat Machiavellianisme yang tinggi, atau persepsi rendah terhadap etika dan tanggung jawab sosial cenderung lebih patuh ketika dihadapkan pada risiko audit pajak yang tinggi. Penemuan ini menekankan perlunya otoritas pajak untuk meningkatkan kesadaran mengenai risiko audit dan pentingnya nilai etika serta tanggung jawab sosial dalam mematuhi hukum pajak.

Selain itu, digitalisasi dan aksesibilitas data yang lebih besar telah memberikan otoritas pajak alat dan teknik baru untuk meningkatkan kepatuhan pajak. Dengan penggunaan teknik ilmu data dan alat analitis, administrasi pajak

sekarang dapat memanfaatkan data dari berbagai sumber seperti e-invoicing, kasir online, informasi akun keuangan, serta data transaksional dari bank, pedagang, atau penyedia layanan pembayaran untuk verifikasi langsung pendapatan atau aset yang dilaporkan oleh wajib pajak. Kemampuan untuk mengumpulkan dan menganalisis data dari pemasok, pelanggan, internet, dan media sosial telah meningkatkan signifikan dalam mengidentifikasi risiko kepatuhan.

Pendekatan ini tidak hanya terbatas pada pengumpulan dan analisis data tetapi juga termasuk penerapan analisis perilaku untuk memahami pola perilaku wajib pajak dan mengembangkan intervensi kepatuhan yang efektif. Integrasi data besar dan analisis perilaku membuka kemungkinan baru dalam membangun pemahaman yang lebih holistik tentang risiko kepatuhan dan mengembangkan strategi yang ditargetkan untuk meningkatkan kepatuhan pajak.

Revolusi dalam kepatuhan pajak yang dijelaskan oleh OECD menunjukkan pergeseran menuju pendekatan yang lebih terarah dan terkelola dalam menghadapi kepatuhan pajak, didorong oleh kemajuan teknologi dan pemahaman yang lebih dalam tentang faktor psikologis. Dengan semakin banyaknya data yang tersedia secara elektronik dan kemudahan dalam transfer, penyimpanan, serta integrasi data, otoritas pajak kini memiliki kemampuan yang belum pernah terjadi sebelumnya untuk mengoptimalkan pengumpulan pendapatan pajak dan memastikan kepatuhan yang lebih tinggi di seluruh sistem pajak. Kesimpulannya, kombinasi antara metodologi, alat, dan teknik yang digunakan dalam audit pajak, bersama dengan pemahaman tentang psikologi wajib pajak, menandai babak

baru dalam usaha meningkatkan kepatuhan pajak dan mengoptimalkan pendapatan pajak.

5.3.2 Audit Pajak dan CRM dalam Pendekatan FMEA

Dokumen oleh Ferenc Bognar (2021) menawarkan wawasan komprehensif mengenai Audit Pajak dan Compliance Risk Management (CRM), dengan fokus pada penggunaan metodologi, alat, dan teknik yang efektif dalam mengelola risiko kepatuhan pajak. Dokumen ini membahas bagaimana manajemen kepatuhan dan audit pajak berperan penting dalam memastikan bahwa organisasi beroperasi sesuai dengan regulasi eksternal dan internal yang berlaku, serta memenuhi harapan masyarakat.

1) Manajemen Kepatuhan dan Audit Pajak
    - Manajemen Kepatuhan
      Didefinisikan sebagai proses pemantauan dan pengelolaan kepatuhan terhadap regulasi eksternal dan internal, yang esensial bagi keberhasilan bisnis dan perkembangan masyarakat yang harmonis.
    - Pendekatan Risiko dalam Manajemen Kepatuhan
      Mengakui bahwa kepatuhan telah menjadi tugas yang independen dan luas, mencakup aspek finansial, ekonomi, pajak, bisnis, legal, etis, keberlanjutan, dan kepemilikan perusahaan.
    - Kerangka Kontrol Internal Terintegrasi COSO
      Menyajikan fondasi untuk pengembangan fungsi kepatuhan, menganut pendekatan berbasis risiko yang terfokus pada kontrol.

2) Metodologi, Alat, dan Teknik:
    - Failure Mode and Effects Analysis (FMEA)
      Sebagai metodologi analisis risiko taktis, FMEA menilai keparahan konsekuensi, frekuensi kejadian, dan probabilitas deteksi, menghasilkan Risk Priority Number (RPN) untuk setiap risiko.
    - Konsistensi dalam Evaluasi Risiko
      Menggunakan metode statistik untuk mengevaluasi konsistensi dalam keputusan manajemen risiko, memastikan bahwa evaluasi risiko bersifat objektif dan dapat diandalkan.
    - Pengumpulan Data
      Melalui fokus kelompok yang melibatkan para ahli kepatuhan, memungkinkan penilaian kasus spesifik dalam manajemen risiko dengan lebih efektif.
    - Skala Penilaian
      Modifikasi skala penilaian untuk memenuhi kebutuhan pengukuran atau estimasi risiko, memfasilitasi analisis yang lebih akurat.
    - Penerapan dalam Manajemen Risiko
      FMEA memungkinkan identifikasi dan mitigasi risiko secara proaktif, dengan prioritas tindakan mitigasi ditentukan berdasarkan RPN.

Efektivitas kepatuhan dan manajemen risiko menjadi krusial dalam audit pajak, di mana adaptasi terhadap perubahan lingkungan mendukung penilaian risiko yang lebih tepat. Integrasi sistem manajemen risiko mencakup identifikasi, penilaian, dan persiapan manajemen risiko, termasuk dalam konteks pajak.

Dalam dunia yang terus berubah, di mana peraturan dan kepatuhan menjadi semakin kompleks, Ferenc Bognar (2021) memberikan pandangan baru dan mendalam mengenai Audit Pajak dan Manajemen Risiko Kepatuhan, dalam konteks metodologi, alat, dan teknik yang digunakan dalam audit pajak untuk mengidentifikasi dan mengelola risiko kepatuhan.

A. Integrasi Model Pertahanan Tiga Garis dalam Manajemen Kepatuhan

Model Pertahanan Tiga Garis yang diperbarui oleh Institut Auditor Internal pada tahun 2020, menekankan pentingnya kerja sama antara berbagai lini pertahanan dalam organisasi untuk memperkuat kepatuhan dan manajemen risiko. Ini tidak hanya mencakup manajemen risiko internal tetapi juga audit internal dan fungsi pengawasan lainnya, memberikan kerangka kerja yang jelas untuk melindungi organisasi sambil mendukung operasional dan keberlanjutan bisnis.

B. Keunggulan Metodologi FMEA dalam Sektor Keuangan

FMEA, sebagai metodologi analisis risiko, telah menunjukkan keefektifannya dalam sektor keuangan dengan menilai dan mengurangi risiko melalui rencana aksi yang ditargetkan. Implementasi FMEA dalam konteks keuangan tidak hanya memperkuat sistem pengendalian internal tetapi juga memfasilitasi identifikasi dan mitigasi risiko operasional dan kepatuhan sebelum mereka mempengaruhi operasi bisnis.

5.4 Cybersecurity dalam CRM

5.4.1 Urgensi Keamanan Siber dengan CRM

Di era yang ditandai dengan meningkatnya ancaman serangan siber, perlindungan terhadap data pajak menempati prioritas utama bagi entitas pemerintahan, khususnya otoritas perpajakan. Calderon et al. (2021) menyoroti bahwa file elektronik yang dipersiapkan untuk Surat Pemberitahuan Tahunan (SPT) orang pribadi berisikan informasi pribadi yang sensitif, termasuk nama lengkap, nomor Jaminan Sosial, dan rincian finansial lainnya. Informasi semacam itu merupakan target berharga bagi pelaku kejahatan siber yang dapat menyalahgunakannya untuk penipuan pajak atau aktivitas penipuan lainnya. Ini menegaskan kebutuhan akan kepatuhan terhadap peraturan dan standar internasional seperti ISO/IEC 27001 yang berkaitan dengan sistem manajemen keamanan informasi, sebagai upaya membangun fondasi keamanan siber yang tangguh.

Serangan siber pada data pajak dapat berdampak luas, mulai dari kerugian finansial bagi individu dan negara, kerusakan reputasi bagi individu dan organisasi terkait, hingga penurunan kepercayaan publik terhadap sistem perpajakan. Konsekuensi ini, sebagaimana dijelaskan oleh Calderon et al. (2021), memperjelas urgensi perlindungan data pajak dalam konteks CRM.

Kepatuhan terhadap regulasi dan standar keamanan informasi memainkan peran penting dalam mengidentifikasi dan mengelola risiko hukum serta operasional yang berkaitan dengan keamanan siber. Pendekatan proaktif dalam mengurangi kerentanan, melalui identifikasi area non-kepatuhan terhadap regulasi

keamanan siber, menjadi sangat penting. Langkah ini tidak hanya mendukung implementasi langkah-langkah keamanan yang adekuat tetapi juga memastikan keandalan sistem perpajakan dari ancaman siber.

Menghadapi peningkatan kompleksitas serangan siber, seperti phishing, malware, dan hacking, diperlukan strategi keamanan siber yang kuat dalam CRM. Calderon et al. (2021) menggarisbawahi pentingnya respons cepat dan efektif terhadap insiden keamanan siber untuk meminimalisir dampak negatif dan memastikan kelangsungan operasi yang aman serta pemulihan data yang efisien.

Peningkatan kesadaran mengenai risiko serangan siber, metodologi yang digunakan pelaku serangan, dan strategi pencegahan menjadi krusial. Inisiatif ini esensial untuk memastikan bahwa semua pihak, termasuk individu yang terlibat langsung dalam pengelolaan data pajak dan masyarakat umum, memiliki pengetahuan dan alat yang diperlukan untuk melindungi diri dari serangan siber.

Dalam sistem perpajakan Amerika Serikat, yang dicirikan oleh keragaman dan kompleksitasnya, kerentanan terhadap pelanggaran data dan tantangan integritas menjadi masalah utama. Mengacu pada kerja Calderon (2021), artikel ini mengeksplorasi kerentanan, risiko, dan tingkat paparan yang luas dalam sistem yang mendukung kepatuhan pajak di AS, dan bertujuan untuk menyoroti pentingnya integrasi keamanan siber dalam CRM sebagai langkah kritis untuk mengamankan sistem perpajakan di Indonesia dan negara-negara lain dengan tantangan serupa.

Menilai persepsi wajib pajak terhadap keamanan data perpajakan memberikan wawasan awal mengenai kerentanan sistem. Analisis lebih lanjut mengidentifikasi

entitas yang berisiko dan menganalisis bahwa sebagian besar ancaman keamanan siber dapat dimodelkan menggunakan tipologi multi-dimensi, diadaptasi dari Stallings (2003). Tipologi ini membantu dalam pemahaman dan pengembangan protokol keamanan untuk mengatasi masalah kerentanan, risiko, dan paparan yang dihadapi entitas dalam sistem perpajakan.

Dengan mengacu pada masalah keamanan perpajakan dalam jaringan virtual yang menghubungkan berbagai pihak dalam sistem, Calderon (2021) mengusulkan protokol keamanan yang dirancang untuk mengelola jenis kerentanan, risiko, dan paparan yang umum dihadapi oleh entitas. Protokol ini berfokus pada penanganan karakteristik jaringan virtual terdistribusi dan entitas yang mungkin mengeksploitasi kerentanan dalam sistem tersebut.

Dalam konteks Indonesia, pendekatan berbasis protokol yang diilhami oleh Calderon (2021) dapat menjadi alat yang berharga dalam menghadapi kerentanan serupa dalam sistem perpajakan. Mengintegrasikan keamanan siber dalam CRM, dengan menyesuaikan protokol yang sesuai dengan spesifikasi sistem perpajakan lokal, adalah kunci untuk meningkatkan ketahanan terhadap serangan siber. Protokol ini harus mencakup identifikasi dan mitigasi risiko yang spesifik terhadap lingkungan perpajakan di Indonesia, sambil mengakomodasi keragaman dan kompleksitas sistem.

5.4.2 Memperkuat CRM dalam menghadapi Serangan Siber

Dalam menghadapi tantangan keamanan pada layanan pajak, analisis keamanan mengungkapkan kerentanan signifikan yang disebabkan oleh interaksi antara berbagai entitas dengan data pajak. Sistem perpajakan menjadi rentan terutama ketika data yang tidak terenkripsi berpindah tangan, meningkatkan potensi intersepsi oleh pihak yang tidak berwenang, yang bisa berujung pada pencurian identitas dan penipuan pajak. Ancaman yang diidentifikasi oleh Model Ancaman Keamanan Pajak (TSTM) seperti intersepsi data, serangan man-in-the-middle (MITM), pembajakan sesi, phishing, dan IP spoofing, semuanya menyoroti risiko yang dapat mengkompromikan integritas data pajak (Baitha dan Vinod 2018; Aziz dan Hamilton 2009; Callegati dkk. 2009).

Menerapkan TSTM dalam kerangka Manajemen Risiko Kepatuhan (CRM) memfasilitasi identifikasi dan pengembangan protokol keamanan yang efektif untuk melindungi sistem perpajakan dari lima kategori utama serangan siber yang diuraikan oleh model tersebut, termasuk intersepsi, interupsi, penetrasi, modifikasi, dan fabrikasi. Adopsi TSTM dalam CRM tidak hanya menekankan pada pentingnya mengenkripsi data dan memastikan autentikasi yang kuat tetapi juga menggarisbawahi kebutuhan untuk memperkuat strategi komunikasi yang aman antar entitas dalam sistem perpajakan. Hal ini mendesak perluasan kesadaran dan pendidikan tentang risiko keamanan siber, mendorong penerapan praktik keamanan terbaik dan penggunaan solusi

teknis seperti enkripsi dan protokol keamanan yang robust untuk komunikasi data (Tanase 2003; Zorabedian 2019).

Dalam menghadapi serangan siber, kebutuhan untuk memperkuat CRM menjadi sangat kritis, terutama dalam sistem perpajakan yang kompleks dan beragam. Pendekatan untuk meningkatkan CRM memerlukan pemahaman yang mendalam tentang persepsi wajib pajak terhadap keamanan data pajak. Studi oleh Miniard dan Cohen (1981) dan Williams et al. (2014) menunjukkan bahwa persepsi ini secara signifikan mempengaruhi penerimaan dan implementasi praktik keamanan pajak yang baru.

Pentingnya memperkuat CRM melalui strategi yang tidak hanya fokus pada aspek teknis keamanan siber tetapi juga mempertimbangkan persepsi dan kekhawatiran wajib pajak. Kepercayaan dan keyakinan wajib pajak terhadap protokol keamanan pajak yang diimplementasikan oleh otoritas pajak adalah krusial untuk meningkatkan penerimaan dan kepatuhan terhadap praktik keamanan pajak yang baru.

1) Otoritas pajak harus secara proaktif berkomunikasi dengan publik mengenai langkah-langkah keamanan yang diambil untuk melindungi data pajak dan bagaimana wajib pajak dapat melindungi diri dari serangan siber.
2) Menggunakan analisis big data dan AI untuk memahami dan merespons secara spesifik terhadap kekhawatiran dan kebutuhan keamanan pajak dari berbagai demografi wajib pajak.
3) Membangun protokol keamanan yang tidak hanya teknis efektif tetapi juga dirancang untuk mengatasi

persepsi dan kekhawatiran spesifik yang diidentifikasi melalui analisis sentimen.

5.4.3 Strategi Cybersecurity dalam CRM

Dalam upaya untuk memperkuat manajemen risiko kepatuhan, integrasi strategi keamanan siber yang efektif menjadi sangat penting, khususnya dalam melindungi data sensitif dan memastikan kepatuhan terhadap regulasi yang berlaku. Pendekatan inovatif dan komprehensif berikut ini dirancang untuk mengoptimalkan keamanan siber sambil mendukung kepatuhan yang efektif.

Adopsi standar industri seperti Kerangka Kerja Keamanan Siber NIST menjadi langkah awal yang vital. Kerangka kerja ini memungkinkan organisasi untuk mengintegrasikan praktik keamanan siber ke dalam proses kepatuhan secara menyeluruh, memastikan bahwa setiap aspek dari keamanan informasi mendapatkan perhatian yang dibutuhkan dan sesuai dengan standar industri.

Melakukan evaluasi dan penilaian risiko secara berkala menjadi kunci dalam mengidentifikasi potensi kerentanan dan risiko keamanan siber. Penilaian ini memastikan bahwa organisasi dapat mengambil langkah-langkah pencegahan sebelum terjadinya pelanggaran keamanan, dan mempertahankan tingkat kepatuhan yang tinggi terhadap regulasi yang berlaku.

Meningkatkan kesadaran tentang keamanan siber di seluruh tingkatan organisasi melalui program pelatihan yang komprehensif merupakan komponen penting lainnya. Pelatihan ini harus mencakup pemahaman tentang risiko

keamanan siber yang umum, identifikasi potensi ancaman, dan pengembangan kebiasaan online yang aman. Program ini harus dirancang untuk mencakup berbagai segmen wajib pajak, mulai dari individu hingga korporasi besar, dan disampaikan melalui berbagai platform untuk memastikan jangkauan yang luas.

Membangun kolaborasi yang efektif antara tim kepatuhan dan keamanan siber merupakan langkah strategis untuk menciptakan sistem yang tangguh. Kerja sama ini memastikan bahwa kebijakan dan prosedur yang diterapkan mendukung baik kepatuhan regulasi maupun keamanan informasi, secara sinergis meningkatkan kedua aspek tersebut.

Penggunaan teknologi canggih seperti kecerdasan buatan (AI) dan pembelajaran mesin (machine learning) dalam sistem keamanan siber memberikan keuntungan signifikan dalam meningkatkan deteksi dan pencegahan serangan siber. Teknologi ini memungkinkan analisis data secara real-time, identifikasi aktivitas mencurigakan, dan otomatisasi respons terhadap ancaman keamanan, mempercepat identifikasi dan mitigasi risiko kepatuhan yang berkaitan dengan keamanan siber.

BAB VI

Potensi Kerentanan Cyber Security di Otoritas Pajak

6.1 Protokol Keamanan Data

6.1.1 Protokol Keamanan

Dalam upaya untuk menjamin keamanan data dan informasi yang krusial, otoritas perpajakan di Indonesia telah mengadopsi serangkaian protokol keamanan yang komprehensif, yang berfokus pada penguatan infrastruktur teknologi informasi. Langkah-langkah ini diatur dalam Surat Edaran SE-45/PJ/2020, yang secara eksplisit menekankan pentingnya menjaga keamanan aset informasi melalui kontrol akses yang ketat, enkripsi data, pemantauan jaringan yang berkelanjutan, dan penerapan pembaruan keamanan secara teratur.

Praktik-praktik spesifik dalam menjaga keamanan asset informasi sebagai berikut:

- Sebagai bagian dari kebijakan keamanan, otoritas pajak membatasi akses ke ruang dan peralatan yang mengelola aset informasi kritikal, memastikan bahwa hanya personel yang terautorisasi yang dapat mengakses area dan informasi sensitif.
- Meskipun Surat Edaran tidak secara langsung menyebutkan enkripsi, praktek ini dianggap sebagai bagian penting dari inisiatif pengamanan data dan

informasi, mengindikasikan bahwa otoritas pajak menerapkan enkripsi sebagai bagian dari strategi keamanan.

- Upaya proaktif untuk mengamankan perangkat dan fasilitas pengolahan data mencakup pemantauan jaringan yang berkelanjutan, sesuai dengan rekomendasi untuk mengamankan infrastruktur TI.
- Sesuai dengan pedoman, otoritas pajak melakukan pemeliharaan dan pemeriksaan berkala pada perangkat komputer dan sistem untuk memastikan bahwa semua pembaruan keamanan diterapkan secara tepat waktu, mencegah potensi eksploitasi kerentanan.

Dalam menerapkan protokol keamanan sesuai dengan standar yang ditetapkan oleh SE-45/PJ/2020, penting untuk dipahami bahwa tidak ada sistem yang sepenuhnya kebal terhadap serangan siber. Potensi kerentanan masih dapat muncul akibat dari perkembangan ancaman siber yang dinamis, yang memerlukan evaluasi dan peningkatan keamanan yang berkelanjutan. Adanya protokol keamanan menunjukkan komitmen organisasi dalam melindungi data dan infrastruktur TI. Namun, kerentanan dapat timbul dari berbagai sumber, termasuk teknik penetrasi yang baru dikembangkan, perangkat lunak berbahaya, dan taktik phishing yang semakin canggih. Oleh karena itu, penting bagi otoritas pajak untuk terus memperbarui dan menyesuaikan strategi keamanan dalam mengatasi ancaman terbaru dan memastikan keamanan data wajib pajak.

Otoritas pajak telah membuat langkah signifikan dalam mengimplementasikan dan mematuhi pedoman keamanan siber yang ketat. Namun, dalam menghadapi

lingkungan ancaman siber yang terus berkembang, evaluasi dan penyesuaian strategi keamanan yang berkelanjutan menjadi kunci untuk mengurangi potensi kerentanan dan memastikan keamanan data pajak. Melalui pendekatan yang dinamis dan responsif terhadap ancaman baru, otoritas pajak dapat memperkuat pertahanan terhadap serangan siber dan melindungi integritas sistem perpajakan.

6.1.2 Prosedur Proteksi Data

Dalam implementasi Big Data Analytics (BDA) dan Business Intelligence (BI), DJP sebagai otoritas pajak di Indonesia telah menerapkan serangkaian prosedur proteksi data (SE DJP Nomor SE-45/PJ/2020). Prosedur yang telah dilakukan merupakan bagian dari prektik baik prosedur proteksi data.

- Organisasi memastikan penggunaan perangkat yang dilengkapi dengan software keamanan terbaru dan sistem enkripsi. Proses autentikasi yang ketat diperlukan untuk akses sistem, yang sejalan dengan standar keamanan data yang diakui secara internasional. Prosedur ini menunjukkan kesesuaian dengan prinsip-prinsip keamanan siber umum, yang menekankan pada pentingnya enkripsi dan autentikasi yang kuat.
- Akses ke ruang server dibatasi dan dijaga, dengan prosedur pemantauan fisik dan elektronik yang ketat. Hal ini mencerminkan penerapan kontrol akses yang efektif, sebuah komponen kritikal dalam pengamanan infrastruktur TI.
- Kontrol lingkungan seperti suhu dan kelembaban menunjukkan kesadaran organisasi akan pentingnya

menjaga integritas fisik data center. Pengawasan akses yang ketat mencegah insiden keamanan yang tidak diinginkan.

- Kebijakan pembatasan penggunaan removable media dan enkripsi yang ketat menunjukkan upaya organisasi dalam mengendalikan transfer data. Hal ini sesuai dengan praktik keamanan data terbaik yang mengurangi risiko kebocoran data.
- Sistem kontrol akses berbasis peran dan audit keamanan berkala menunjukkan pendekatan yang terstruktur dan sistematis dalam mengelola akses data. Hal ini menggambarkan kesadaran akan risiko internal dan eksternal serta upaya untuk mengatasinya secara proaktif.

6.2 Analisis Kerentanan Teknis

6.2.1 Identifikasi Kerentanan Teknis

Dalam sistem BDA dan BI di otoritas pajak Indonesia, prosedur untuk identifikasi kerentanan teknis telah terstruktur dan sejalan dengan SE DJP Nomor SE-45/PJ/2020. Proses identifikasi ini melibatkan beberapa langkah yang dirancang untuk mengungkapkan dan menangani kerentanan potensial:

- Organisasi mengimplementasikan pemindaian keamanan otomatis yang terjadwal, bersama dengan penilaian risiko berkala. Pendekatan ini mewakili praktik standar dalam manajemen risiko TI, memungkinkan identifikasi cepat dan efektif dari potensi kerentanan.
- Penggunaan audit keamanan internal dan layanan pihak ketiga untuk pengujian penetrasi dan audit independen memberikan perspektif holistik.

Pendekatan ini membantu menghilangkan bias internal dan memastikan objektivitas dalam penilaian kerentanan.

- Setelah identifikasi kerentanan, protokol respons insiden yang telah ditentukan diaktifkan. Protokol ini mencakup langkah-langkah seperti isolasi sistem yang terpengaruh, analisis sebab akar, dan implementasi perbaikan. Pendekatan ini sesuai dengan prinsip-prinsip manajemen insiden siber yang disarankan oleh para ahli keamanan TI.
- Proses dokumentasi insiden dan pembelajaran yang dihasilkan merupakan bagian penting dari sistem manajemen pengetahuan di organisasi, yang memperkuat siklus pembelajaran dan peningkatan berkelanjutan.

Surat Edaran DJP Nomor: SE-45/PJ/2020, yang mengatur pengamanan data dan infrastruktur TI, menyiratkan pentingnya pendekatan holistik dalam penanganan kerentanan teknis. Prosedur yang diikuti oleh DJP mencerminkan penerapan prinsip-prinsip ini melalui:

- Perlindungan data melalui password dan autentikasi adalah langkah dasar namun kritikal dalam keamanan siber.
- Kontrol akses fisik yang ketat untuk ruang server dan data center menunjukkan pengakuan DJP akan pentingnya pengamanan infrastruktur fisik.
- Praktik ini menjamin bahwa perangkat dan sistem terus beroperasi sesuai standar keamanan yang ditetapkan.
- Pengendalian lingkungan data center merupakan langkah penting untuk menjaga integritas dan keandalan infrastruktur TI.

- Kebijakan penggunaan removable media yang ketat mengurangi risiko kebocoran data.
- Audit ini membantu dalam mengevaluasi dan meningkatkan efektivitas kebijakan dan prosedur keamanan yang ada.
- Program pelatihan yang berkelanjutan meningkatkan kesadaran dan kepatuhan terhadap keamanan di kalangan staf.
- Perawatan dan pemeriksaan berkala atas perangkat dan lingkungan data center memastikan keamanan operasional yang efektif.

Kesiapan dan respons yang efektif terhadap kerentanan teknis merupakan kunci dalam menjaga keamanan data dan sistem dalam lingkungan BDA dan BI.

6.2.2 Potensi Eksploitasi Akibat Kerentanan Teknis

Dalam kerangka kerja keamanan siber, potensi eksploitasi akibat kerentanan teknis merupakan area penting yang memerlukan penelaahan mendalam. Otoritas pajak harus mampu mendokumentasikan insiden-insiden tertentu yang menggambarkan bagaimana kerentanan teknis dapat menyebabkan eksploitasi yang serius, dengan merujuk pada kasus-kasus spesifik:

- Sebuah insiden menyoroti kerentanan dalam sistem autentikasi pengguna, di mana kelemahan pada proses verifikasi memungkinkan serangan brute-force. Eksploitasi dari kerentanan ini berpotensi memungkinkan akses tidak sah ke data yang sangat sensitif. Hal ini menyoroti pentingnya kekuatan mekanisme autentikasi dalam sistem keamanan informasi.

- Kasus lain mencakup konfigurasi yang salah pada server aplikasi, yang mengakibatkan pengiriman data sensitif tanpa enkripsi yang adekuat. Risiko dalam situasi ini adalah kemungkinan pengintersepsian data oleh penyerang melalui teknik sniffing. Risiko tersebut menekankan pentingnya enkripsi yang tepat dan konfigurasi keamanan yang ketat dalam pengelolaan data.

Langkah-langkah responsif yang diambil oleh otoritas pajak setelah mengidentifikasi kerentanan ini termasuk:

- Implementasi mekanisme penguncian akun setelah beberapa upaya login yang gagal, yang menunjukkan respons proaktif terhadap ancaman brute-force.
- Memperkuat enkripsi pada komunikasi data dan mengoptimalkan konfigurasi keamanan jaringan untuk mencegah kebocoran data.

Insiden-insiden ini memberikan wawasan kritis tentang dinamika kerentanan dan eksploitasi dalam konteks keamanan siber. Hal ini menyoroti bagaimana otoritas pajak telah merespons secara efektif terhadap insiden keamanan, sesuai dengan pedoman. Respons ini tidak hanya memperlihatkan kapabilitas teknis organisasi dalam menangani kerentanan, tetapi juga refleksi dari komitmen institusi terhadap pengelolaan risiko keamanan siber yang efektif. Pentingnya pemantauan konstan dan evaluasi keamanan, sebagaimana ditunjukkan oleh insiden-insiden ini, tidak bisa dilebih-tegaskan. Otoritas pajak di Indonesia telah menunjukkan bagaimana deteksi dini dan respons yang cepat dan terukur dapat mengurangi risiko eksploitasi

secara signifikan dan memperkuat integritas keseluruhan sistem keamanan informasi.

6.3 Tantangan Infrastruktur

6.3.1 Infrastruktur TI Eksisting

Dalam mendukung sistem BDA dan BI, infrastruktur TI pada otoritas pajak telah dikembangkan untuk memenuhi standar keamanan dan keandalan. Berikut adalah aspek kunci dari infrastruktur TI:

- Ruang server dan data center kami dilengkapi dengan sistem keamanan fisik yang ketat, termasuk pengawasan CCTV, kontrol akses biometrik, dan pengamanan oleh penjaga keamanan, guna mencegah akses tidak sah.
- Redundansi telah terintegrasi dalam sistem, dengan protokol disaster recovery dan business continuity, memastikan layanan BDA dan BI tetap operasional meskipun terjadi gangguan.
- Organisasi melakukan pemeliharaan dan pembaruan terjadwal untuk memastikan kinerja maksimal dari semua perangkat keras dan perangkat lunak.
- Data dienkripsi dan dilindungi dengan firewall serta sistem deteksi intrusi canggih, mencegah kebocoran atau eksploitasi data.
- Jaringan yang digunakan di organisasi dioptimalkan untuk performa tinggi, mendukung analitik data besar dan proses BI yang membutuhkan intensitas data tinggi, memungkinkan akses insight bisnis real-time.
- Seluruh infrastruktur TI sesuai dengan pedoman, termasuk pengamanan perangkat keras, manajemen

lingkungan data center, dan kontrol akses ke fasilitas pengolahan data.

Tantangan infrastruktur yang diidentifikasi termasuk:

- Akses tidak sah ke ruang server dan data center.
- Gangguan fisik terhadap infrastruktur.
- Fluktuasi pasokan listrik.
- Pemeliharaan dan pemantauan lingkungan data center.
- Perlindungan dari ancaman lingkungan seperti bencana alam.

6.3.2 Resiko Infrastruktur

Risiko infrastruktur TI yang dihadapi oleh otoritas pajak di Indonesia dapat dikategorikan sebagai berikut:

- Serangan Phishin. Serangan ini merupakan salah satu risiko paling umum, di mana organisasi dapat menerima komunikasi yang tampaknya sah namun bertujuan untuk mendapatkan informasi sensitif. Fenomena ini menyoroti pentingnya kesadaran keamanan dan pelatihan bagi anggota organisasi.
- Malware dan Ransomware. Risiko yang berkaitan dengan perangkat lunak berbahaya ini mencakup potensi infeksi sistem, pencurian data, dan permintaan tebusan. Risiko ini menandakan perlunya solusi keamanan siber yang efektif dan respons cepat terhadap insiden.
- Kehilangan Data. Risiko ini muncul dari kegagalan perangkat keras, kesalahan manusia, atau serangan siber, mempengaruhi integritas dan ketersediaan data.

Kehilangan data ini menggarisbawahi pentingnya strategi cadangan data dan pemulihan bencana.

- Eksploitasi Kerentanan Perangkat Lunak. Kerentanan dalam perangkat lunak yang tidak diperbarui atau dikonfigurasi dengan baik dapat menjadi pintu masuk bagi penyerang. Kerentanan ini menuntut pembaruan sistem yang teratur dan manajemen patch yang efisien.
- Ancaman Insider. Ancaman dari dalam organisasi adalah faktor risiko yang signifikan, yang dapat berupa tindakan sengaja atau tidak sengaja yang merugikan. Hal ini memerlukan kontrol akses yang ketat dan pemantauan aktivitas internal.
- Serangan DDoS. Risiko ini berkaitan dengan upaya untuk membanjiri server dengan lalu lintas yang berlebihan, mengganggu layanan. Respons terhadap risiko ini melibatkan kapasitas pemrosesan yang memadai dan solusi mitigasi serangan.
- Akses Tidak Sah. Risiko ini mencakup akses tidak sah yang diperoleh melalui celah keamanan atau kelemahan kontrol akses, menyoroti perlunya pengamanan jaringan yang efektif.

Dalam menanggapi risiko-risiko ini, otoritas pajak menerapkan serangkaian langkah-langkah:

- Pelatihan kesadaran keamanan sebagai strategi kunci dalam meningkatkan kemampuan staf untuk mengenali dan merespons ancaman siber.
- Implementasi solusi keamanan siber, sebagai bagian penting dari strategi pertahanan DJP.
- Pembaruan dan pemeliharaan sistem berkala, vital untuk menjaga keamanan infrastruktur TI.

- Prosedur manajemen risiko yang kuat, termasuk audit keamanan internal dan eksternal untuk menilai dan memperkuat pertahanan.

Pemahaman tentang risiko keamanan siber yang dihadapi oleh otoritas pajak dan langkah-langkah komprehensif yang diambil untuk mengurangi risiko harus sejalan dengan pedoman keamanan dan mencerminkan komitmen organisasi terhadap keamanan siber yang proaktif dan berlapis.

6.4 Tanggapan terhadap Insiden

6.4.1 Prosedur Tanggap Darurat

Otoritas pajak di Indonesia telah mengembangkan prosedur tanggap darurat terhadap pelanggaran data. Proses tanggap darurat ini mencakup beberapa langkah kritikal:

- Identifikasi dan penilaian, melibatkan identifikasi cepat dan penilaian terhadap lingkup pelanggaran data. Identifikasi ini mencerminkan penerapan metodologi penilaian risiko yang efektif untuk menentukan seriusnya insiden.
- Pemberitahuan dilakukan termasuk notifikasi segera kepada pihak-pihak terkait, termasuk otoritas pengatur dan pemangku kepentingan. Pendekatan ini sesuai dengan prinsip transparansi dan komunikasi dalam manajemen insiden.
- Isolasi sistem yang terpengaruh adalah langkah penting untuk mencegah penyebaran lebih lanjut dari

pelanggaran tersebut, menunjukkan penerapan kontrol keamanan yang efektif.

- Eradikasi sebagai tindakan yang diambil untuk menghilangkan ancaman menggarisbawahi kapasitas otoritas pajak di Indonesia untuk merespons dan menangani insiden dengan cepat.
- Proses pemulihan menggambarkan implementasi strategi yang efektif untuk mengembalikan sistem ke operasi normal, dengan penekanan pada integritas data.
- Investigasi forensik yang dilakukan menunjukkan penerapan pendekatan sistematis dalam menentukan penyebab pelanggaran dan mengumpulkan bukti.
- Pemeliharaan komunikasi yang jelas dan terbuka selama proses menunjukkan kesadaran DJP akan pentingnya menjaga kepercayaan dan keterlibatan pihak-pihak yang terdampak.
- Tinjauan dan perbaikan, menggarisbawahi pentingnya pembelajaran dan peningkatan berkelanjutan dari setiap insiden, melalui proses tinjauan menyeluruh dan implementasi perbaikan.
- Pemanfaatan pengalaman dari insiden untuk meningkatkan pelatihan keamanan dan kesadaran serta memperkuat protokol tanggap darurat, menyoroti pendekatan proaktif DJP terhadap peningkatan keamanan siber.

Selanjutnya, ketentuan dalam SE-45/PJ/2020 yang berkaitan dengan pengamanan data center, seperti sistem monitoring data center dan network monitoring system, menunjukkan adanya langkah-langkah proaktif untuk mendeteksi dan merespons terhadap insiden keamanan

siber. Penerapan sistem-sistem ini, bersamaan dengan kontrol akses yang ketat ke data center, mencerminkan komitmen DJP untuk melindungi infrastruktur TI dari ancaman siber. Analisis ini menyoroti bahwa prosedur tanggap darurat DJP adalah komprehensif dan sejalan dengan pedoman keamanan siber yang ditetapkan. Pentingnya prosedur tanggap darurat ini tidak hanya terletak pada respons terhadap insiden tetapi juga dalam pencegahan, deteksi, dan mitigasi insiden masa depan.

6.4.2 Manajemen Insiden

Dalam menghadapi insiden keamanan siber, otoritas pajak mengimplementasikan serangkaian langkah tanggap yang terkoordinasi dan sistematis, berlandaskan pada pedoman keamanan siber dan protokol yang telah ditetapkan. Proses manajemen insiden ini meliputi::

- Insiden segera dilaporkan ke pusat operasi keamanan organisasi, yang kemudian mengaktifkan tim tanggap darurat keamanan siber.
- Organisasi melakukan penilaian awal untuk menentukan cakupan dan dampak insiden, termasuk jenis data yang terpengaruh dan sistem yang terlibat.
- Langkah-langkah segera diambil untuk mengisolasi dan membatasi sistem yang terpengaruh untuk mencegah penyebaran lebih lanjut dari serangan tersebut.
- Otoritas perpajakan mengidentifikasi dan menghapus sumber dari serangan, seperti malware atau akses yang tidak sah, dari jaringan.

- Sistem yang terpengaruh dikembalikan ke operasi normal dengan mengimplementasikan prosedur pemulihan yang telah ditetapkan, sering kali dari cadangan data yang aman.
- Otoritas perpajakan melakukan investigasi mendalam untuk menentukan penyebab insiden dan membuat perubahan yang diperlukan untuk mencegah kejadian serupa di masa depan.
- Organisasi berkomunikasi secara proaktif dengan semua pihak terdampak, termasuk staf, wajib pajak, dan pihak berwenang, untuk memberi tahu tentang insiden dan langkah-langkah yang diambil.
- Insiden dan tanggapan dilaporkan kepada otoritas yang relevan sesuai dengan hukum dan regulasi yang berlaku.
- Berdasarkan hasil analisis, organisasi memperbarui kebijakan dan prosedur keamanan, dan jika perlu, mengimplementasikan teknologi keamanan yang lebih baru untuk memperkuat pertahanan.
- Setelah insiden ditangani, organisasi melakukan evaluasi pasca-insiden untuk mengambil pelajaran dan memperbaiki proses tanggap darurat.

Langkah-langkah ini merupakan bagian dari protokol keamanan siber organisasi yang berlapis dan dinamis, yang senantiasa diperbaharui untuk mengikuti praktik terbaik dan mematuhi pedoman yang ditetapkan dalam SE-45/PJ/2020.

Prosedur manajemen insiden pada otoritas pajak di Indonesia menunjukkan suatu proses yang matang dan terorganisir dengan baik. Protokol ini sesuai dengan

pedoman keamanan siber yang diuraikan dalam SE-45/PJ/2020, menunjukkan bahwa organisasi tidak hanya memiliki protokol yang jelas tetapi juga efektif dalam menangani insiden keamanan siber. Proses ini tidak hanya menangani dampak jangka pendek dari insiden tetapi juga berfokus pada perbaikan dan pencegahan jangka panjang, mengindikasikan pendekatan holistik dan berkelanjutan dalam menghadapi ancaman siber.

6.4.3 Efektivitas Respon Keamanan

Dalam keamanan siber, evaluasi efektivitas prosedur respons keamanan yang dilaksanakan oleh otoritas pajak di Indonesia merupakan aspek kritis dalam strategi keseluruhan manajemen insiden. Berdasarkan SE-45/PJ/2020 dan praktik keamanan siber terbaik, prosedur respons keamanan organisasi telah dirancang untuk mengatasi berbagai insiden dengan cara cepat dan efisien.

Otoritas pajak di Indonesia menunjukkan tingkat keyakinan yang tinggi terhadap efektivitas prosedur respons keamanan dalam menangani insiden keamanan siber. Proses ini telah dirancang dan diterapkan berdasarkan pedoman SE-45/PJ/2020 serta praktik terbaik dalam keamanan siber. Efektivitas respons keamanan yang diimplementasikan oleh otoritas pajak adalah sebagai berikut:

- Organisasi mengevaluasi dan menguji prosedur melalui simulasi insiden dan latihan tanggap darurat. Langkah ini menunjukkan pendekatan proaktif dalam mempersiapkan dan memastikan kesiapan tim dalam menanggapi insiden dengan cepat dan efisien.
- Proses yang telah dirancang untuk mengidentifikasi, mengisolasi, dan mengatasi insiden keamanan secara

efisien menunjukkan pemahaman mendalam tentang dinamika ancaman siber dan pentingnya respons cepat.

- Proses review menyeluruh yang dijalankan untuk mengidentifikasi penyebab dan mengimplementasikan perbaikan, mencerminkan peningkatan berkelanjutan.
- Pendokumentasian insiden dan tanggapan memungkinkan organisasi untuk secara sistematis belajar dari setiap kejadian dan melakukan penyesuaian yang diperlukan pada prosedur.
- Keterlibatan otoritas pajak dalam berbagi pengetahuan dengan entitas pemerintah lain dan mitra industri menunjukkan komitmen terhadap peningkatan strategi keamanan siber yang berkelanjutan.

Otoritas pajak di Indonesia menunjukkan sikap proaktif terhadap manajemen insiden keamanan siber. Meskipun diakui bahwa tidak ada sistem yang sepenuhnya kebal terhadap risiko keamanan siber, prosedur respons keamanan yang ada memberikan perlindungan yang kuat dan merupakan bagian integral dari strategi keamanan siber. Hal ini menunjukkan keseimbangan antara teknologi, prosedur, dan faktor manusia dalam menciptakan pertahanan keamanan siber yang efektif.

6.5 Pengujian Keamanan

6.5.1 Pengujian Penetrasi

Pengujian penetrasi pada sistem BDA dan BI merupakan komponen kunci dalam strategi manajemen risiko dan keamanan siber. Berdasarkan pedoman SE-45/PJ/2020 dan Lampiran I SE DJP Nomor SE-36/PJ/2017, menyajikan gambaran tentang frekuensi pengujian penetrasi dan temuan utamanya:

- Pengujian penetrasi dilakukan dengan frekuensi yang tergantung pada perubahan lingkungan ancaman siber dan dinamika infrastruktur TI. Pendekatan ini mencerminkan adaptasi terhadap ancaman siber yang terus berkembang dan kebutuhan untuk respons keamanan yang dinamis.
- Hasil pengujian umumnya meliputi:
  - Kerentanan perangkat lunak, termasuk masalah konfigurasi dan kebutuhan pembaruan atau patch, yang menunjukkan pentingnya pemeliharaan software yang berkelanjutan.
  - Kontrol akses, menyoroti kebutuhan penyempurnaan proses autentikasi dan otorisasi untuk mencegah akses tidak sah.
  - Kerentanan jaringan, yang menggarisbawahi perlunya menguatkan arsitektur jaringan untuk melawan upaya penyerangan.
  - Penanganan dan perlindungan data sensitif, terutama dalam aspek penyimpanan dan transmisi, menekankan pada kebutuhan perlindungan data yang ketat.
  - Rekomendasi untuk peningkatan dalam kebijakan keamanan internal dan prosedur tanggap darurat.

- Setiap temuan dari pengujian penetrasi dievaluasi dan ditindaklanjuti dengan rencana perbaikan yang terperinci, yang kemudian diimplementasikan untuk menguatkan keamanan sistem.

Berdasarkan SE-45/PJ/2020, khususnya terkait pengamanan data center dan ruang server, prosedur pengujian keamanan mencakup pemeriksaan dan pengujian berkala pada seluruh perangkat dan fasilitas pengolahan data, serta pelatihan personel yang memadai. Hal ini menunjukkan kesadaran otoritas pajak di Indonesia akan pentingnya pemeliharaan infrastruktur TI dan komitmen terhadap pengendalian operasional dan layanan yang efektif.

Otoritas pajak di Indonesia telah mengadopsi pendekatan komprehensif dalam pengujian keamanan siber, dengan fokus pada identifikasi dan mitigasi kerentanan secara proaktif. Meskipun pedoman SE-45/PJ/2020 memberikan kerangka kerja yang luas, masih ada kebutuhan aturan tambahan yang lebih spesifik dalam konteks pengujian keamanan siber.

6.5.2 Audit Keamanan Sistem

Dalam proses audit keamanan sistem BDA dan BI komponen penting adalah memastikan keselarasan dengan kebijakan dan standar keamanan yang berlaku. Audit ini, mencakup langkah-langkah:

- Penilaian risiko yang melibatkan penilaian komprehensif untuk mengidentifikasi aset kritis, potensi kerentanan, dan ancaman terhadap sistem BDA

dan BI. Pendekatan ini mencerminkan praktik terbaik dalam manajemen risiko keamanan informasi.

- Evaluasi kontrol keamanan, baik administratif, fisik, maupun teknis. Proses ini dilakukan untuk memastikan implementasi dan operasi kontrol keamanan yang benar.
- Pemeriksaan konfigurasi dan pengelolaan patch, untuk memastikan bahwa sistem secara konsisten diperbarui dengan patch keamanan terkini, mengurangi risiko eksploitasi kerentanan yang dikenal.
- Uji penetrasi dan pemindaian kerentanan melalui simulasi serangan dilakukan untuk mengungkap kelemahan dalam sistem dan mengidentifikasi kerentanan yang belum terdeteksi, mendorong peningkatan keamanan proaktif.
- Review kebijakan dan prosedur, untuk memastikan kecukupan, penerapan yang tepat, dan kepatuhan terhadap kebijakan dan prosedur yang berkaitan dengan BDA dan BI.

Otoritas pajak di Indonesia menerapkan prosedur audit keamanan yang komprehensif dan menyeluruh, meliputi berbagai aspek keamanan TI. Hal ini mencerminkan kepatuhan terhadap standar keamanan siber dan menunjukkan keseriusan dalam menjaga integritas sistem BDA dan BI. Proses audit ini tidak hanya mencakup penilaian teknis tetapi juga mempertimbangkan faktor manusia dan prosedural, yang merupakan elemen penting dalam menciptakan pertahanan keamanan siber yang efektif. Selanjutnya, temuan dari audit ini memberikan wawasan penting untuk perbaikan berkelanjutan dalam praktik keamanan siber DJP, menyoroti pentingnya

peninjauan berkala dan adaptasi dengan ancaman siber yang terus berkembang.

6.5.3 Validasi Kontrol Keamanan

Proses validasi kontrol keamanan DJP mengikuti serangkaian protokol yang sistematis dan terstruktur. Proses dan efektivitas validasi kontrol keamanan meliputi:

- Audit Internal, yang melibatkan pemeriksaan internal yang rutin oleh tim keamanan TI, fokus pada penilaian dan verifikasi efektivitas kontrol keamanan yang ada. Kegiatan ini merupakan praktik inti untuk memastikan kepatuhan terhadap standar keamanan yang berlaku.
- Penilaian risiko yang berkesinambungan memungkinkan organisasi untuk mengidentifikasi kerentanan dan ancaman potensial, memberikan dasar untuk penyesuaian dan perbaikan kontrol keamanan.
- Uji penetrasi, dilakukan sebagai instrumen penting untuk mengevaluasi ketahanan sistem terhadap serangan siber, mengungkapkan kelemahan yang mungkin tidak terdeteksi melalui metode lainnya.
- Sistem pemantauan keamanan canggih digunakan untuk deteksi dini aktivitas mencurigakan atau pelanggaran keamanan, vital untuk respons cepat.
- Setelah audit, umpan balik dikumpulkan dan tindakan diterapkan dengan cepat untuk meningkatkan kontrol keamanan.

Dalam praktik, proses validasi kontrol keamanan dapat dikategorikan efektif dalam menjaga integritas sistem BDA dan BI. Namun, dalam menghadapi ancaman siber yang terus berkembang dan perubahan teknologi, DJP mengakui perlunya perbaikan dan adaptasi berkelanjutan. Pendekatan ini tidak hanya mengevaluasi keefektifan kontrol keamanan saat ini tetapi juga menekankan pentingnya kerja sama antar unit dan pelatihan berkelanjutan, memastikan bahwa semua personel siap menghadapi tantangan keamanan siber. Pendekatan ini penting dalam memastikan bahwa sistem keamanan tidak hanya memadai untuk kebutuhan saat ini tetapi juga dapat menyesuaikan dengan kondisi masa depan.

6.6 Pengelolaan Akses dan Kontrol

6.6.1 Kontrol Akses

Dalam konteks keamanan siber, Direktorat Jenderal Pajak (DJP) menerapkan sistem kontrol akses yang terstruktur dan berlapis untuk sistem Big Data Analytics (BDA) dan Business Intelligence (BI), sesuai dengan pedoman Lampiran I SE DJP Nomor SE-36/PJ/2017 dan SE-45/PJ/2020. Analisis kualitatif berikut ini menguraikan sistem kontrol akses dan efektivitasnya:

- Kontrol Akses Berbasis Peran (RBAC): Penerapan RBAC memungkinkan hak akses yang spesifik berdasarkan peran atau jabatan pegawai. Pendekatan ini mencerminkan praktik manajemen akses yang efisien dan terstruktur, yang penting dalam membatasi akses ke data sesuai kebutuhan tugas.

- Autentikasi Kuat: Sistem autentikasi yang melibatkan username unik dan password untuk setiap pegawai menjamin bahwa akses dapat ditelusuri dan dijamin keamanannya. Ini menunjukkan pentingnya mekanisme autentikasi yang kuat dalam kontrol akses.
- Pengelolaan Identitas dan Akses: Penggunaan solusi pengelolaan identitas untuk mengelola siklus hidup akun pengguna menunjukkan pendekatan holistik dalam manajemen akses, dari pembuatan hingga penghapusan hak akses.
- Audit dan Pemantauan Akses: Pemantauan dan pencatatan aktivitas pengguna mendukung kebijakan audit keamanan yang efektif, memungkinkan DJP untuk melakukan review dan investigasi jika terjadi aktivitas mencurigakan.
- Pengendalian Akses Fisik: Kontrol akses fisik ke data center menunjukkan pengakuan akan pentingnya keamanan fisik bersamaan dengan keamanan siber, yang merupakan aspek penting dalam menjaga keamanan data.

Berdasarkan dokumen SE-45/PJ/2020, DJP memiliki prosedur yang jelas dan ketat terkait pengelolaan akses ke infrastruktur data center, menunjukkan penerapan praktik keamanan siber yang efektif dan komprehensif. Proses ini tidak hanya memastikan perlindungan terhadap akses tidak sah tetapi juga menggambarkan komitmen terhadap keamanan data secara menyeluruh.

Dokumen Lampiran I SE DJP Nomor SE-36/PJ/2017 menggarisbawahi berbagai tingkat pengelolaan akses dan kontrol, dari standar keamanan yang ketat hingga standar keamanan yang lebih rendah. Ini menunjukkan adanya

kerangka kerja yang beragam untuk mengelola hak akses, yang mencerminkan fleksibilitas dan kebutuhan adaptasi terhadap berbagai skenario keamanan.

Analisis ini menyoroti bahwa DJP mengadopsi pendekatan yang matang dan terstruktur dalam kontrol akses untuk sistem BDA dan BI. Sistem kontrol akses ini bukan hanya sekadar memenuhi persyaratan regulasi dan kebijakan internal tetapi juga merupakan bagian penting dari upaya berkelanjutan untuk menjaga integritas dan keamanan data. Pendekatan multi-lapis ini sangat penting dalam menghadapi ancaman siber yang terus berkembang dan mendukung strategi.

6.6.2 Monitoring Akses

Prosedur pemantauan akses yang komprehensif untuk menjaga data sensitif, dijalankan otoritas pajak di Indonesia berdasarkan SE-45/PJ/2020 dan Lampiran I SE DJP Nomor SE-36/PJ/2017. Berikut adalah mekanisme pemantauan akses dan deteksi akses tidak sah:

- Pencatatan komprehensif setiap akses ke data sensitif memungkinkan audit dan pengawasan berkelanjutan, memberikan data penting mengenai siapa yang mengakses, kapan, dan data apa yang diakses.
- Penerapan sistem manajemen identitas untuk mengatur hak akses menunjukkan komitmen organisasi terhadap pengelolaan akses yang ketat, memastikan bahwa hanya pengguna yang berwenang yang dapat mengakses informasi sensitif.

- Sistem pemantauan aktivitas akses secara real-time adalah kunci dalam deteksi dini akses tidak sah, menunjukkan pendekatan yang responsif dan proaktif dalam pengelolaan keamanan informasi.
- Implementasi solusi untuk mendeteksi pola akses tidak biasa atau mencurigakan menggarisbawahi pemahaman DJP tentang pentingnya teknologi canggih dalam mengidentifikasi ancaman internal dan eksternal.
- Konfigurasi sistem untuk memicu alarm dan pemberitahuan terhadap aktivitas mencurigakan menunjukkan efektivitas mekanisme respons keamanan dalam mengidentifikasi potensi pelanggaran.
- Kegiatan audit dan review rutin terhadap log akses mengkonfirmasi adanya evaluasi berkelanjutan terhadap aktivitas akses, yang merupakan bagian penting dari siklus perbaikan berkelanjutan dalam pengelolaan keamanan.
- Adanya protokol tanggap darurat yang jelas untuk situasi akses tidak sah menunjukkan kesiapan DJP dalam menghadapi insiden keamanan, mencakup investigasi dan tindakan pencegahan atau korektif yang diperlukan.

DJP telah mengembangkan sistem pemantauan akses yang efektif dan menyeluruh, dirancang untuk melindungi data sensitif dan mendeteksi akses tidak sah. Mekanisme ini mencerminkan kepatuhan terhadap standar keamanan yang ditetapkan, sekaligus menyoroti pentingnya teknologi, prosedur, dan pendidikan dalam menciptakan lingkungan keamanan informasi yang aman. Dalam praktik, pendekatan ini menunjukkan efektivitas dalam menjaga integritas dan privasi data, memperkuat pertahanan terhadap ancaman

siber, dan mendukung kepatuhan terhadap regulasi yang relevan. Namun, mengingat evolusi ancaman siber yang terus-menerus, DJP perlu terus mengadaptasi dan memperbarui praktik pemantauan dan pengelolaan akses ini untuk mengatasi tantangan keamanan yang muncul.

6.6.3 Pencegahan Akses Tidak Sah

Otoritas pajak di Indonesia mengadopsi serangkaian langkah keamanan komprehensif untuk mencegah akses tidak sah ke sistem BDA dan BI, sejalan dengan pedoman SE-45/PJ/2020 dan Lampiran I SE DJP Nomor SE-36/PJ/2017. Pencegahan akses tidak sah melalui langkah-langkah:

- Implementasi MFA menggarisbawahi komitmen organisasi terhadap verifikasi identitas pengguna secara ketat sebelum memberikan akses. Penggunaan faktor-faktor seperti pengetahuan, kepemilikan, dan biometrik meningkatkan keamanan autentikasi.
- Enkripsi data yang disimpan dan ditransmisikan memastikan kerahasiaan dan integritas data, kunci dalam melindungi informasi sensitif dari intersepsi dan manipulasi.
- Pemisahan jaringan khusus untuk BDA dan BI serta penggunaan firewall mencerminkan pendekatan yang berhati-hati dalam mengontrol akses jaringan dan mengurangi risiko serangan siber.
- Pengelolaan hak akses yang dikendalikan berdasarkan prinsip 'need-to-know' dan berbasis peran menunjukkan pendekatan yang terstruktur dalam pemberian dan pemantauan akses.

- Pemeliharaan sistem yang berkesinambungan melalui pembaruan dan patching menandakan kesadaran organisasi akan pentingnya mengatasi kerentanan yang dikenal untuk mencegah eksploitasi.
- Penerapan sistem pemantauan dan analisis perilaku untuk deteksi aktivitas mencurigakan menggarisbawahi upaya organisasi dalam mengidentifikasi akses tidak sah secara dini.
- Protokol tanggap insiden dan rencana pemulihan bencana mencerminkan kesiapan organisasi dalam menghadapi insiden akses tidak sah, dengan langkah-langkah respons yang terperinci.

Dalam praktik, pendekatan efektif dalam mencegah akses tidak sah ke sistem BDA dan BI. Organisasi menunjukkan penggabungan strategis antara langkah-langkah teknis, prosedural, dan manusia dalam sistem keamanan. Penerapan langkah-langkah ini menunjukkan praktik keamanan yang matang dan disiplin, dengan fokus pada pencegahan, deteksi, dan respons terhadap akses tidak sah. Analisis ini menggarisbawahi bahwa, meskipun langkah-langkah yang diambil cukup komprehensif, tantangan keamanan siber yang terus berkembang memerlukan evaluasi dan adaptasi berkelanjutan terhadap strategi keamanan. Hal ini termasuk mempertimbangkan teknologi baru, tren ancaman, dan peningkatan pelatihan untuk staf, untuk memastikan bahwa sistem keamanan organisasi tetap efektif dan relevan.

6.7 Analisis Kritis

Strategi keamanan siber DJP mencakup aspek-aspek kritikal seperti kontrol akses, pemantauan akses, pengujian keamanan, dan manajemen insiden. Ini mencerminkan praktik industri terbaik dengan pendekatan berlapis dan kesesuaian dengan standar internasional, seperti ISO/IEC 27001. Respons dinamis terhadap ancaman yang berkembang dan fokus pada adaptasi berkelanjutan menunjukkan relevansi tinggi strategi ini terhadap tantangan keamanan siber modern.

Area untuk Peningkatan dalam Strategi Keamanan Siber DJP

1. Enkripsi Data

Meskipun strategi keamanan otoritas pajak di Indonesia mencakup enkripsi sebagai elemen kunci, detail mengenai standar enkripsi yang diterapkan dan prosedur manajemen kunci belum sepenuhnya transparan. Untuk meningkatkan keamanan dan kepercayaan pemangku kepentingan, penting untuk memperjelas penggunaan standar enkripsi yang spesifik dan praktik manajemen kunci yang digunakan. Hal ini termasuk menjelaskan protokol untuk pembuatan, distribusi, penyimpanan, dan pemusnahan kunci enkripsi.

2. Ancaman Insider

Strategi organisasi perlu memberikan perhatian lebih pada mitigasi risiko yang berasal dari ancaman insider. Hal ini dapat dicapai melalui penerapan analisis perilaku yang lebih komprehensif, memperkuat prinsip-prinsip akses

berdasarkan kebutuhan untuk mengetahui dan pemisahan tugas yang lebih ketat. Mendeteksi dan merespons perilaku yang mencurigakan dari dalam organisasi merupakan kunci untuk mencegah kebocoran data dan insiden keamanan lainnya.

3. Teknologi Baru

Informasi saat ini belum menyoroti bagaimana otoritas pajak berencana untuk memanfaatkan teknologi canggih seperti kecerdasan buatan (AI) dan pembelajaran mesin (ML) dalam strategi keamanan sibernya. Integrasi teknologi ini dapat signifikan meningkatkan kapasitas deteksi ancaman secara real-time dan memfasilitasi respons otomatis terhadap insiden keamanan. Pengembangan dan penerapan model AI dan ML yang dapat belajar dari pola ancaman sebelumnya sangat direkomendasikan.

4. Pelatihan dan Kesadaran Keamanan Siber

Detail tentang implementasi program pelatihan dan peningkatan kesadaran keamanan siber dapat ditingkatkan efektivitas inisiatif ini dengan pembaruan pelatihan untuk mencakup ancaman terkini dan teknik penipuan yang sering digunakan oleh penyerang. Program ini juga harus menyediakan simulasi serangan siber untuk menguji dan memperkuat kesiapsiagaan organisasi dalam menghadapi insiden nyata.

5. Keterbukaan dan Transparansi

Organisasi memiliki peluang untuk meningkatkan keterbukaan terkait insiden keamanan yang terjadi. Membagikan informasi tentang insiden, termasuk jenis ancaman, respons yang dilakukan, dan pelajaran yang dipetik, tidak hanya memperkuat kepercayaan stakeholder tetapi juga berkontribusi pada kesadaran dan kesiapsiagaan komunitas yang lebih luas terhadap ancaman keamanan siber. Penting untuk kemudian mempertimbangkan pembuatan laporan insiden terbuka atau studi kasus yang dapat diakses oleh publik sebagai bagian dari komitmen mereka terhadap transparansi dan pembelajaran berkelanjutan.

Melalui peningkatan di area-area ini, organisasi dapat memperkuat framework keamanan siber dan lebih efektif dalam melindungi aset dan data penting dari ancaman siber yang terus berkembang.

BAB VII

Efektivitas Manajemen Risiko Cyber Security

7.1 Identifikasi Risiko Proaktif

Otoritas pajak penting untuk menetapkan pedoman pengamanan perangkat dan fasilitas pengolahan data dan informasi. Pedoman atau kebijakan termasuk pengaturan untuk mengamankan perangkat komputer milik organisasi di seluruh unit kerja serta pengamanan fasilitas pengolahan data dan informasi yang sensitif. Pedoman ini mencakup langkah-langkah seperti kontrol akses fisik dan digital ke perangkat dan data, enkripsi data, serta implementasi firewall dan sistem keamanan lainnya untuk melindungi terhadap ancaman siber. Tujuan utamanya adalah untuk memastikan bahwa hanya personel yang berwenang yang dapat mengakses informasi sensitif dan bahwa informasi tersebut dilindungi dari ancaman eksternal maupun internal.

7.1.1 Evaluasi Sistem

Dalam evaluasi sistem berkelanjutan, DJP mengadopsi serangkaian proses dan metodologi yang komprehensif. Identifikasi risiko secara proaktif dimulai dengan evaluasi sistem keamanan secara berkala, dilengkapi dengan penggunaan alat penilaian kerentanan untuk mengidentifikasi dan menilai kerentanan dalam sistem TI.

Alat penilaian kerentanan yang digunakan memungkinkan DJP untuk mengidentifikasi risiko keamanan yang belum diketahui dan mengatasinya sebelum dapat dimanfaatkan oleh penyerang.

Setelah kerentanan teridentifikasi, organisasi menerapkan kontrol berdasarkan standar SNI ISO/IEC 27001:2013 dan kebijakan internal. Standar ini menyediakan kerangka kerja untuk mengelola keamanan informasi yang mencakup aspek teknis, organisasi, dan fisik.

Selain itu, baseline konfigurasi keamanan diterapkan untuk mengurangi risiko dan mencegah instalasi perangkat lunak yang tidak sah, sebagai bagian dari upaya mitigasi risiko. Hal ini termasuk pencegahan terhadap instalasi perangkat lunak yang tidak sah dan memastikan bahwa semua sistem dikonfigurasi dengan cara yang meminimalkan risiko.

Berdasarkan standar ISO/IEC 27001, DJP mengimplementasikan proses yang meliputi penilaian risiko, evaluasi kerentanan, pengelolaan risiko, mitigasi risiko, serta review dan peningkatan berkelanjutan. Pendekatan ini memastikan bahwa sistem keamanan informasi DJP resilien dan responsif terhadap ancaman. Di samping itu, dalam penerapan ISO/IEC 27005, DJP mengadopsi pendekatan berbasis risiko yang mencakup identifikasi konteks, aset dan risiko, analisis dan evaluasi risiko, penanganan risiko, komunikasi dan konsultasi risiko, serta monitoring dan review.

DJP juga menerapkan kerangka kerja COBIT 4.1, fokus pada pengelolaan dan kontrol TI. Hal ini melibatkan penilaian risiko, evaluasi kontrol, pengelolaan kerentanan,

aksi mitigasi, serta monitoring dan review berkelanjutan. Penerapan siklus PDCA mendukung peningkatan berkelanjutan dalam pengelolaan risiko dan kontrol keamanan TI. Dengan mengadopsi ITIL V2, DJP mengimplementasikan proses yang terstruktur untuk manajemen layanan TI, termasuk manajemen insiden, manajemen masalah, manajemen perubahan, manajemen rilis, dan manajemen tingkat layanan, semuanya dengan fokus pada peningkatan berkelanjutan dalam manajemen keamanan layanan TI. Integrasi proses-proses ini memastikan bahwa kerentanan sistem teridentifikasi dan dikelola secara proaktif, dengan mempertahankan ketahanan sistem informasi dalam menghadapi ancaman keamanan siber yang dinamis.

Dengan mengintegrasikan proses manajemen layanan TI yang terstruktur, seperti manajemen insiden, masalah, perubahan, rilis, dan tingkat layanan, DJP memastikan bahwa kerentanan sistem dapat dikelola secara efektif. Fokus pada peningkatan berkelanjutan dalam manajemen keamanan layanan TI menunjukkan kesadaran organisasi akan pentingnya menjaga ketahanan sistem informasi.

7.1.2 Intelligence Threat

Intelligence Threat, merupakan suatu pendekatan yang digunakan untuk mengidentifikasi, menganalisis, dan mengatasi ancaman keamanan yang potensial terhadap suatu organisasi atau infrastruktur. Pendekatan ini bersifat proaktif, berfokus pada pemahaman tentang ancaman-ancaman yang bisa berdampak pada organisasi sebelum ancaman tersebut menjadi nyata dan menimbulkan

kerusakan. Threat Intelligence melibatkan pengumpulan dan analisis informasi tentang aktor ancaman, motivasi mereka, dan metode serangan yang digunakan. Tujuannya adalah untuk membuat organisasi lebih resilien terhadap serangan dengan menyediakan wawasan yang bisa digunakan untuk memperkuat pertahanan keamanan.

Komponen utama dari Intelligence Threat meliputi:

- Indicators of Compromise – IoCs. Informasi yang dapat menunjukkan potensi kompromi atau serangan terhadap sistem TI, seperti alamat IP jahat, URL, hash file, dan tanda-tanda lain dari aktivitas mencurigakan.
- Tactics, Techniques, and Procedures – TTPs. Mendeskripsikan cara kerja aktor ancaman, termasuk metode yang digunakan untuk menyerang dan menyusup ke dalam sistem.
- Informasi tentang aktor ancaman, termasuk motivasi, sasaran, dan kapabilitas, dapat membantu organisasi mengerti mengapa organisasi menjadi target dan bagaimana ancaman tersebut dapat mempengaruhi.
- Intelligence Sharing. Berbagi informasi tentang ancaman dengan organisasi lain dan komunitas keamanan siber membantu meningkatkan kesadaran dan persiapan terhadap ancaman baru.

Implementasi Intelligence Threat melibatkan penggunaan teknologi untuk mengumpulkan data dari berbagai sumber, termasuk feed intelijen ancaman, log sistem, dan sumber terbuka. Analisis data ini membantu dalam mengidentifikasi pola atau aktivitas mencurigakan yang menunjukkan adanya ancaman.

Dalam upaya proaktif menghadapi ancaman siber, DJP mengimplementasikan serangkaian strategi berdasarkan standar internasional seperti ISO/IEC 27001, ISO/IEC 27002, dan ISO/IEC 27005. Standar ISO/IEC 27001 berperan penting dalam proses identifikasi ancaman keamanan informasi, analisis risiko, dan pengambilan tindakan pencegahan. DJP memanfaatkan standar ini untuk mengembangkan strategi keamanan siber yang menyeluruh, yang mencakup pengumpulan, analisis, dan pemanfaatan intelijen ancaman.

Mengacu pada ISO/IEC 27002, DJP menerapkan praktik manajemen keamanan informasi. Manajemen keamanan informasi ini melibatkan penggunaan alat otomatis, sistem deteksi intrusi (IDS) dan sistem manajemen informasi keamanan, serta berpartisipasi dalam jejaring antarorganisasi untuk berbagi dan menerima intelijen ancaman. Pendekatan ini memastikan bahwa DJP dapat secara proaktif menghadapi potensi serangan siber dengan memperbarui kebijakan keamanan, mengembangkan program pelatihan yang disesuaikan, dan mengimplementasikan kontrol teknis yang efektif.

Selanjutnya, dalam penerapan ISO/IEC 27005, DJP mengambil langkah-langkah sistematis dalam manajemen risiko keamanan informasi. Proses ini mencakup penggunaan alat pemantauan keamanan siber untuk mengumpulkan data, menerima laporan keamanan dari berbagai sumber, serta melakukan pemindaian kerentanan secara teratur. Analisis intelijen ancaman dilakukan melalui evaluasi risiko, korelasi data, dan penilaian dampak bisnis, yang semuanya membantu dalam menentukan prioritas tindakan mitigasi. Organisasi memprioritaskan

pengembangan strategi mitigasi risiko berdasarkan hasil analisis intelijen ancaman, termasuk rencana kontingensi dan respons insiden, serta komunikasi risiko ke seluruh organisasi. Strategi ini untuk memastikan bahwa kesiapan organisasi menghadapi insiden keamanan siber yang mungkin terjadi, dan merespons dinamika ancaman siber.

7.2 Analisis Prediktif

Analisis Prediktif adalah proses menggunakan data, algoritma statistik, dan teknik pembelajaran mesin untuk mengidentifikasi kemungkinan hasil di masa depan berdasarkan data historis. Tujuannya adalah untuk memberikan perkiraan terbaik tentang apa yang akan terjadi di masa depan, bukan hanya untuk mengetahui apa yang telah terjadi atau apa yang sedang terjadi. DJP mengembangkan model prediktif perilaku penyerang, analisis prediktif dapat digunakan untuk memprediksi dan mencegah serangan siber sebelum terjadi. Dalam keamanan siber, analisis prediktif digunakan untuk:

- Memodelkan perilaku penyerang, dengan memahami bagaimana penyerang beroperasi dan prediksi serangan yang akan dilakukan berdasarkan pola historis.
- Deteksi ancaman proaktif, dengan mengidentifikasi tanda-tanda awal serangan yang sedang direncanakan atau akan dilancarkan.
- Manajemen kerentanan, diterapkan dengan memperkirakan kerentanan mana yang paling mungkin dieksploitasi oleh penyerang dan memprioritaskan perbaikan berdasarkan risiko.

- Adaptasi dengan ancaman yang berkembang, dimana model prediktif dapat secara dinamis disesuaikan untuk merespon perubahan taktik, teknik, dan prosedur penyerang.

Analisis prediktif merupakan pendekatan yang lebih proaktif dalam keamanan siber, memungkinkan organisasi untuk tidak hanya bereaksi terhadap ancaman yang sudah terjadi tetapi juga untuk memprediksi dan mencegah ancaman sebelum menyebabkan kerusakan. Analisis prediktif menjadi sangat penting dalam lingkungan yang dinamis dan cepat berubah seperti keamanan siber, di mana penyerang terus-menerus mengembangkan metode baru untuk mengeksploitasi sistem dan infrastruktur TI.

7.2.1 Model Prediksi Perilaku Penyerang

Dalam upaya DJP untuk mengembangkan model prediktif perilaku penyerang, integrasi BDA dan BI memainkan peran krusial. Proses implementasi melibatkan beberapa tahapan teknis kunci yang bertujuan untuk memahami, mencegah, dan merespons ancaman siber secara proaktif. Berikut adalah tahapan tersebut:

1) Pengumpulan Data Komprehensif
    - Log Server. Mengumpulkan data dari server yang mencatat semua request dan response, termasuk waktu akses, sumber request, dan jenis data yang diakses.
    - Firewall. Mencatat percobaan akses masuk dan keluar yang diblokir atau diizinkan oleh firewall, memberikan insight tentang upaya akses yang tidak sah.

- Intrusion Detection System – IDS. Mengumpulkan peringatan dan log tentang aktivitas mencurigakan yang mungkin menunjukkan upaya penetrasi atau serangan.
- Sumber Eksternal, termasuk laporan intelijen ancaman dari organisasi keamanan siber, yang menyediakan data tentang ancaman terbaru, indikator kompromi, dan taktik, teknik, serta prosedur (TTPs) yang digunakan oleh penyerang.

2) Integrasi ke dalam Data Lake atau Platform Manajemen Data
   - Data Lake, adalah sebuah sistem penyimpanan yang memungkinkan pengumpulan data dalam format aslinya, termasuk data terstruktur dan tidak terstruktur. Ini memfasilitasi analisis terpadu dari berbagai sumber data.
   - Pengolahan Data, termasuk normalisasi, pembersihan, dan transformasi data untuk mempersiapkannya untuk analisis. Proses ini memastikan bahwa data yang digunakan akurat dan konsisten.
3) Analisis Terpadu Menggunakan BDA dan BI
   - Menggunakan algoritma dan teknik pembelajaran mesin untuk menganalisis volume data yang besar dengan tujuan mengidentifikasi pola, tren, dan anomali yang mungkin menunjukkan perilaku penyerang.
   - Memanfaatkan alat BI untuk memvisualisasikan hasil analisis, memudahkan identifikasi pola kompleks, dan mendukung pengambilan keputusan berbasis data.

4) Pengembangan Model Prediksi Perilaku Penyerang
    - Menggunakan hasil analisis untuk membangun model prediktif yang dapat mengidentifikasi kemungkinan serangan berdasarkan perilaku historis dan tren saat ini.
    - Model dilatih dengan data historis dan divalidasi untuk memastikan akurasi dan keandalannya dalam memprediksi perilaku penyerang.
5) Implementasi dan Pemantauan Berkelanjutan
    - Model yang telah divalidasi diterapkan dalam operasi sehari-hari DJP untuk pemantauan dan deteksi proaktif serangan.
    - Model dan sistem pemantauan terus diperbarui dengan data baru untuk menyesuaikan dengan evolusi taktik penyerang, memastikan bahwa DJP tetap selangkah lebih maju dalam menghadapi ancaman siber.

Implementasi ini menunjukkan pendekatan yang holistik dan multi-layer dalam keamanan siber, mengintegrasikan teknologi canggih dan intelijen ancaman untuk melindungi infrastruktur TI penting DJP dari serangan siber yang semakin canggih.

Dalam komunikasi dan pelaporan, DJP menggunakan dashboard BI untuk mempresentasikan hasil dari model prediksi, memudahkan analisis dan pengambilan keputusan. Temuan dan rekomendasi disampaikan kepada tim keamanan siber dan manajemen tingkat atas, memastikan bahwa informasi penting disebarluaskan dengan efektif.

7.2.2 Deteksi Anomali dan Respons

Dalam deteksi anomali dan respons terhadap insiden keamanan siber, DJP memanfaatkan BDA dan BI untuk mengidentifikasi dan merespons aktivitas siber yang mencurigakan. Proses ini melibatkan beberapa langkah penting yang dimulai dengan pengumpulan data kontinu dari berbagai sumber, termasuk log jaringan, aplikasi, dan keamanan, serta transaksi pengguna dan aliran lalu lintas. Data yang terkumpul ini kemudian diolah dan diintegrasikan untuk menghilangkan kebisingan dan dipersiapkan untuk analisis, dengan tujuan menciptakan pandangan holistik tentang aktivitas jaringan.

Penerapan model deteksi anomali merupakan langkah kunci dalam proses ini. Model berbasis algoritme statistik, machine learning, atau AI dilatih untuk mengenali pola aktivitas normal dan, dengan demikian, mampu mengidentifikasi penyimpangan sebagai anomali. Pemantauan real-time aktivitas jaringan dan aplikasi memungkinkan perbandingan dengan model perilaku normal yang telah ditetapkan. DJP menggunakan pembelajaran berkelanjutan untuk menyesuaikan model secara dinamis, meningkatkan kemampuan deteksi dengan memperhatikan perubahan pola aktivitas normal. Proses scoring dan thresholding digunakan untuk menentukan seberapa jauh aktivitas menyimpang dari baseline normal dan menilai apakah aktivitas tersebut mencurigakan.

Setelah deteksi anomali, langkah-langkah respons diambil. Sistem mengirimkan alert ke tim keamanan siber, yang kemudian menilai prioritas dan urgensi berdasarkan potensi dampak dan risiko. Investigasi awal dilakukan untuk menentukan sifat sebenarnya dari anomali tersebut,

apakah merupakan false positive atau indikasi serangan siber yang sebenarnya. Tindakan perbaikan diambil jika ancaman dikonfirmasi, yang dapat mencakup isolasi sistem yang terinfeksi atau pemblokiran alamat IP yang mencurigakan. Analisis forensik berikutnya memungkinkan pengumpulan bukti dan pemahaman tentang metode serangan untuk mencegah insiden serupa di masa depan. Sistem deteksi anomali juga diperbarui dengan informasi dari insiden tersebut untuk meningkatkan akurasi deteksi di masa depan. Terakhir, kebijakan dan prosedur keamanan siber ditinjau dan disesuaikan berdasarkan pelajaran yang dipetik dari insiden tersebut.

7.3 Integrasi Sistem Peringatan Dini

7.3.1 Pengembangan dan Integrasi Teknologi Peringatan Dini

Direktorat Jenderal Pajak (DJP) memanfaatkan teknologi peringatan dini yang terintegrasi dalam sistem BDA dan BI untuk meningkatkan deteksi dan respons terhadap ancaman keamanan siber. Proses pengembangan dan integrasi teknologi ini melibatkan beberapa langkah strategis dan teknis yang kritis. Pertama, penentuan kebutuhan dan persyaratan sistem peringatan dini dilakukan berdasarkan analisis aset yang berharga dan skenario ancaman yang mungkin terjadi. Hal ini melibatkan penyusunan persyaratan teknis yang rinci, termasuk waktu respons yang diinginkan, jenis ancaman yang harus dideteksi, dan metode notifikasi. Kemudian, pemilihan teknologi dilakukan dengan memilih alat dan platform BDA yang dapat menganalisis data besar dengan cepat dan

efisien, serta alat BI yang mengintegrasikan data dari BDA dan menyajikan informasi keamanan dalam format yang mudah diakses.

Pembangunan atau modifikasi infrastruktur yang ada dilakukan untuk mendukung pengumpulan, pemrosesan, dan analisis data secara real-time. Sistem sensor dan pengumpulan data, diintegrasikan dengan platform BDA. Data dari berbagai sumber, termasuk endpoint security, IDS/IPS, firewall, dan sistem manajemen patch, diintegrasikan untuk memberikan pandangan komprehensif tentang keamanan jaringan. Teknologi pemrosesan stream seperti Apache Spark atau Storm digunakan untuk analisis real-time, dan model deteksi anomali dikembangkan dengan teknik machine learning dan AI. Sistem peringatan dini dikonfigurasi untuk mengirimkan peringatan melalui email, SMS, atau integrasi dengan sistem tiket ketika aktivitas mencurigakan terdeteksi. Dashboard operasional dibuat dalam alat BI untuk visualisasi real-time dari ancaman yang terdeteksi. Otomatisasi respons terhadap insiden juga diintegrasikan, memungkinkan tindakan otomatis seperti isolasi jaringan atau pemblokiran alamat IP.

Namun, implementasi teknologi peringatan dini menghadapi tantangan signifikan. Mengelola dan memproses volume data yang besar membutuhkan infrastruktur yang skalabel dan efisien. Memastikan kinerja real-time merupakan tantangan lainnya, yang memerlukan solusi pemrosesan data yang cepat. Integrasi sistem peringatan dini dengan sistem BDA dan BI yang ada harus dilakukan dengan hati-hati untuk menghindari gangguan pada operasional. Selain itu, pengembangan algoritma

untuk meminimalkan false positives adalah kunci untuk menghindari kelelahan peringatan di tim keamanan.

7.3.2 Automasi Respons ke Ancaman

Dalam rangka meningkatkan responsivitas terhadap ancaman keamanan siber, DJP mengadopsi strategi automasi respons ke ancaman yang terintegrasi dengan sistem peringatan dini. Proses ini melibatkan serangkaian langkah teknis yang dirancang untuk mengaktifkan protokol dan prosedur secara otomatis untuk mengidentifikasi dan merespons ancaman.

Pertama, pengembangan protokol respons automatis di DJP mencakup pembuatan aturan dan skenario respons. Aturan ini didasarkan pada kebijakan keamanan yang ada dan dirancang untuk mendefinisikan tindakan yang harus diambil ketika ancaman tertentu terdeteksi. Skenario ancaman yang berbeda diidentifikasi, dan alur kerja untuk respons otomatis dirancang untuk masing-masing skenario. Implementasi sistem orkestrasi keamanan siber yang memungkinkan DJP untuk mengintegrasikan berbagai solusi keamanan dan mengotomatisasi tugas-tugas tertentu. Integrasi ini juga meliputi penyatuan alat orkestrasi dengan infrastruktur TI yang ada, termasuk solusi identifikasi dan akses manajemen, sistem deteksi intrusi, firewall, dan sistem pemantauan jaringan.

Protokol khusus diaktifkan dalam situasi tertentu, termasuk protokol isolasi yang mengisolasi sistem atau jaringan yang terinfeksi, penutupan otomatis port dan aplikasi yang mencurigakan, dan pengelolaan patch otomatis untuk mengurangi kerentanan. Pengujian dan

validasi sistem ini merupakan langkah kritis untuk memastikan efektivitasnya. Simulasi ancaman digunakan untuk menguji sistem, dan penilaian keandalan dilakukan untuk mengevaluasi kemampuan sistem dalam merespons ancaman nyata secara otomatis. Pelatihan dan latihan reguler dengan tim keamanan siber memastikan bahwa mereka memahami cara kerja sistem dan bagaimana berinteraksi dengan sistem tersebut.

Pemantauan dan peninjauan sistem automasi respons berkelanjutan adalah kunci untuk memastikan operasional yang efektif. Kinerja sistem dipantau secara rutin, dan aturan serta respons diupdate berdasarkan hasil pemantauan serta umpan balik dari insiden keamanan yang terjadi. Proses ini bertujuan untuk meningkatkan efektivitas sistem dan mengurangi insiden false positives.

7.3.3 Peningkatan Kapasitas Analisis dan Respons

Dalam upaya meningkatkan kapasitas analisis dan respons terhadap ancaman keamanan siber, DJP telah mengambil inisiatif untuk mengintegrasikan sistem peringatan dini dengan BDA dan BI. Integrasi ini memungkinkan DJP untuk memanfaatkan volume data besar dan analitik canggih, meningkatkan kemampuan mereka untuk memprediksi, mendeteksi, dan merespons insiden keamanan secara lebih efektif.

Dalam konteks peningkatan kapasitas analisis, langkah pertama yang diambil adalah pengayaan data. Proses ini melibatkan integrasi data dari berbagai sumber internal dan eksternal, memberikan konteks yang lebih luas dan meningkatkan akurasi analisis. Teknik analitik tingkat

lanjut, termasuk penggunaan machine learning dan AI, diterapkan untuk mengidentifikasi pola tersembunyi yang dapat menunjukkan perilaku mencurigakan atau ancaman mendatang. Pengembangan model prediktif juga penting, memanfaatkan data historis dan tren keamanan siber untuk meramalkan jenis serangan yang mungkin terjadi di masa depan.

Meningkatkan kapasitas respons melibatkan penggunaan alat otomatisasi untuk mempercepat proses respons insiden. Hal ini memungkinkan tindakan cepat seperti isolasi otomatis dari sistem yang terinfeksi atau penutupan otomatis port yang tidak aman. Orkestrasi alat keamanan merupakan langkah penting lainnya, yang memastikan bahwa berbagai alat keamanan bekerja secara sinkron untuk merespons ancaman secara efisien.

Pengukuran efektivitas peningkatan kapasitas dilakukan melalui serangkaian metode. Metrik kinerja seperti waktu deteksi, waktu respons, dan tingkat keberhasilan mitigasi insiden ditetapkan untuk mengukur efektivitas sistem peringatan dini. Simulasi serangan dan latihan dilakukan untuk menguji dan mengukur seberapa baik sistem dapat mengidentifikasi dan merespons ancaman. Selain itu, review dan analisis insiden dilakukan secara berkala untuk menilai kontribusi sistem peringatan dini dalam deteksi dan respons serta mengidentifikasi area perbaikan.

7.4 Framework Manajemen Risiko

Di Indonesia, aktivitas hacking atau peretasan sistem menjadi perhatian utama. Undang-undang Informasi Elektronik (UU ITE) di Indonesia mengatur tentang tindakan peretasan ilegal, menetapkan bahwa akses tidak sah ke informasi atau data dapat dianggap sebagai tindak pidana.

7.4.1 Kebijakan Pengelolaan Keamanan Informasi

Otoritas pajak di Indonesia mengadopsi standar internasional ISO/IEC 27002 dan ISO/IEC 27005 untuk pengelolaan keamanan informasi. Standar ini memberikan kerangka kerja yang komprehensif untuk mengelola risiko keamanan informasi.

- ISO/IEC 27002 menetapkan kontrol keamanan informasi yang dapat digunakan untuk melindungi aset informasi dari ancaman. Kontrol ini mencakup kontrol teknis, kontrol operasional, dan kontrol manajemen.
- ISO/IEC 27005 memberikan kerangka kerja untuk penilaian risiko keamanan informasi. Kerangka kerja ini membantu organisasi untuk mengidentifikasi, menilai, dan mengendalikan risiko keamanan informasi.

Implementasi strategi mitigasi berbasis data:

1) Membangun infrastruktur yang aman dan terkendali
   Untuk membangun infrastruktur yang aman dan terkendali, organisasi melakukan hal-hal berikut:

- Jaringan dirancang dengan keamanan yang ketat. Jaringan tersebut hanya dapat diakses oleh perangkat yang telah terdaftar dan memiliki izin.
- Server dilindungi dengan keamanan yang ketat. Server tersebut dilengkapi dengan firewall, antivirus, dan sistem enkripsi.
- Perangkat penyimpanan data juga dilindungi dengan keamanan yang ketat. Perangkat tersebut ditempatkan di ruangan yang aman dan dilengkapi dengan sistem keamanan fisik.

2) Menggunakan teknologi keamanan yang memadai
Untuk menggunakan teknologi keamanan yang memadai, organisasi menggunakan teknologi keamanan berikut:

- Firewall untuk melindungi jaringan dari serangan dari luar.
- Antivirus untuk melindungi perangkat dari malware.
- Sistem enkripsi untuk melindungi data dari penyalahgunaan.

DJP telah menerapkan strategi Compliance Risk Management (CRM) dalam rangka meningkatkan kepatuhan wajib pajak. DJP mengadopsi CRM berdasarkan Surat Edaran Direktur Jenderal Pajak Nomor SE-24/PJ/2019 tentang Pedoman Manajemen Risiko Kepatuhan Pajak. Surat edaran ini menetapkan kerangka kerja untuk implementasi CRM di DJP. Strategi ini juga dapat diterapkan untuk meningkatkan kepatuhan terhadap peraturan industri, seperti General Data Protection Regulation (GDPR),

California Consumer Privacy Act (CCPA), dan Health Insurance Portability and Accountability Act (HIPAA).

Langkah awal dalam penerapan CRM adalah pemetaan risiko. DJP dapat melakukan pemetaan risiko kepatuhan terhadap peraturan industri dengan menggunakan pendekatan top-down dan bottom-up. Pemetaan risiko top-down dilakukan dengan mengidentifikasi risiko-risiko kepatuhan terhadap peraturan industri secara umum. Risiko-risiko ini dapat diidentifikasi berdasarkan faktor-faktor berikut:

- **Jenis peraturan industri yang berlaku**
- **Sifat dan karakteristik wajib pajak**
- **Sistem dan proses DJP**

Pemetaan risiko bottom-up dilakukan dengan mengidentifikasi risiko-risiko kepatuhan terhadap peraturan industri secara spesifik pada masing-masing wajib pajak. Risiko-risiko ini dapat diidentifikasi berdasarkan data dan informasi yang diperoleh dari wajib pajak, seperti laporan keuangan, SPT, dan hasil pemeriksaan.

Penilaian risiko dilakukan untuk menentukan tingkat keparahan dan dampak dari masing-masing risiko. Penilaian risiko dapat dilakukan dengan menggunakan metode-metode berikut:

- Metode kualitatif, digunakan untuk menilai risiko-risiko yang sulit dikuantifikasi, seperti risiko kepatuhan pajak yang disebabkan oleh faktor-faktor non-teknis.
- Metode kuantitatif. digunakan untuk menilai risiko-risiko yang dapat dikuantifikasi, seperti risiko kepatuhan pajak yang disebabkan oleh faktor-faktor teknis.

Pengendalian risiko adalah tindakan yang dilakukan untuk mengurangi tingkat keparahan dan dampak dari risiko. Pengendalian risiko ditetapkan berdasarkan hasil penilaian risiko. Pengendalian risiko dapat berupa pengendalian teknis, pengendalian operasional, dan pengendalian manajemen.

Penerapan manajemen risiko dalam pengawasan kepatuhan pajak di DJP:

- menggunakan data statistik untuk mengidentifikasi wajib pajak yang berisiko tinggi melakukan pelanggaran pajak. Wajib pajak yang berisiko tinggi tersebut kemudian diprioritaskan untuk dilakukan pemeriksaan.
- menggunakan teknologi informasi untuk meningkatkan efektivitas pemeriksaan pajak. Teknologi informasi dapat digunakan untuk menganalisis data dan informasi wajib pajak secara lebih cepat dan akurat.
- bekerja sama dengan instansi lain untuk meningkatkan efektivitas pengawasan kepatuhan pajak. Kerja sama ini dapat dilakukan dengan berbagi informasi dan data dengan instansi lain, seperti instansi penegak hukum.

DJP telah Penggunaan sistem informasi untuk memonitor dan mengevaluasi pengawasan wajib pajak, termasuk penggunaan data pemicu yang diperoleh dari hasil penyandingan data pada sistem informasi.

- **Melakukan penyandingan data**
  Penyandingan data adalah proses membandingkan data dari dua atau lebih sumber data, untuk mengidentifikasi potensi pelanggaran pajak.
  - **Data SPT dengan data laporan keuangan**
  - **Data SPT dengan data transaksi perbankan**
  - **Data SPT dengan data transaksi barang impor**

- **Menganalisis data**
  Analisis data adalah proses mengolah data untuk mendapatkan informasi, untuk memahami perilaku wajib pajak dan untuk mengidentifikasi potensi risiko kepatuhan pajak. Analisis data antara lain, **analisis statistic, analisis data mining, dan analisis big data**
- Laporan berupa dokumen yang berisi hasil analisis data, digunakan untuk membuat keputusan terkait pengawasan wajib pajak.
  - **Laporan pengawasan wajib pajak**
  - **Laporan risiko kepatuhan wajib pajak**
  - **Laporan hasil pemeriksaan pajak**

DJP juga menggunakan data pemicu untuk memonitor dan mengevaluasi pengawasan wajib pajak. Data pemicu adalah data yang menunjukkan adanya potensi pelanggaran pajak. DJP menggunakan data pemicu antara lain:

- **Data SPT yang tidak disampaikan tepat waktu**
- **Data SPT yang tidak lengkap atau tidak benar**
- **Data wajib pajak yang memiliki transaksi yang mencurigakan**

DJP menggunakan data pemicu untuk mengidentifikasi wajib pajak yang berisiko tinggi melakukan pelanggaran pajak. Wajib pajak yang berisiko tinggi tersebut kemudian diprioritaskan untuk dilakukan pemeriksaan pajak.

Melindungi aplikasi web sangat penting, mengingat banyaknya informasi sensitif dan pribadi yang tersimpan di dalamnya. DJP telah menerapkan beberapa strategi untuk melindungi aplikasi webnya, antara lain:

- **Pengujian pena sebagai layanan (PTaaS)**
  PTaaS adalah layanan yang menyediakan pengujian pena untuk aplikasi web. Pengujian pena adalah proses yang dilakukan untuk mengidentifikasi kerentanan keamanan dalam aplikasi web. DJP menggunakan PTaaS untuk mengidentifikasi dan mengatasi kerentanan potensial dalam aplikasi webnya. PTaaS dapat membantu DJP untuk:
  - **Meningkatkan keamanan aplikasi web**
  - **Memenuhi persyaratan peraturan**
  - **Menghemat waktu dan sumber daya**
- **Pengujian pena standar**
  Pengujian pena standar adalah proses yang dilakukan untuk mengidentifikasi kerentanan keamanan dalam aplikasi web dengan menggunakan metode dan alat yang standar. DJP juga menggunakan pengujian pena standar untuk mengidentifikasi dan mengatasi kerentanan potensial dalam aplikasi webnya. Pengujian pena standar dapat membantu DJP untuk:
  - **Meningkatkan keamanan aplikasi web**
  - **Memenuhi persyaratan peraturan**
  - **Menghemat biaya**
- **Penerapan kontrol keamanan aplikasi web**
  DJP juga menerapkan kontrol keamanan aplikasi web untuk melindungi aplikasi webnya. Kontrol keamanan aplikasi web adalah tindakan yang dilakukan untuk mengurangi risiko keamanan

dalam aplikasi web. DJP menerapkan kontrol keamanan aplikasi web antara lain:

- **Kontrol akses**
- **Kontrol autentikasi**
- **Kontrol otentikasi dua faktor**
- **Kontrol enkripsi**
- **Kontrol validasi input**
- **Kontrol manajemen patch**

7.4.2 Integrasi data dan analytic

Dalam menerapkan standar ISO/IEC 27005 untuk manajemen risiko keamanan informasi, DJP berupaya mengintegrasikan data dan analitik dari BDA dan BI ke dalam proses manajemen resiko. Integrasi ini bertujuan untuk memanfaatkan data besar dan analitik canggih dalam memprediksi, mendeteksi, dan merespons insiden keamanan.

Pertama, proses integrasi data dan analitik dimulai dengan pengumpulan data terpadu. DJP mengumpulkan data keamanan dari berbagai sumber internal dan eksternal, termasuk log sistem, sensor jaringan, intelijen ancaman, dan umpan data kerentanan. Data ini dikonsolidasikan menggunakan platform BDA yang mampu mengelola dan mengintegrasikan data besar dari sumber-sumber heterogen.

Selanjutnya, pemrosesan dan analisis data dilakukan. Teknologi pemrosesan data real-time digunakan untuk ekstraksi, transformasi, dan pemuatan data ke dalam sistem penyimpanan yang siap untuk analisis. Algoritma machine learning dan metode statistik dalam BDA diterapkan untuk mengidentifikasi pola, tren, dan anomali dalam data. Alat BI

kemudian digunakan untuk mengubah analitik ini menjadi laporan dan dashboard, memberikan wawasan intuitif tentang risiko keamanan informasi yang ada dan potensial.

Dalam proses manajemen risiko, DJP memanfaatkan hasil dari BDA untuk identifikasi risiko, menggunakannya untuk mengidentifikasi aset berisiko, ancaman potensial, dan kerentanan. Penilaian risiko dilakukan dengan mengintegrasikan data analitik ke dalam kerangka kerja penilaian risiko ISO/IEC 27005, menentukan dampak dan kemungkinan risiko. Strategi penanganan risiko disusun berdasarkan wawasan yang diperoleh dari BI, mempertimbangkan efektivitas kontrol yang ada dan biaya penerapan kontrol baru. Pemantauan dan review risiko dilakukan secara berkelanjutan menggunakan dashboard BI, memastikan bahwa data risiko selalu diperbarui.

Pengambilan keputusan strategis di DJP didukung oleh wawasan dari proses analitik. Ini termasuk penggunaan analitik prediktif untuk membentuk strategi keamanan siber jangka panjang dan alokasi sumber daya. Efektivitas integrasi data dan analitik diukur melalui penentuan Key Risk Indicators (KRI) dan Key Performance Indicators (KPI), serta evaluasi dan peningkatan berkelanjutan berdasarkan umpan balik dari operasional keamanan siber.

7.4.3 Respons otomatis terhadap ancaman

Dalam rangka menghadapi ancaman keamanan siber secara efisien dan efektif, DJP mengadopsi pendekatan respons otomatis yang selaras dengan standar ISO/IEC 27005 untuk manajemen risiko keamanan informasi. Proses pengembangan mekanisme respons otomatis ini dimulai

dengan integrasi sistem otomatisasi keamanan siber, ke dalam infrastruktur keamanan informasi yang ada. Integrasi ini memungkinkan respons otomatis terhadap insiden keamanan siber yang diidentifikasi.

Langkah penting dalam proses ini adalah penentuan aturan dan prosedur untuk respons otomatis. Aturan-aturan ini dibuat berdasarkan penilaian risiko yang teliti, dengan mempertimbangkan aset yang terlibat, tingkat keparahan ancaman, dan dampak potensialnya. Selanjutnya, pemodelan ancaman dan respons dilakukan untuk mensimulasikan skenario ancaman dan mengembangkan rencana respons yang tepat. Rencana ini diatur sedemikian rupa sehingga dapat dipicu secara otomatis ketika kondisi tertentu terpenuhi.

Implementasi respons otomatis melibatkan konfigurasi sistem untuk mendeteksi pola perilaku yang menandakan ancaman, seperti tanda tangan malware atau pola lalu lintas jaringan yang tidak biasa. Ketika pola-pola ini terdeteksi, sistem memicu aksi mitigasi otomatis, seperti memutus koneksi jaringan, mengkarantina email atau file mencurigakan, dan memblokir alamat IP atau domain yang diidentifikasi sebagai ancaman.

Evaluasi efektivitas mekanisme respons otomatis merupakan langkah penting untuk memastikan sistem beroperasi sebagaimana mestinya. DJP melakukan simulasi serangan untuk menguji respons sistem, memastikan reaksi yang tepat dan tepat waktu terhadap ancaman. Metrik kinerja, termasuk waktu deteksi ke insiden, waktu untuk respons, dan keberhasilan mitigasi, digunakan untuk mengevaluasi efektivitas sistem. Berdasarkan hasil

pengujian dan analisis metrik, aturan dan prosedur diubah dan disesuaikan untuk meningkatkan efektivitas respons otomatis dalam menghadapi ancaman siber yang potensial.

7.4.4 Strategi Mitigasi Berbasis Data

Strategi Mitigasi Berbasis Data di otoritas pajak:

- Pengamanan Fasilitas Pengolahan Data dan Informasi
  Otoritas pajak menetapkan pedoman khusus untuk mengamankan perangkat dan fasilitas pengolahan data. Tujuannya adalah untuk melindungi data dan perangkat dari akses tidak sah atau perusakan. Perlindungan data ini mencakup langkah-langkah seperti kontrol akses, penggunaan enkripsi, dan penerapan firewall untuk memastikan keamanan data.

  Beberapa langkah yang dilakukan Otoritas pajak untuk mengamankan fasilitas pengolahan data dan informasi antara lain:

  - Membangun sistem keamanan fisik yang kuat, seperti CCTV, dan sistem alarm.
  - Melakukan kontrol akses terhadap fasilitas pengolahan data dan informasi, seperti dengan menggunakan kartu akses dan sistem biometrik.
  - Melakukan pengamanan terhadap perangkat dan data, seperti dengan menggunakan sistem enkripsi.
- Peningkatan Keamanan Sistem
  Langkah-langkah ditetapkan organisasi untuk memperkuat sistem keamanan data, mengingat pentingnya menjaga kerahasiaan, integritas, dan ketersediaan informasi pajak serta data lain yang

sensitif. Strategi ini bertujuan untuk melindungi data dari akses tidak sah atau perusakan.

- Melakukan klasifikasi data berdasarkan tingkat sensitivitasnya.
- Melakukan pengamanan terhadap data yang sensitif, seperti dengan menggunakan sistem enkripsi dan sistem akses kontrol.
- Melakukan backup data secara berkala.

Implementasi strategi mitigasi berbasis data ini diharapkan dapat meningkatkan keamanan sistem otoritas pajak dan melindungi data dari berbagai ancaman. Penerapan strategi mitigasi berbasis data:

- sistem enkripsi untuk melindungi data-data sensitif,seperti data NPWP, data transaksi, dan data rahasia negara.
- sistem akses kontrol untuk membatasi akses terhadap fasilitas pengolahan data dan informasi hanya kepada orang-orang yang berwenang.
- backup data secara berkala untuk mencegah terjadinya kehilangan data akibat bencana atau serangan siber.

7.5 Analisis Kritis

Otoritas pajak mengadopsi pendekatan manajemen risiko yang komprehensif, mencakup evaluasi sistem, penggunaan intelligence threat, analisis prediktif, dan respons otomatis terhadap ancaman. Melalui integrasi standar ISO/IEC 27001:2013 dan penerapan kerangka kerja seperti COBIT 4.1 dan ITIL V2, organisasi penting untuk

menunjukkan komitmen terhadap pengelolaan keamanan informasi yang berbasis standar internasional.

1. Evaluasi Sistem dan Identifikasi Risiko

Organisasi mengadopsi pendekatan yang kuat dalam evaluasi sistem dan identifikasi risiko, menggunakan alat penilaian kerentanan dan standar ISO/IEC 27001:2013. Namun, tantangan utama adalah memastikan bahwa alat penilaian kerentanan terus diperbarui untuk mengatasi ancaman siber terbaru yang terus berkembang. Perlu memberikan atensi pada integrasi teknologi penilaian kerentanan yang menggunakan AI untuk secara dinamis belajar dan beradaptasi dengan ancaman baru. Peningkatan frekuensi evaluasi sistem untuk lebih responsif terhadap perubahan lingkungan keamanan juga diperlukan.

2. Intelligence Threat dan Analisis Prediktif

Penggunaan intelligence threat dan analisis prediktif adalah langkah positif, namun efektivitasnya sangat bergantung pada kualitas dan keaktualan data yang digunakan. Aspek penting untuk diupayakan organisasi meliputi:

- Memperkuat kerjasama dengan lembaga lain dan industri untuk pertukaran intelijen ancaman yang lebih luas dan real-time.
- Meningkatkan investasi dalam teknologi analitik canggih seperti machine learning dan AI untuk analisis prediktif yang lebih akurat.

3. Automasi Respons terhadap Ancaman

Mekanisme respons otomatis terhadap ancaman meningkatkan efisiensi dalam menangani insiden. Namun, risiko over-reliance pada automasi tanpa supervisi manusia yang memadai dapat menyebabkan miss-detection atau false positives. Area peningkatan meliputi:

- Implementasi hybrid model dalam respons insiden yang menggabungkan keputusan otomatis dan pengawasan manusia.
- Pengembangan dan pelatihan tim respons insiden siber untuk penilaian cepat dan pengambilan keputusan dalam kasus kompleks.

4. Framework Manajemen Risiko

Adopsi framework seperti ISO/IEC 27005 dan COBIT 4.1 menunjukkan komitmen DJP terhadap manajemen risiko yang terstruktur. Namun, implementasi framework ini perlu lebih fleksibel dan adaptif. Area peningkatan meliputi:

- Memperkenalkan metodologi agile dalam manajemen risiko untuk adaptasi yang lebih cepat terhadap ancaman dinamis.
- Menyelaraskan manajemen risiko dengan strategi bisnis secara keseluruhan untuk memastikan bahwa keamanan siber mendukung tujuan bisnis.

5. Peningkatan Kapasitas Analisis dan Respons

Pengintegrasian sistem peringatan dini dengan BDA dan BI meningkatkan kapasitas analisis dan respons, tetapi penting untuk terus meningkatkan kemampuan analisis data. Area peningkatan meliputi:

- Penggunaan cloud-based analytics untuk skala dan fleksibilitas yang lebih besar dalam analisis data keamanan.
- Pelatihan berkelanjutan untuk tim analis dalam teknik analisis data terkini dan interpretasi hasil analisis.

Strategi manajemen risiko cyber security pada otoritas pajak menunjukkan upaya yang komprehensif dan matang dalam menghadapi ancaman siber. Namun, lingkungan siber yang terus berubah menuntut adaptasi dan inovasi berkelanjutan. Organisasi perlu terus mengevaluasi dan memperbarui strategi mereka, tidak hanya untuk mengikuti perkembangan teknologi dan ancaman terbaru tetapi juga untuk memastikan bahwa pendekatan keamanan siber mereka tetap selaras dengan tujuan organisasi dan dinamika industri. Melalui peningkatan berkelanjutan dan adaptasi strategis, organisasi dapat memperkuat pertahanan siber dan meningkatkan ketahanan terhadap ancaman siber yang semakin kompleks.

BAB VIII

DAMPAK CYBER SECURITY TERHADAP KINERJA AUDIT PAJAK

8.1 Cyber Security dalam Audit Pajak

8.1.1 Cyber Security Untuk Melindungi Data Dan Sistem Informasi Pajak

Di era digital saat ini, data dan sistem informasi pajak memiliki peran yang sangat krusial dalam pengumpulan dan pengelolaan pajak. Kedua elemen ini tidak hanya memudahkan proses administrasi pajak tetapi juga meningkatkan efisiensi dan efektivitas pengawasan pajak. Namun, seiring dengan kemudahannya, risiko terhadap keamanan data dan sistem informasi juga meningkat. Oleh karena itu, penerapan cyber security menjadi sangat penting dalam melindungi data dan sistem informasi pajak dari ancaman serangan siber.

Mengapa Cyber Security Penting?

1) Perlindungan Data Wajib Pajak
   Data wajib pajak merupakan informasi sensitif yang mencakup data pribadi, informasi keuangan, dan transaksi bisnis. Keamanan data ini harus terjaga

untuk melindungi privasi wajib pajak dan menjaga kepercayaan publik terhadap sistem pajak.

2) Integritas Sistem Informasi Pajak
   Serangan siber dapat merusak integritas data dan sistem, mengakibatkan kerugian finansial dan reputasi bagi otoritas pajak. Dengan cyber security yang kuat, integritas dan ketersediaan data dan sistem informasi pajak dapat terjaga.
3) Pencegahan Penipuan Pajak
   Penipuan pajak sering kali dilakukan dengan memanipulasi data dan sistem informasi pajak. Cyber security yang efektif dapat mendeteksi dan mencegah upaya penipuan pajak, menjaga keadilan dan efisiensi sistem pajak.

Dalam audit pajak, cyber security berperan sebagai benteng pertahanan utama yang melindungi data dan sistem informasi pajak dari ancaman siber. Dalam konteks audit pajak, cyber security memegang peran kritis sebagai garis pertahanan utama terhadap berbagai ancaman siber yang mengancam integritas, kerahasiaan, dan ketersediaan data dan sistem informasi pajak. Penerapan teknis dari cyber security dalam audit pajak melibatkan beberapa aspek kunci, yang secara bersama-sama membentuk benteng pertahanan yang kokoh.

Bagaimana kebocoran data wajib pajak atau serangan siber terhadap infrastruktur TI otoritas pajak terjadi, memerlukan pemahaman tentang beberapa mekanisme dasar dan kerentanan yang dimanfaatkan oleh pelaku kejahatan siber.

8.1.1.1 Kebocoran Data Wajib Pajak

A. Eksploitasi Kerentanan Perangkat Lunak

Pelaku kejahatan siber seringkali mengeksploitasi kerentanan dalam perangkat lunak yang digunakan oleh otoritas pajak. Eksploitasi tersebut melibatkan penggunaan exploit yang memanfaatkan celah keamanan dalam basis data, aplikasi web, atau sistem manajemen konten untuk mendapatkan akses tidak sah ke data wajib pajak. Dalam audit pajak, pemanfaatan kerentanan perangkat lunak oleh pelaku kejahatan siber merupakan masalah serius yang dapat mengganggu integritas keseluruhan proses audit.

Ketika kerentanan dalam perangkat lunak atau jaringan dimanfaatkan, data pajak yang sensitif bisa diakses, diubah, atau dihapus oleh pihak yang tidak berwenang. Hal ini mengancam integritas data yang merupakan fondasi dari proses audit pajak. Audit memerlukan data yang akurat dan lengkap untuk analisis dan pengambilan keputusan. Jika data tersebut telah dikompromikan, hasil audit tidak bisa diandalkan, mengakibatkan penilaian pajak yang salah atau bahkan keputusan audit yang tidak adil.

Eksploitasi kerentanan perangkat lunak dalam audit pajak dapat berupa:

1) Identifikasi Kerentanan
   Pelaku kejahatan siber menggunakan alat dan teknik canggih untuk mengidentifikasi kerentanan dalam perangkat lunak yang digunakan oleh otoritas pajak. Kerentanan ini termasuk celah keamanan dalam sistem manajemen basis data, aplikasi web, dan platform manajemen konten. Kerentanan dapat ditemukan melalui pemindaian otomatis atau

penelitian manual terhadap kode sumber yang tersedia secara publik atau dokumentasi sistem.

2) Pengembangan dan Penerapan Exploit
   Setelah kerentanan diidentifikasi, pelaku kejahatan mengembangkan exploit—kode atau teknik khusus yang dirancang untuk memanfaatkan celah keamanan tersebut. Exploit ini kemudian digunakan untuk mendapatkan akses tidak sah ke sistem, memungkinkan penyerang untuk mengakses, memodifikasi, atau menghapus data pajak yang sensitif.
3) Dampak terhadap Integritas Data Pajak
   Akses tidak sah ini mengancam integritas data yang merupakan fondasi kritis dari proses audit pajak. Integritas data merujuk pada keakuratan dan konsistensi data sepanjang siklus hidupnya. Dalam audit pajak, keutuhan data sangat penting untuk memastikan bahwa semua informasi yang dianalisis dan digunakan dalam proses pengambilan keputusan adalah akurat dan belum diubah atau dikompromikan.
4) Konsekuensi terhadap Proses Audit
   Ketika data pajak yang sensitif dikompromikan, auditor pajak berdasarkan pada informasi yang tidak lengkap atau salah, mengakibatkan analisis yang tidak akurat dan keputusan audit yang mungkin tidak adil atau salah. Keputusan audit yang dimaksud tersebut termasuk penilaian pajak yang tidak tepat, baik terlalu tinggi atau terlalu rendah, dan rekomendasi audit yang tidak didasarkan pada fakta yang akurat. Lebih lanjut, kebocoran data juga bisa mengungkapkan strategi audit atau informasi sensitif lainnya kepada

pihak yang tidak berhak, mengurangi efektivitas audit masa depan.

Dalam menghadapi risiko ini, sangat penting bagi otoritas pajak untuk menerapkan solusi keamanan yang komprehensif, termasuk pembaruan perangkat lunak teratur, penerapan patch keamanan segera setelah tersedia, dan penggunaan alat deteksi intrusi untuk mengidentifikasi upaya akses tidak sah. Selain itu, audit keamanan TI secara berkala dan pengujian penetrasi sistem bisa membantu mengidentifikasi dan mengatasi kerentanan sebelum dimanfaatkan oleh penyerang.

Mengatasi kerentanan ini membutuhkan pendekatan berlapis yang tidak hanya fokus pada aspek teknis tetapi juga melibatkan pelatihan karyawan tentang ancaman siber dan praktik terbaik untuk mengurangi risiko kebocoran data atau eksploitasi sistem.

B. Phishing dan Teknik Social Engineering

Serangan phishing menggunakan email atau komunikasi yang menyamar sebagai sumber terpercaya untuk memancing pengguna (dalam hal ini, karyawan otoritas pajak atau wajib pajak sendiri) memasukkan informasi sensitif seperti username dan password ke dalam website palsu, yang kemudian digunakan untuk mengakses sistem dan mencuri data. Mengungkapkan informasi login atau data sensitif lainnya melalui teknik social engineering bisa menyebabkan kebocoran informasi pajak.

Dalam audit pajak, serangan phishing dan teknik social engineering ini menargetkan individu dengan tujuan memperoleh akses tidak sah ke sistem informasi pajak

melalui pengelabuan. Kerahasiaan data wajib pajak adalah penting untuk menjaga kepercayaan publik dan mematuhi hukum privasi. Kebocoran data bisa berdampak negatif terhadap reputasi otoritas pajak dan mengurangi kepercayaan wajib pajak.

Phishing dan teknik social engineering dalam Audit Pajak:

1) Serangan Phishing dilakukan dengan mengirimkan email atau pesan yang terlihat legitim, seringkali menyamar sebagai komunikasi resmi dari otoritas pajak, untuk memancing korban memasukkan kredensial ke dalam halaman web palsu. Halaman ini dirancang untuk menyerupai antarmuka resmi otoritas pajak, menipu karyawan atau wajib pajak agar membagikan informasi sensitif.
2) Dalam teknik social engineering, penyerang menggunakan manipulasi psikologis untuk memperoleh informasi sensitif atau mempengaruhi individu agar melakukan tindakan yang merugikan keamanan data, seperti membuka lampiran berisi malware atau memberikan akses langsung ke sistem pajak.

Dampak terhadap Audit Pajak:

1) Pengungkapan kredensial akses melalui serangan phishing memungkinkan penyerang mengakses sistem audit pajak, memperoleh data wajib pajak tanpa otorisasi, dan potensial memanipulasi atau mencuri informasi penting. Kerahasiaan data merupakan pilar penting dalam proses audit pajak; pelanggaran ini

dapat merusak integritas audit dan menimbulkan pertanyaan tentang validitas hasil audit.

2) Akses tidak sah ini tidak hanya mengancam privasi data tapi juga integritasnya, kunci dalam menentukan kewajiban pajak yang akurat. Jika data yang dikompromikan digunakan dalam audit, hasilnya bisa menjadi tidak akurat atau menyesatkan, mempengaruhi keputusan pajak dan potensial mengakibatkan kerugian finansial bagi wajib pajak atau negara.
3) Kebocoran data melalui teknik ini juga dapat merusak kepercayaan publik terhadap otoritas pajak. Kepercayaan ini esensial untuk kepatuhan pajak sukarela; kerusakan tersebut dapat berdampak jangka panjang terhadap kepatuhan pajak dan penerimaan pajak negara.

Serangan phishing dan teknik social engineering mengeksploitasi kerentanan manusia daripada teknologi per se. Dalam audit pajak, konsekuensi dari serangan ini bukan hanya teknis tapi juga psikologis, mengancam integritas data pajak dan kepercayaan publik. Menghadapi ancaman ini memerlukan kombinasi kebijakan keamanan siber yang kuat, pelatihan kesadaran keamanan untuk staf otoritas pajak dan wajib pajak, serta teknologi keamanan informasi untuk mendeteksi dan mencegah serangan sebelum serangan dapat merusak sistem audit pajak.

C. Insider Threats

Kebocoran data dapat juga terjadi karena tindakan dari dalam, di mana karyawan atau pihak internal dengan akses ke sistem informasi pajak secara sengaja atau tidak

sengaja membocorkan data sensitif. Akses tidak sah atau pembocoran data oleh karyawan dapat merusak proses audit dari dalam. Misalnya, jika informasi tentang audit yang sedang berlangsung bocor, ini bisa memberi kesempatan kepada wajib pajak yang tidak bermoral untuk mengubah catatan mereka sebelum audit selesai, mengganggu keadilan dan keakuratan audit.

Ancaman internal, atau risiko yang berasal dari individu dalam organisasi, menimbulkan tantangan signifikan dalam lingkup keamanan informasi, khususnya dalam konteks audit pajak.

Vektor Ancaman:

1) Karyawan dapat mengirimkan data pajak sensitif melalui saluran komunikasi yang tidak aman, seperti email tanpa enkripsi, menempatkan data tersebut pada risiko intersepsi oleh pihak tidak berwenang. Hal ini melibatkan risiko kebocoran informasi yang dapat digunakan untuk menghindari kewajiban pajak atau manipulasi audit.
2) Penggunaan USB drive atau perangkat penyimpanan eksternal lainnya untuk mengangkut data pajak meningkatkan risiko kehilangan data atau pencurian fisik, yang bisa menyebabkan kompromi data audit secara luas.
3) Karyawan yang mengakses sistem informasi pajak tanpa otorisasi atau untuk tujuan non-resmi dapat mengubah atau menghapus data penting, mempengaruhi integritas dan keandalan basis data yang digunakan untuk audit pajak.

Kebocoran atau pengubahan tidak sah data pajak mengganggu integritas dataset yang digunakan dalam audit pajak, yang bisa menyebabkan penilaian pajak yang tidak akurat dan potensial kerugian pendapatan bagi lembaga pajak. Kompromi data pajak sensitif merusak kerahasiaan wajib pajak, mempengaruhi kepercayaan pada sistem pajak, dan mungkin melanggar peraturan perlindungan data. Akses tidak sah yang menghasilkan penghapusan atau pengubahan data dapat mengurangi ketersediaan informasi penting, menghambat kemampuan auditor dalam melakukan analisis pajak yang efektif.

Ancaman internal dalam audit pajak menuntut pendekatan yang komprehensif untuk mengelola risiko keamanan informasi, yang mencakup aspek teknis, prosedural, dan manusia. Dengan memperkuat keamanan dari dalam, otoritas pajak dapat meminimalisir potensi kerentanan dan memastikan proses audit yang lebih aman dan lebih dapat diandalkan.

8.1.1.2 Serangan Siber terhadap Infrastruktur TI

A. DDoS (Distributed Denial of Service):

Serangan Distributed Denial of Service (DDoS) merupakan taktik serangan siber yang dirancang untuk mengganggu normalitas operasional server, sistem, atau jaringan dengan cara membanjiri target dengan volume lalu lintas internet yang massif. Teknik ini bertujuan untuk melebihi kapasitas pemrosesan dan bandwidth, sehingga layanan yang disediakan menjadi tidak tersedia bagi pengguna yang sah. Serangan DDoS biasanya dilakukan melalui botnet, yakni jaringan perangkat yang terinfeksi

malware dan dikendalikan secara remote untuk mengirim permintaan secara simultan ke target. Dalam konteks infrastruktur TI otoritas pajak, hal tersebut mencakup sistem pengumpulan data pajak, platform audit elektronik, atau database wajib pajak.

Dalam audit pajak, serangan Distributed Denial of Service (DDoS) dapat memiliki dampak signifikan terhadap kemampuan auditor dalam melaksanakan tugas secara efektif. Pengaruh serangan DDoS terhadap proses audit pajak dapat meliputi:

1) Serangan DDoS yang membanjiri server dengan lalu lintas internet secara berlebihan menyebabkan sistem informasi pajak menjadi tidak tersedia. Akibatnya, auditor pajak kehilangan akses ke aplikasi dan database yang krusial untuk melakukan tugas audit, seperti verifikasi transaksi, analisis laporan keuangan, dan penilaian kepatuhan pajak wajib pajak.
2) Dengan sistem yang tidak dapat diakses, jadwal audit terganggu. Tugas-tugas yang seharusnya dilakukan secara berurutan mengalami penundaan, mengakibatkan keseluruhan proses audit berlangsung lebih lambat dari yang direncanakan.
3) Keputusan penting yang bergantung pada analisis data dan hasil audit juga tertunda. Ini termasuk penerapan keputusan pajak, seperti penyesuaian pajak, penalti, atau pemberian pengembalian pajak kepada wajib pajak. Penundaan ini tidak hanya mempengaruhi efisiensi kerja auditor tapi juga dapat mempengaruhi penerimaan negara dari pajak dan resolusi sengketa pajak dengan wajib pajak.

Implikasi bagi auditor pajak

1) Auditor perlu mengantisipasi kemungkinan gangguan ini dan mempertimbangkan alternatif strategi audit, seperti penggunaan data offline atau dokumentasi fisik, sementara menunggu pemulihan sistem.
2) Penting untuk menjaga komunikasi yang transparan dengan wajib pajak mengenai potensi penundaan dalam proses audit akibat serangan DDoS, meminimalisir ketidakpastian dan menjaga kepercayaan.
3) Auditor harus mendokumentasikan gangguan yang disebabkan oleh serangan DDoS sebagai bagian dari laporan audit, termasuk dampaknya terhadap jadwal audit dan pemeriksaan pajak.
4) Kerja sama erat dengan tim teknologi informasi (TI) untuk memahami risiko keamanan siber dan langkah-langkah mitigasi yang dapat dilakukan untuk meminimalisir dampak serangan DDoS di masa mendatang.

Dalam menghadapi serangan DDoS, penting bagi auditor pajak untuk menyesuaikan pendekatan auditor dan tetap fleksibel dalam melaksanakan audit. Menggunakan praktik terbaik dalam manajemen risiko dan keamanan siber adalah kunci untuk meminimalisir dampak negatif dari serangan tersebut terhadap proses audit.

Dalam audit pajak, pentingnya menjaga kelancaran dan kecepatan proses audit tidak hanya berhubungan dengan efisiensi internal, tetapi juga berdampak signifikan pada keseluruhan siklus penerimaan pajak dan persepsi publik terhadap otoritas pajak. Dampak penundaan penyelesaian audit akibat serangan DDoS:

1) Keterlambatan dalam menyelesaikan audit berarti bahwa keputusan terkait kewajiban pajak, baik itu menetapkan jumlah yang harus dibayarkan wajib pajak atau mengidentifikasi potensi pengembalian pajak, juga tertunda. Hal ini tidak hanya mempengaruhi wajib pajak yang bersangkutan tetapi juga mengganggu proyeksi dan realisasi penerimaan pajak oleh pemerintah.
2) Penundaan dalam proses audit dan penilaian pajak dapat menyebabkan penundaan dalam penerimaan pendapatan pajak. Hal ini berarti bahwa dana yang diharapkan untuk berbagai program pemerintah dan pembangunan mungkin tidak tersedia sesuai jadwal, potensial mempengaruhi pelaksanaan proyek-proyek publik dan layanan.
3) Serangan DDoS yang berkepanjangan dan kemampuan otoritas pajak yang terbatas dalam menangani serangan ini dapat menciptakan kesan bahwa otoritas pajak tidak mampu melindungi data sensitif wajib pajak atau menjaga kelancaran layanan. Hal ini dapat merusak kepercayaan publik, yang merupakan aset penting dalam memastikan kepatuhan pajak sukarela dan efektivitas sistem pajak secara keseluruhan.

Tindakan yang dapat diambil oleh auditor pajak:

1) Penting untuk menjaga komunikasi yang baik dengan wajib pajak selama masa gangguan, memberikan update tentang status audit dan perkiraan waktu penyelesaian. Ini membantu menjaga kepercayaan dan meminimalkan frustrasi dari pihak wajib pajak.

2) Bekerja sama dengan departemen teknologi informasi untuk memahami langkah-langkah yang diambil untuk mengatasi serangan DDoS dan mempercepat pemulihan sistem. Pemahaman ini memungkinkan auditor untuk menyesuaikan rencana audit mereka secara realistis.
3) Menyesuaikan rencana dan jadwal audit untuk memprioritaskan kasus-kasus penting atau sensitif waktu, serta memanfaatkan sumber daya yang tersedia secara efektif selama periode gangguan.
4) Mendokumentasikan dampak serangan DDoS terhadap proses audit dan komunikasi ini ke manajemen senior serta dalam laporan audit, sebagai bagian dari evaluasi risiko dan tanggapan institusi.

Memahami dan mengatasi dampak dari serangan DDoS terhadap proses audit pajak membutuhkan pendekatan yang komprehensif, termasuk manajemen risiko, komunikasi efektif, dan kolaborasi antar-departemen. Hal ini tidak hanya membantu dalam mitigasi jangka pendek tetapi juga dalam membangun resiliensi jangka panjang terhadap serangan siber serupa di masa depan.

B. Ransomware:

Ransomware adalah jenis malware yang mengenkripsi file pada sistem yang terinfeksi dan meminta tebusan untuk kunci dekripsi. Serangan ransomware dapat mengunci akses ke data pajak penting, menghambat operasi audit dan layanan kepada wajib pajak. Serangan ransomware dapat mengenkripsi data audit penting, membuatnya tidak dapat diakses oleh auditor. Hal ini tidak hanya menghambat

proses audit tetapi juga bisa menunda pengumpulan pajak dan penyelesaian sengketa pajak.

Keamanan siber dalam audit pajak bukan hanya tentang melindungi data dari akses tidak sah, tetapi juga tentang memastikan bahwa proses audit dapat berjalan dengan efisien, efektif, dan adil. Serangan siber yang berhasil tidak hanya dapat mengganggu operasi harian otoritas pajak tetapi juga dapat merusak integritas sistem audit pajak secara keseluruhan, mengancam kerahasiaan data wajib pajak, dan menghambat penerapan dan penegakan hukum pajak. Oleh karena itu, langkah pengamanan yang komprehensif dan berlapis sangat diperlukan untuk melindungi infrastruktur TI otoritas pajak dari ancaman siber, mendukung kelancaran proses audit pajak, dan menjaga kepercayaan publik terhadap sistem perpajakan.

Dalam audit pajak, menghadapi ancaman siber seperti ransomware dan penyusupan jaringan membutuhkan pemahaman mendalam tentang bagaimana serangan-serangan ini dapat mempengaruhi proses audit. Dampak serangan siber terhadap audit pajak:

1) Akses Data Terhambat
   Enkripsi file oleh ransomware membatasi akses auditor ke data penting, seperti catatan transaksi atau dokumen pendukung, yang diperlukan untuk menyelesaikan audit secara akurat dan tepat waktu.
2) Penghambatan Proses Audit
   Kehilangan akses ke data audit memperlambat atau bahkan menghentikan proses audit, mengakibatkan penundaan dalam penyelesaian audit dan pengajuan laporan audit.

3) Dampak terhadap Penerimaan Pajak
   Penundaan dalam proses audit dapat menyebabkan penundaan dalam penilaian dan pengumpulan pajak, mempengaruhi arus kas pemerintah dan alokasi dana untuk layanan publik.

Penyusupan jaringan melibatkan akses tidak sah ke jaringan internal, yang memungkinkan penyerang untuk mencari data sensitif atau menanam backdoor untuk akses masa depan. Dampaknya pada audit pajak meliputi:

1) Penyusupan memungkinkan penyerang mengakses informasi pajak yang sensitif, berpotensi mengungkap data wajib pajak atau informasi tentang audit yang sedang berlangsung, yang dapat disalahgunakan.
2) Kehadiran backdoor atau alat lain yang ditinggalkan oleh penyerang dalam jaringan dapat memungkinkan manipulasi data tanpa deteksi, mengancam integritas audit pajak dan kepercayaan pada hasilnya.

Untuk menghadapi ancaman siber, auditor pajak dan otoritas pajak harus menerapkan strategi keamanan yang komprehensif:

1) Auditor harus dilengkapi dengan pengetahuan tentang ancaman siber dan praktik terbaik untuk menghindari serangan, termasuk pengenalan teknik phishing dan keamanan data.
2) Memastikan bahwa backup data penting dilakukan secara berkala dan disimpan di lokasi yang aman, memungkinkan pemulihan cepat dalam kasus serangan ransomware.
3) Kerjasama erat dengan tim TI untuk memastikan bahwa sistem audit dilindungi dengan solusi

keamanan siber terkini, seperti firewall, anti-malware, dan enkripsi data.

4) Pengembangan dan pelatihan protokol tanggap darurat siber, memastikan tim siap untuk merespons dan memitigasi dampak serangan siber dengan cepat.

8.1.2 Pentingnya cyber security dalam audit pajak

Pentingnya cyber security dalam audit pajak tidak dapat diabaikan. Dengan meningkatnya ancaman siber, menjaga keamanan data dan sistem informasi pajak adalah prioritas utama yang mendukung integritas dan efisiensi sistem perpajakan. Investasi dalam cyber security adalah investasi dalam kepercayaan publik dan kepatuhan pajak, yang pada akhirnya mendukung fungsi vital penerimaan negara untuk pembangunan dan kesejahteraan masyarakat. Dalam konteks audit pajak, cyber security bukan lagi sekedar opsi tambahan, melainkan telah menjadi kebutuhan fundamental. Mengingat volume besar transaksi pajak yang dilakukan secara elektronik, keamanan siber menjadi kunci utama dalam menjaga integritas dan kepercayaan terhadap sistem perpajakan. Aspek ini sangat kritis mengingat dampak yang dapat ditimbulkan oleh insiden keamanan siber terhadap pengumpulan pajak dan privasi wajib pajak.

Mengapa Penting?

1) Dengan meningkatnya serangan siber, sistem informasi pajak yang tidak aman bisa menjadi target bagi pelaku kejahatan siber. Cyber security membantu dalam mengidentifikasi, mencegah, dan merespons serangan siber secara efektif.

2) Kepercayaan publik terhadap sistem pajak sangat bergantung pada kemampuan otoritas pajak dalam menjaga kerahasiaan dan integritas data. Insiden kebocoran data dapat merusak kepercayaan ini dan mengurangi kepatuhan pajak.
3) Banyak negara telah mengimplementasikan regulasi ketat terkait keamanan data dan privasi. Otoritas pajak harus mematuhi regulasi ini untuk menghindari sanksi hukum dan denda.
4) Cyber security yang efektif memungkinkan auditor pajak untuk mengakses data yang dibutuhkan dengan cepat dan aman, meningkatkan efisiensi dan efektivitas audit.

8.1.3 Implementasi Regulasi Keamanan Data dan Privasi di Beberapa Negara

Pemahaman tentang regulasi keamanan data dan privasi di berbagai negara sangat penting bagi auditor pajak, mengingat regulasi ini mempengaruhi cara pengumpulan, pengolahan, dan penyimpanan data pajak.

1. Uni Eropa (General Data Protection Regulation - GDPR)

GDPR merupakan salah satu regulasi perlindungan data paling ketat dan komprehensif di dunia, yang diberlakukan pada Mei 2018. Regulasi ini mengatur pengolahan data pribadi individu dalam Uni Eropa (UE) dan Area Ekonomi Eropa (EEA). GDPR menekankan pada prinsip akuntabilitas, di mana organisasi harus tidak hanya mematuhi regulasi tetapi juga dapat membuktikan kepatuhan melalui dokumentasi dan rekam jejak keamanan data.

Relevansi GDPR dengan Audit Pajak:

a) Pengumpulan dan Pengolahan Data Wajib Pajak
   - Otoritas pajak dan entitas bisnis diharuskan mengumpulkan dan memproses data wajib pajak hanya sejauh yang diperlukan untuk tujuan audit dan kepatuhan pajak, sesuai dengan prinsip minimisasi data, pembatasan tujuan, dan keamanan data.
   - Individu memiliki hak yang diperkuat di bawah GDPR, termasuk hak untuk mengakses data sendiri, meminta koreksi, serta membatasi atau menolak pengolahan data.

b) Transparansi dan Akuntabilitas
   - Otoritas pajak dan perusahaan harus menyediakan informasi yang transparan dan mudah diakses mengenai pengumpulan, penggunaan, dan pengelolaan data wajib pajak, termasuk menyampaikan informasi tentang hak-hak subjek data secara jelas.
   - Entitas yang bertanggung jawab atas pengumpulan dan pengolahan data wajib pajak harus bisa mendemonstrasikan kepatuhan terhadap GDPR, melalui dokumentasi kebijakan keamanan data, rekaman proses pengolahan data, serta hasil audit keamanan dan privasi data secara berkala.

2. Amerika Serikat (Health Insurance Portability and Accountability Act (HIPAA) dan California Consumer Privacy Act (CCPA)

Meskipun AS tidak memiliki undang-undang perlindungan data yang bersifat umum seperti GDPR, terdapat regulasi seperti HIPAA yang mengatur keamanan dan privasi data kesehatan, dan CCPA yang merupakan undang-undang privasi konsumen di California. CCPA memberikan hak yang lebih besar kepada konsumen terkait akses dan kontrol atas data pribadi. Regulasi tersebut dan relevansinya dengan audit pajak di AS:

a) HIPAA dirancang untuk melindungi informasi kesehatan pasien dan menerapkan standar keamanan untuk mengamankan data kesehatan elektronik. HIPAA melibatkan penyedia layanan kesehatan, rencana kesehatan, dan pihak ketiga yang memproses informasi kesehatan. Auditor pajak yang bekerja dengan entitas di sektor kesehatan harus memastikan bahwa penanganan data pajak yang berhubungan dengan informasi kesehatan pasien mematuhi HIPAA. Hal ini termasuk verifikasi bahwa kontrol keamanan yang sesuai ada di tempat dan bahwa ada prosedur untuk mengelola akses dan pengungkapan informasi tersebut.
b) California Consumer Privacy Act (CCPA) memberikan warga California hak yang lebih luas terhadap privasi data mereka, termasuk hak untuk mengetahui tentang pengumpulan data pribadi, hak untuk meminta penghapusan data, dan hak untuk menolak penjualan data pribadi. Auditor pajak yang bekerja dengan organisasi yang beroperasi di California perlu memahami bagaimana CCPA mempengaruhi

pengumpulan dan pengolahan data pribadi, termasuk data pajak. Hal tersebut berarti memastikan kepatuhan terhadap permintaan akses dan penghapusan data serta menerapkan langkah-langkah keamanan yang memadai untuk melindungi data pribadi.

3. Australia (Privacy Act 1988 dan Australian Privacy Principles (APPs))

Australia mengatur perlindungan data dan privasi melalui Privacy Act dan APPs yang mengatur standar, hak, dan kewajiban seputar pengumpulan, penggunaan, dan pemberian akses kepada informasi pribadi. Auditor pajak di Australia harus memastikan bahwa praktik pengolahan data pajak mereka sesuai dengan APPs, khususnya dalam hal transparansi dalam pengumpulan data, pemeliharaan kualitas data, dan keamanan informasi pribadi.

a) Privacy Act 1988. Regulasi ini memberlakukan kewajiban pada organisasi tertentu dalam hal pengumpulan, penggunaan, penyimpanan, dan pengungkapan informasi pribadi. Hal ini termasuk agensi pemerintah, perusahaan, dan organisasi non-profit tertentu di Australia, yang semuanya dapat terlibat dalam pengolahan data pajak.
b) Australian Privacy Principles (APPs) menetapkan standar, hak, dan kewajiban untuk pengelolaan informasi pribadi. APPs mencakup prinsip-prinsip seperti transparansi dalam pengumpulan data, akurasi dan keamanan data, serta hak individu untuk mengakses dan mengoreksi informasi pribadi.

Relevansi dengan Audit Pajak

a) Auditor pajak harus memastikan bahwa wajib pajak diberitahu tentang pengumpulan informasi pribadi, termasuk tujuan pengumpulannya dan bagaimana informasi tersebut akan digunakan. Hal ini sesuai dengan APP 1, yang menekankan pada pentingnya transparansi dan pemberitahuan kepada individu.
b) Sesuai dengan APP 10, auditor pajak harus mengambil langkah-langkah yang wajar untuk memastikan bahwa data pajak yang dikumpulkan, gunakan, atau ungkapkan akurat, lengkap, dan terkini. Hal ini penting untuk memastikan bahwa keputusan audit berdasarkan data yang andal.
c) Sesuai dengan APP 11, informasi pribadi yang dikumpulkan atau diolah sebagai bagian dari audit pajak harus dilindungi dari risiko akses, pengungkapan, pengubahan, atau kerusakan yang tidak sah. Hal ini termasuk menerapkan langkah keamanan fisik, teknis, dan administratif yang sesuai.

4. Kanada (Personal Information Protection and Electronic Documents Act (PIPEDA))

PIPEDA mengatur cara organisasi swasta mengumpulkan, menggunakan, dan mengungkapkan informasi pribadi dalam praktik bisnis. Hal ini termasuk persyaratan untuk konsen eksplisit dalam pengumpulan data sensitif, seperti informasi keuangan yang sering kali dikelola dalam proses audit pajak. Auditor di Kanada harus memastikan kepatuhan terhadap PIPEDA, terutama dalam pengumpulan dan pengolahan data pajak.

Relevansi PIPEDA untuk Audit Pajak di Kanada. PIPEDA mengharuskan organisasi untuk memperoleh konsen eksplisit ketika mengumpulkan, menggunakan, atau mengungkapkan informasi pribadi yang sensitif. Dalam konteks audit pajak, hal ini berarti auditor harus memastikan bahwa konsen eksplisit diperoleh dari wajib pajak untuk setiap pengumpulan dan penggunaan data keuangan dan pribadi yang sensitif.

a) Pengumpulan dan Pengolahan Data Pajak
   - Sesuai dengan prinsip PIPEDA, pengumpulan informasi pribadi harus terbatas pada apa yang diperlukan secara wajar untuk tujuan yang diidentifikasi. Auditor harus memastikan bahwa hanya informasi yang benar-benar diperlukan untuk audit pajak yang dikumpulkan dari wajib pajak.
   - Pengolahan data pajak harus dilakukan dengan cara yang adil dan sah, dengan mematuhi semua ketentuan PIPEDA yang relevan, termasuk mengamankan informasi pribadi dari risiko kehilangan, pencurian, dan akses tidak sah.

b) Transparansi dan Akuntabilitas
   - Organisasi harus jelas dan transparan mengenai cara mengumpulkan, menggunakan, dan mengungkapkan informasi pribadi. Auditor pajak harus memastikan bahwa wajib pajak diberi tahu tentang pengolahan data mereka dengan cara yang memenuhi standar PIPEDA.
   - Organisasi bertanggung jawab untuk memastikan kepatuhan dengan PIPEDA, termasuk saat menyerahkan pengolahan data kepada pihak

ketiga. Hal ini berarti auditor pajak harus memverifikasi bahwa penyedia layanan juga mematuhi PIPEDA dalam penanganan data pajak.

Di Asia dan Asia Tenggara, berbagai negara telah mengembangkan dan menerapkan regulasi keamanan data dan privasi untuk menjawab tantangan yang berkaitan dengan perlindungan data pribadi. Berikut adalah contoh dari beberapa negara di kawasan ini:

1. Singapura (Personal Data Protection Act (PDPA))

PDPA di Singapura mengatur pengumpulan, penggunaan, dan pengungkapan data pribadi oleh organisasi, dan menetapkan standar keamanan yang harus dipatuhi. PDPA juga menuntut organisasi untuk mendapatkan persetujuan dari individu sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi. PDPA dirancang untuk melindungi data pribadi individu dalam pengolahan oleh organisasi, sekaligus memungkinkan kebutuhan organisasi untuk memproses data untuk tujuan bisnis yang sah. Hal ini merupakan keseimbangan penting antara perlindungan privasi dan operasional bisnis.

Aplikasi PDPA dalam Audit Pajak:

a) Sesuai dengan PDPA, otoritas pajak dan perusahaan di Singapura harus memperoleh persetujuan eksplisit dari wajib pajak sebelum mengumpulkan, menggunakan, atau mengungkapkan data pribadi mereka untuk tujuan audit pajak. Hal ini termasuk memberikan informasi yang jelas tentang tujuan pengumpulan data.

b) Data pribadi yang dikumpulkan untuk audit pajak harus digunakan secara eksklusif untuk tujuan audit tersebut. PDPA melarang penggunaan data untuk tujuan lain tanpa persetujuan tambahan.
c) Otoritas pajak dan perusahaan di Singapura wajib menerapkan tindakan keamanan yang memadai untuk melindungi data pribadi dari kehilangan, pencurian, modifikasi yang tidak sah, atau akses tidak berwenang. Hal ini mencakup langkah-langkah fisik, teknis, dan administratif.
d) Wajib pajak memiliki hak untuk meminta akses dan mengoreksi data pribadi yang dipegang oleh otoritas pajak atau perusahaan, memastikan akurasi data yang digunakan dalam proses audit.
e) Entitas yang melakukan audit pajak harus dapat mendemonstrasikan kepatuhan terhadap PDPA, termasuk bagaimana mengumpulkan, menggunakan, dan melindungi data pribadi. Hal tersebut melibatkan menjaga catatan kegiatan pengolahan data dan menerapkan kebijakan privasi yang jelas.

2. Indonesia (Undang-Undang Perlindungan Data Pribadi (UU PDP))

Indonesia telah mengambil langkah besar dalam melindungi data pribadi melalui pengesahan Undang-Undang Perlindungan Data Pribadi (UU PDP). UU ini mengatur kerangka kerja yang komprehensif untuk pengolahan data pribadi, mirip dengan GDPR di Uni Eropa, mencakup berbagai aspek mulai dari pengumpulan hingga penghapusan data, serta menegaskan hak-hak subjek data.

UU PDP Indonesia mengatur pengumpulan, penggunaan, penyimpanan, dan penghapusan informasi pribadi, memberikan warga negara hak atas data dan menempatkan kewajiban pada pengendali dan pemroses data. Aplikasi UU PDP dalam Audit Pajak:

a) Sesuai dengan UU PDP, otoritas pajak dan auditor harus memastikan bahwa pengumpulan data pajak dari wajib pajak dilakukan dengan dasar konsen yang sah atau berdasarkan ketentuan hukum yang berlaku, memastikan bahwa wajib pajak diinformasikan dan menyetujui penggunaan data untuk tujuan audit.
b) Data pribadi yang dikumpulkan untuk keperluan audit pajak harus digunakan secara eksklusif untuk tujuan tersebut, sesuai dengan prinsip pembatasan tujuan yang ditetapkan dalam UU PDP. Auditor harus menghindari penggunaan data untuk tujuan lain tanpa konsen yang eksplisit dari subjek data.
c) Wajib pajak memiliki hak untuk diinformasikan tentang pengumpulan dan penggunaan data serta hak untuk meminta penghapusan data jika tidak lagi diperlukan atau jika pengumpulan datanya tidak didasarkan pada konsen. Auditor harus memfasilitasi hak-hak ini dan memastikan bahwa prosedur ada untuk menanggapi permintaan subjek data.
d) Otoritas pajak dan auditor wajib menerapkan tindakan keamanan untuk melindungi data pribadi dari akses tidak sah, kehilangan, atau kerusakan. Hal ini termasuk langkah-langkah teknis seperti enkripsi dan langkah-langkah administratif seperti kebijakan privasi dan pelatihan kesadaran keamanan untuk staf.

3. Malaysia (Personal Data Protection Act 2010 (PDPA))

PDPA Malaysia bertujuan untuk melindungi data pribadi individu yang diproses oleh organisasi komersial dan mengatur transfer data pribadi ke luar Malaysia. Act ini memerlukan organisasi untuk memperoleh konsen dari subjek data untuk pengolahan data pribadi dan menerapkan langkah-langkah keamanan yang tepat untuk melindungi data tersebut. Dalam audit pajak, penting bagi perusahaan untuk mematuhi PDPA dalam pengumpulan dan pengolahan data pajak. Berikut adalah penjelasan yang lebih spesifik tentang aplikasi PDPA dalam konteks audit pajak di Malaysia, berfokus pada kepatuhan dan praktik terbaik: Undang-undang ini dirancang untuk melindungi data pribadi individu yang diproses oleh organisasi dan entitas komersial di Malaysia, memberikan kerangka kerja bagi pengolahan data yang aman dan bertanggung jawab. PDPA menekankan pada pentingnya konsen subjek data, keamanan data, dan batasan terhadap pengungkapan data pribadi.

Aplikasi PDPA dalam Audit Pajak:

a) Sebelum mengumpulkan data pribadi wajib pajak, perusahaan dan auditor pajak harus memperoleh konsen eksplisit dari individu tersebut. Konsen eksplisit ini termasuk memberikan penjelasan yang jelas tentang tujuan pengumpulan data dan bagaimana data tersebut akan digunakan dalam konteks audit pajak.
b) PDPA mengharuskan organisasi untuk menerapkan tindakan keamanan fisik, teknis, dan administratif untuk melindungi data pribadi dari risiko kehilangan, penyalahgunaan, akses yang tidak sah, pengungkapan, perubahan, dan penghancuran. Hal

tersebut sangat relevan dalam audit pajak, di mana data keuangan dan pribadi yang sensitif sering kali diolah.

c) Perusahaan harus transparan tentang pengolahan data pribadi, termasuk menyediakan informasi kepada wajib pajak tentang hak di bawah PDPA dan bagaimana dapat mengakses atau mengoreksi data.

4. Filipina (Data Privacy Act of 2012)

Data Privacy Act di Filipina bertujuan untuk melindungi data pribadi individu yang disimpan dalam sistem informasi dan komunikasi. Act ini menciptakan Komisi Privasi Nasional untuk memantau dan memastikan kepatuhan terhadap act tersebut. Auditor pajak harus memastikan bahwa proses pengumpulan, penggunaan, dan penyimpanan data pajak wajib pajak sesuai dengan ketentuan Data Privacy Act (DPA) untuk menghindari pelanggaran. Berikut adalah penjelasan tentang aplikasi DPA dalam konteks audit pajak di Filipina:

a) Auditor pajak harus memastikan bahwa persetujuan diperoleh dari wajib pajak sebelum mengumpulkan data pribadi. Hal ini mencakup memberikan informasi yang jelas tentang tujuan pengumpulan data dan bagaimana data tersebut akan digunakan.
b) Data pribadi yang dikumpulkan untuk tujuan audit pajak harus digunakan secara eksklusif untuk tujuan tersebut. Penggunaan data di luar konteks yang telah disetujui tanpa persetujuan tambahan dapat dianggap sebagai pelanggaran.
c) DPA mengharuskan entitas, termasuk otoritas pajak dan perusahaan audit, untuk mengimplementasikan

tindakan keamanan yang memadai untuk melindungi data pribadi dari akses tidak sah, penggunaan, pengungkapan, pengubahan, kerusakan, atau kehilangan.

d) Wajib pajak memiliki hak untuk mengakses data pribadi yang disimpan dan meminta koreksi jika data tersebut tidak akurat. Auditor harus memastikan prosedur ada untuk memfasilitasi hak-hak ini.
e) National Privacy Commission (NPC) memantau kepatuhan terhadap DPA. Auditor dan perusahaan audit perlu memastikan bahwa kegiatan audit dan pengolahan data pajak mereka sesuai dengan pedoman yang ditetapkan oleh NPC untuk menghindari sanksi.

8.2 Dampak Efektivitas Cyber Security terhadap Kinerja Audit Pajak

Implementasi cyber security yang efektif berperan vital dalam memastikan efisiensi dan efektivitas audit pajak. Dengan membangun dan memelihara lingkungan teknologi informasi yang aman, auditor pajak dapat mengakses, menganalisis, dan memproses data pajak dengan cara yang lebih cepat dan lebih aman.

8.2.1 Efektivitas Cyber Security dalam meningkatkan Efisiensi dan Efektivitas Audit Pajak

Efektivitas cyber security dalam meningkatkan efisiensi dan efektivitas audit pajak dapat diukur melalui beberapa dimensi kunci yang mencakup aspek teknis,

prosedural, dan manusia. Sistem keamanan siber dianggap efektif jika memenuhi kriteria berikut:

1) Ketangguhan terhadap Serangan
    a) Sistem keamanan yang efektif mampu mendeteksi serangan atau upaya serangan sejak dini dan merespons dengan cepat untuk mencegah kerusakan atau kebocoran data. Sistem ini meliputi penerapan teknologi seperti Intrusion Detection Systems (IDS) dan Intrusion Prevention Systems (IPS).
    b) Kemampuan untuk pulih dari serangan dengan minimnya kerugian atau gangguan terhadap operasional merupakan indikator efektivitas. Hal ini mencakup rencana pemulihan bencana dan backup data yang teratur.
2) Pengelolaan Akses yang Ketat
    a) Sistem yang efektif menggunakan mekanisme otentikasi kuat dan manajemen akses berbasis peran untuk memastikan hanya pengguna yang berwenang yang dapat mengakses informasi.
    b) Proteksi fisik untuk perangkat keras dan infrastruktur TI, serta pengendalian akses logis ke sistem dan jaringan.
3) Enkripsi Data

    Penggunaan enkripsi canggih untuk melindungi data sensitif, baik saat disimpan (at rest) maupun saat ditransmisikan (in transit), memastikan bahwa data tidak dapat diakses atau dibaca oleh pihak yang tidak berwenang.

4) Pembaruan dan Pemeliharaan Sistem
    a) Untuk memastikan bahwa semua komponen sistem selalu diperbarui untuk melindungi terhadap kerentanan terbaru merupakan aspek penting dari keamanan siber yang efektif.
    b) Melakukan pengujian keamanan secara berkala, termasuk pengujian penetrasi dan scanning kerentanan, untuk menemukan dan mengatasi celah keamanan.
5) Kepatuhan terhadap Standar dan Regulasi
    a) Mengadopsi dan mematuhi standar keamanan siber internasional, seperti ISO/IEC 27001, menunjukkan komitmen terhadap keamanan siber yang efektif.
    b) Memastikan kepatuhan dengan regulasi keamanan data dan privasi lokal dan internasional, seperti GDPR atau PDPA, menunjukkan efektivitas perlindungan data.

Efisiensi audit pajak dan efektivitas cyber security adalah dua aspek yang saling terkait erat dalam era digital saat ini. Efisiensi audit pajak merujuk pada kemampuan audit untuk dilakukan dengan cara yang hemat waktu dan sumber daya, sementara tetap mencapai tujuan audit yang diinginkan, seperti akurasi dalam penilaian pajak dan kepatuhan terhadap peraturan pajak. Efektivitas cyber security, di sisi lain, merujuk pada kemampuan sistem keamanan untuk melindungi data dan sistem informasi dari ancaman siber, memastikan integritas, kerahasiaan, dan ketersediaan data.

1) Optimalisasi Akses Data
   Cyber security yang efektif memungkinkan auditor pajak untuk mengakses data wajib pajak yang dibutuhkan dengan cara yang aman dan cepat, melalui otentikasi dan otorisasi pengguna yang kuat. Penggunaan VPN dan enkripsi data memastikan bahwa akses remote ke database pajak dilindungi dari intersepsi dan penyalahgunaan.
2) Minimisasi Downtime
   Implementasi firewall, sistem deteksi intrusi, dan protokol keamanan lainnya membantu mencegah serangan DDoS dan ancaman lain yang dapat menyebabkan downtime sistem. Dengan meminimalkan downtime, cyber security memastikan bahwa data tersedia kapan saja dibutuhkan untuk audit, meningkatkan efisiensi proses audit.
3) Automasi Deteksi Ancaman
   Teknologi keamanan modern yang memanfaatkan kecerdasan buatan dan pembelajaran mesin dapat secara otomatis mendeteksi dan merespons ancaman siber secara real-time. Hal ini mengurangi beban kerja manual dalam memonitor keamanan sistem, memungkinkan auditor untuk fokus pada analisis data pajak.
4) Integritas Data
   Cyber security yang efektif memastikan integritas data dengan melindungi terhadap modifikasi data tidak sah. Mekanisme seperti blockchain dan digital signatures dapat memastikan bahwa data yang diakses dan dianalisis selama audit pajak belum diubah, meningkatkan kepercayaan pada hasil audit.

5) Membangun Kepercayaan
   Keamanan data yang efektif membangun kepercayaan antara otoritas pajak, wajib pajak, dan pemangku kepentingan lainnya. Ketika wajib pajak percaya bahwa informasi wajib pajak ditangani dengan aman, wajib pajak lebih cenderung untuk bekerja sama, mempermudah proses audit.
6) Mematuhi regulasi keamanan data dan privasi seperti GDPR atau PDPA menunjukkan komitmen terhadap perlindungan data. Kepatuhan ini tidak hanya menghindarkan dari denda dan sanksi tetapi juga memastikan bahwa proses audit dilakukan dalam kerangka kerja hukum yang jelas.

Efektivitas audit pajak dan efektivitas cyber security berperan penting dalam memastikan keadilan dan keakuratan dalam sistem perpajakan, serta melindungi integritas data dan sistem informasi pajak dari ancaman siber. Keduanya saling terkait dan saling mempengaruhi dalam banyak aspek operasional dan teknis audit pajak modern. Hubungan antara efektivitas audit pajak dan efektivitas cyber security:

1) Pengamanan Data dalam Proses Audit
   a) Cyber security memastikan bahwa data pajak yang sensitif dienkripsi, baik saat disimpan (at rest) maupun saat ditransmisikan (in transit). Hal ini melindungi data dari akses tidak sah, memastikan bahwa auditor dapat mengandalkan keutuhan data selama proses audit.
   b) Manajemen Akses: Penerapan kontrol akses berbasis peran memastikan bahwa hanya

auditor dan staf yang berwenang yang dapat mengakses data pajak. Teknik autentikasi kuat, seperti otentikasi multifaktor (MFA), meningkatkan keamanan akses ini.

2) Deteksi dan Pencegahan Penipuan Pajak
   a) Solusi cyber security yang memanfaatkan kecerdasan buatan (AI) dan machine learning dapat membantu dalam mendeteksi pola tidak biasa atau mencurigakan dalam data pajak yang mungkin menunjukkan upaya penipuan. Hal ini memungkinkan auditor untuk secara proaktif mengidentifikasi dan menyelidiki potensi masalah.
   b) Teknologi seperti blockchain dapat digunakan untuk memastikan integritas data transaksi pajak, membuat data lebih resisten terhadap modifikasi tidak sah dan memberikan audit trail yang jelas.
3) Kolaborasi dengan Pihak Ketiga.
   Dalam kasus audit pajak yang melibatkan pihak ketiga, seperti konsultan pajak atau penyedia layanan IT, efektivitas cyber security memastikan bahwa data pajak ditangani dengan aman, menjaga kepercayaan dan integritas selama proses audit.

8.2.2 Dampak Cyber Security Terhadap Efisiensi Dan Efektivitas Audit Pajak

Penerapan cyber security yang efektif dapat membawa dampak positif yang signifikan terhadap proses audit pajak, meningkatkan efisiensi dan efektivitas audit. Berikut beberapa cara penerapan cyber security berkontribusi positif:

1) Cyber security memastikan data pajak dilindungi dari akses tidak sah, manipulasi, dan pencurian, menjaga integritas data yang esensial untuk analisis dan keputusan audit yang akurat.
2) Dengan protokol keamanan yang kuat, auditor pajak dapat mengakses data yang dibutuhkan dengan cepat dan aman, tanpa khawatir akan intersepsi atau kebocoran data.
3) Sistem keamanan siber yang canggih memungkinkan deteksi dini aktivitas mencurigakan yang bisa menunjukkan adanya pelanggaran pajak, memungkinkan intervensi yang tepat waktu.
4) Mengetahui bahwa data mereka dilindungi dengan baik meningkatkan kepercayaan wajib pajak terhadap sistem pajak, yang dapat mendorong kepatuhan pajak yang lebih baik.
5) Automasi dan teknologi keamanan siber dapat mengurangi waktu dan biaya yang terkait dengan audit pajak, meningkatkan efisiensi operasional dan memungkinkan alokasi sumber daya yang lebih efektif.

Sementara manfaat cyber security bagi proses audit pajak tidak diragukan lagi, terdapat pula dampak negatif potensial yang perlu diperhatikan, terutama terkait dengan protokol keamanan yang ketat:

1) Protokol keamanan yang sangat ketat dapat memperlambat proses pengambilan dan pemrosesan data, mengakibatkan penundaan dalam pelaksanaan audit pajak.
2) Tingkat keamanan yang tinggi sering kali memerlukan prosedur yang kompleks dan memakan waktu, menambah beban kerja auditor dan potensial mengurangi efisiensi operasional.
3) Batasan keamanan dapat mempersulit berbagi data antar tim atau dengan pihak luar, yang diperlukan untuk analisis atau keperluan audit yang komprehensif.
4) Pengaturan keamanan yang ketat dapat membatasi akses ke data penting, terkadang bahkan bagi auditor yang memerlukannya, menimbulkan hambatan dalam pemeriksaan dan analisis data.

REFERENSI

Abomhara, M., & Koien, G. M. (2015). Cyber Security and The Internet of Things: Vulnerabilities, Threats, Intruders And Attacks. Journal of Cyber Security and Mobility, Vol 4, pp: 65-88. *River Publishers.* DOI: 10.13052/jcsm2245-1439.414

Alfred J. Menezes, Paul C. Van Oorschot, & Scott A. Vanstone. (2018). Handbook of Applied Cryptography.

Ali, W. A. (2019). Effects of Business Intelligence on The Continuous Auditing Process. International Journal of Innovative Science and Research Technology (IJISRT), 4(3), 377–383.

Amos, Z., (2022). Top 8 Common Cyber security Weaknesses in Businesses - Cyber security Magazine. [online] Cyber security Magazine. Available at: <https://Cyber security-magazine.com/top-8-common- Cyber security-weaknesses-in-businesses/.

A. Al Mamun, K. Salah, S. Al-maadeed, & T.R. Sheltami. (2017). Bigcrypt for big data encryption, in Software Defined Systems (SDS). Fourth International Conference on, pp. 93–99, 2017.

Backer (2022). KPMG. Cybersecurity risks in the financial statement audit https://kpmg.com/be/en/home/insights/2022/06/de-cybersecurity-risks-in-the-financial-statement-audit.html

Baitha, A., & Vinod, S. (2018). Session Hijacking and Prevention Technique. International Journal of Engineering & Technology, 7(2.6), 193-198. https://doi.org/10.14419/ijet.v7i2.6.10566.

Bean, R., & Davenport, T.H. (2019). The AI Advantage: How to Put the Artificial Intelligence Revolution to Work. MIT Press.

Benjamin, A., & Hamilton, G,. (2009). Detecting Man-in-the-Middle Attacks by Precise Timing. 2009 Third International Conference on Emerging Security Information, Systems and Technologies, 18–23 June. https://ieeexplore.ieee.org/abstract/document/5211025.

Berberich, G. (2005). The effects of audit methodology and audit experience on the development of auditors' knowledge of the client's business (Unpublished PhD dissertation). University of Waterloo, Ontario, Canada. Retrieved from http://hdl.handle.net/10012/740

Board International. Business Intelligence for the office of finance. Retrieved from https://www.board.com/en/document/business-intelligence-finance-ebook.

Brender, N., & Gauthier, M. (2018). Impacts of blockchain on the auditing profession. ISACA Journal, 5, 27-32.

Calderon, T., Melanie G., McCoskey C. O. (2021). Journal of Forensic and Investigative Accounting Volume 13: Issue 1, January–June, Toward a Protocol for Tax Data Security

Callegati, F., Walter C., & Marco, R,.. (2009). Man-in-the-Middle Attack to the HTTPS Protocol." *IEEE Explore,* 7(1), 78–81.

Ca´rdenas, A.A., Manadhata, P.K., & Rajan, S. (2013). Big Data Analytics For Security Intelligence. University of Texas at Dallas@ Cloud Security Alliance, pp. 1–22, 2013

Cavelty, M. D. (2012). The Militarisation of Cyber Security as a Source of Global Tension. *Strategic Trends.*

Chaudhuri, S., Dayal, U., & Narasayya, V. (2011). An overview of business intelligence technology. Communications of the ACM, 54(8), 88–98.

Chen, H., Chiang, R.H.L., & Storey, V.C. (2012). Business Intelligence and Analytics: From Big Data to Big Impact. MIS Quarterly, 36(4), 1165-1188.

Chen, C.J.P., Srinidhi, B. & Su, X. (2014). Effect of auditing: Evidence from variability of stock returns and trading volume. China Journal of Accounting Research, 7(4), 223–245.

Cisco. Internet of Things (IoT). Retrived from http://www.cisco.com/web/solutions/trends/iot/portfolio.html.

Clay K. W., Wynn, D., Madupalli, R., Karahanna, E., & Duncan, B. K.. (2014). Explaining Users' Security Behaviors with the Security Belief Model. *Journal of Organizational & End User Computing* 26 (3), 23–46. https://doi.org/10.4018/joeuc.2014070102. http://ezproxy.uakron.edu:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&

AN=990 91907&site=ehost-live. Accessed February 8, 2020.

Cohen, M., Rozario, A., & Zhang, C. (A.) (2019). Exploring the use of robotic process automation (RPA) in substantive audit procedures. The CPA Journal, 89(7), 49–53.

Craigen, D., Diakub-Thibault, N., & Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review, 4*(10).

Crespo, B.G.N., & Garwood, A. (2014). Fighting Bot Nets With Cyber-Security Analytics: Dealing With Heterogeneous Cyber-Security Information In New Generation Siems. Availability, Reliability and Security (ARES), 2014 Ninth International Conference on, pp. 192–198.

Cole, E,. (2021). Cyber Crisis: Protecting Your Business from Real Threats in the Virtual World. Hardcover.

Cui, H.T,. (2016). Research on The Model of Big Data Serve Security in Cloud Environment. Computer Communication and the Internet (ICCCI), 2016 IEEE International Conference on, pp. 514–517.

Danda B. R,. Cybersecurity in Big Data Era: From Securing Big Data to Data-Driven Security *Senior Member, IEEE*, Ronald Doku and Moses Garuba. Retrieved from: https://par.nsf.gov/servlets/purl/10094358

Davenport, T.H., & Harris, J. (2017). Competing on Analytics: The New Science of Winning (Updated Edition). Harvard Business Review Press.

Davenport, T.H. (2013). Analytics at Work: Smarter Decisions, Better Results.

Davis, G. A., & Woratschek, C. R. (2015). Evaluating business intelligence/business analytics software for use in the information systems curriculum. Information Systems Education Journal, 13(1), 23.

Deloite (2017). Cybersecurity and The Role of Internal Audit. An Urgent Call To Action. Retrieved from: https://www2.deloitte.com/us/en/pages/risk/articles/cybersecurity-internal-audit-role.html/#:~:text=,audit

Duan, L., & Xu, L. D. (2012). Business Intelligence for Enterprise Systems: A Survey. IEEE Transactions on Industrial Informatics, 8(3), 679–687.

Eaton, Grenier, & Layman. (2019). Accounting and Cybersecurity Risk Management. Current Issues In Auditing American Accounting Association. Vol. 13, No. 2 Fall 2019. pp. C1–C9 . DOI: 10.2308/ciia-52419

EMC2. (2015). New EMC Innovations Redefine IT Performance and Efficiency. Retrieved from: http://www.emc.com/about/news/press/2015/20150504-01.htm.

European Court of Auditors. (2020). Smart Audit: The Digital Transformation of Audit. ECAjournal. Retrieved from https://medium.com/ecajournal/smart-audit-the-digital transformation-of-audit-b283e1653bd4

Evelson, B. (2020). The Forrester Wave™: Business Intelligence Platforms, Q3 2020. Forrester Research.

Fatima, H., Satpathy,S., Mahapatra, S., Dash, G., & Pradhan, S.K.,. (2017). Data fusion & visualization application for network forensic investigation-a case study, in *Anti-Cyber Crimes (ICACC), 2017 2nd International Conference on*, pp. 252–256.

Few, S. (2009). Now You See It: Simple Visualization Techniques for Quantitative Analysis. Analytics Press.

Gai, K., Qiu, M. & Elnagdy, S. A,. (2016). A Novel Secure Big Data Cyber Incident Analytics Framework for Cloud-Based Cybersecurity Insurance in Big Data Security on Cloud (BigDataSecurity). IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference on, pp. 171–176.

Gardikis, G., Tzoulas, K., Tripolitis, K., Bartzas, A., Costicoglou, S. Lioy, A., Gaston, B., Fernandez, C. Davila, C., Litke, A. (2017). Shield: A Novel Nfv-Based Cybersecurity Framework. Network Softwarization (NetSoft), *2017 IEEE Conference on*, pp. 1–6.

George A. A., (1970). The Market for 'Lemons': Quality Uncertainty and the Market Mechanism,' The Quarterly Journal of Economics 84: 488-500.

Gołębiowska, A., Jakubczak, W., Prokopowicz, D., Jakubczak, R. (2021). Cybersecurity of Business Intelligence Analytics Based on the Processing of Large Sets of Information with the Use of Sentiment Analysis and Big Data. *European Research Studies Journal Volume XXIV, Issue 4, 2021. pp. 850-871*

Gottwalt, F., & Karduck, A.P,. (2015). Simin Light of Big Data, *Innovations in Information Technology (IIT), 2015 11th International Conference on*, pp. 326–331.

Han, J., Pei, J., & Kamber, M. (2011). Data Mining: Concepts and Techniques. Morgan Kaufmann Publishers.

Harrison, R., Parker, A., Brosas, G., Chiong, R., & Tian, X. (2015). The role of technology in the management and exploitation of internal business intelligence. Journal of Systems and Information Technology, 17(3), 247–262.

Hashem, I. A. T. et al., (2016). The Role Of Big Data In Smart City. *Int J Inf Manage*, vol. 36, no. 5, pp. 748-758.

Hirsch, D. D,. (2013). The glass house effect: Big Data, the new oil, and the power of analogy, *Me. L. Rev*., vol. 66, p. 373.

Huang, F., & Vasarhelyi, M. A. (2019). Applying robotic process automation (RPA) in auditing: A framework. International Journal of Accounting Information Systems, 35, 100433.

Inmon, W. H. (2005). Building the Data Warehouse. John Wiley & Sons.

International Telecommunications Union (ITU) estimate: Wikipedia, 'Global Internet Usage,' https://en.wikipedia.org/wiki/ Global_Internet_usage.

Iqbal, R. F., Doctor, B. M., Mahmud, S., & Yousuf, U., (2018). Big data analytics: computational intelligence techniques and application areas. Technol Forecast Soc Change, pp. 119253.

IRS (2021) https://www.irs.gov/pub/irs-pdf/p4557.pdf

IRS (2021) p5293. https://www.irs.gov/pub/irs-pdf/p5293.pdf

IRS. (2023).Tax Security 2.0: The Taxes-Security-Together Checklist. Retrieved from: https://www.irs.gov/tax-profesionals/tax-security-2-point-0-the-taxes-security-together-checklist.

Islam, M. R., Habiba, M., & Kashem, M. I. I,. (2017). A framework for Providing Security to Personal Healthcare Records. Networking, Systems and Security (NSysS). International Conference on, pp. 168–173.

Johannes M. B., & Van Eeten, M., J., G. Cybersecurity: Stakeholder Incentives, Externalities, and Policy Options.

Kamordzhanova, N., & Selezneva, A. (2019). The Impact Of The Digital Economy on Accounting, Reporting and Audit. Advances in Economics, Business and Management Research, 79. Proceedings of the International Science and Technology Conference "Far East Con", 228–230.

Kascelan, L. (2011). Advantages and limitations in implementation of business intelligence system in Montenegro: Case study Telenor Montenegro. Economic Review: Journal of Economics and Business, 9(2), 19-30.

Kasper, M., Rablen., M.D. (2023). Tax compliance after an audit Higher or lower?. Journal of Economic Behavior and Organization. 157–171 https://doi.org/10.1016/j.jebo.2023.01.013. Elsevier

B.V. The CC BY license (http://creativecommons.org/licenses/by/4.0/)

Kaur, K., Syed, A., Mohammad, A., & Halgamuge, M. N. (2017). An Evaluation Of Major Threats In Cloud Computing Associated With Big Data. Big Data Analysis (ICBDA), 2017 IEEE 2nd International Conference on, pp. 368–372.

Kepner, J., Gadepally, V., Michaleas, P., Schear, N., Varia, M., Yerukhimovich, A., & Cunningham, R.K. (2014). Computing on Masked Data: A High Performance Method for Improving Big Data Veracity. High Performance Extreme Computing Conference (HPEC), *2014 IEEE*, pp. 1–6.

Kimball, R., & Ross, M. (2013). The Data Warehouse Toolkit: The Definitive Guide to Dimensional Modeling. John Wiley & Sons.

Kompas. (2021). https://money.kompas.com/read/2021/10/26/173828526/imbas-kejahatan cyber-bank-bank-dunia-merugi-rp-1420-triliun-per-tahun

Kurose, J.F., & Ross, K. W,. (2010). "Computer Networks: A Top-Down Approach. Pearson.

Laudon, K.C., & Laudon, J.P. (2016). "Management Information Systems: Managing the Digital Firm."

Le, D. C., Zincir-Heywood, A. N., & Heywood, M. I. (2016). Data Analytics On Network Traffic Flows For Botnet Behaviour Detection. Computational Intelligence (SSCI), 2016 IEEE Symposium Series on, pp. 1–7.

Lee, N.Y. & Wu, B.H. (2017). Privacy Protection Technology and Access Control Mechanism for Medical Big Data. 2017 6th IIAI International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 424–429.

Liu, C., Cai, Y., & Wang, Y. (2016). Security Evaluation of Rc4 Using Big Data Analytics. Software Engineering and Service Science (ICSESS), 2016 7th IEEE International Conference on, pp. 316–320.

Marr, B. (2015). Big Data: Using SMART Big Data, Analytics and Metrics To Make Better Decisions and Improve Performance. John Wiley & Sons.

Matthew, T. (2003). *IP Spoofing: An Introduction*. Symantec Press.

Maurer & Nelson (2021). The Global Cyber Threat. Retrieved from https://www.imf.orf/en/Publications/fandd/issues/2021/03/global-cyber-threat-to-financial-systems-maurer.

Mayer-Schönberger, V., & Cukier, K. (2014). Big Data: A Revolution That Will Transform How We Live, Work and Think.

McClure, S., Scambray, J., & Kurtz, G. (2005). **Hacking Exposed: Network Security Secrets & Solutions.** McGraw-Hill. 2005

Mengke, Y., Xiaoguang, Z., Jianqiu, Z., & Jianjian, X,. (2016). Challenges and Solutions of Information Security Issues in The Age of Big Data. China Communications, vol. 13, no. 3, pp. 193–202.

Miloslavskaya, N., Tolstoy, A., & Zapechnikov, S. (2016). Taxonomy for Unsecure Big Data Processing In Security Operations Centers. Future Internet of Things and Cloud Workshops (FiCloudW), IEEE International Conference on, pp. 154–159.

Miloslavskaya, N. (2017). Security Intelligence Centers for Big Data Processing, Future Internet of Things and Cloud Workshops (FiCloudW), 2017 5th International Conference on, pp. 7–13.

Miniard, P, & Cohen, J. (1981). An Examination of The Fishbein–Ajzen Behavioral-Intention Model's Concepts and Measures. Journal of Experimental Social Psychology, 17, 309-339. https://doi.org/10.1016/0022-1031(81)90031- 7. Accessed February 8, 2020.

Mőckli. (2012). Zurich: Center for Security Studies. Retrieved from: http://papers.ssrn.com/sol3/papers.cfm?abstract_id =2007043.

Murali, R. S. (2010). Business intelligence as internal audit tool. UAE Internal Audit Association, 15, 1-5.

Murillo, J. (2024). US Multinational Entities (MNEs) Cannot Afford To Sit On The Sidelines. Retrived from: https://www.ey.com/en_us/tax/beps-pillar-two-as-policies-evolve-engagement-is-key

Niagahoster (2023). Retrieved from: https://www.niagahoster.co.id/blog/cyber-security

OECD. Tax Administration. (2022). Retrieved from: https://www.oecd-ilibrary.org/sites/1e797131-

en/1/3/6/index.html?itemId=/content/publication/1e797131
en&_csp_=38baa8bc2bc68a4be5b070db809f1650&itemIGO=oecd&itemContentType=book

Popa, M., & Toma, C. (2009). Stages for the development of the audit processes of distributed informatics systems. Journal of Applied Quantitative Methods, 4(3), 359–371.

Provost, F., & Fawcett, T. (2013). Data Science for Business: What You Need to Know about Data Mining and Data-Analytic Thinking. O'Reilly Media. Retrived from: https://www.sgstechnologies.net.

Puri, C., & Dukatz, C. (2015). Analyzing and Predicting Security Event Anomalies: Lessons Learned From A Large Enterprise Big Data Streaming Analytics Deployment. Database and Expert Systems Applications (DEXA), 2015 26th International Workshop on, pp. 152–158, 2015.

Raja, M. C., & Rabbani, M. A.. (2014). Big Data Analytics Security Issues In Data Driven Information System. *IJIRCCE*, vol. 2, no. 10.

Reddy, G. N., & Reddy, G. J. (2014). A Study Of Cyber Security Challenges And Its Emerging Trends on Latest Technologies. *arXiv preprint arXiv:1402.1842*.

Rezaee Z., Elam, R., & Sharbatoghlie, A. (2001). Continuous auditing: the audit of the future. Managerial Auditing Journal ,16(3), 150–158.

Rittinghouse & Ransome. (2010). Cloud Security: A Comprehensive Guide to Secure Cloud Computing. Wiley Publishing Inc.

Saenko, I., Kotenko, I., & Kushnerevich, A. (2017). Parallel Processing of Big Heterogeneous Data For Security Monitoring Of IoT Networks. Parallel, Distributed and Network-based Processing (PDP), 2017 25th Euromicro International Conference on, pp. 329–336.

Schiliro, F. (2022). Towards a Contemporary Definition of Cybersecurity. https://arxiv.org/pdf/2302.02274.pdf

Seemma, P. S., Nandhini, S., & Sowmiya, M. (2018). Overview of cyber security. *International Journal of Advanced Research in Computer and Communication Engineering, 7*(11), 125-128.

Shea, S., Gills, A. S., & Clark, C. (n.d.). (2022). What is cybersecurity? (TechTarget) Retrieved October 2022, from TechTarget:

Siegel, E. (2016). Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, or Die. John Wiley & Sons.

Soceanu, A., Vasylenko, M., Egner, A., & Muntean, T,. (2015). Managing the privacy and security of ehealth data. Control Systems and Computer Science (CSCS), 20th International Conference on, pp. 439–446, 2015.

Stallings, W. (2003). *Network Security Essentials: Applications and Standards*. 2nd ed. Upper Saddle River, NJ: Pearson.

Stallings, W. (2017). Cryptography and Network Security: Principles and Practice.. Pearson.

Stanciu, A., Mihai F., & Aleca, O. (2009). Business intelligence: Trends and evolutions in applications development. Audit Financiar, 7(6), 15-22.

Statistics from Internet Live Stats, 'Internet Users,' http://www.internetlivestats.com/internet-users/.

Telecommunications Policy 33. (2009): 706-719; and Eric Luiijf, et al, 'Ten National Cyber Security Strategies: A Comparison,' in Critical Information Infrastructure Security: 6th International Workshop, CRITIS 2011, Lucerne, Switzerland, September 8-9, 2011, Revised Selected Papers, ed. Sandro Bologna et al. (Springer-Verlag Berlin Heidelberg, 2013), 1-17.

Trigo, A., Belfo, F., & Estébanez, R. P. (2014). Accounting information systems: The challenge of the real-time reporting. Procedia Technology, 16, 118-127.

Urwin, M., (2023). Business Intelligence Applications and Examples to Know Companies in sectors from tech to fashion are making more data-driven decisions. Retrived from: https://builtin.com/big-data/business-intelligence-examples-applications.

Valeur, F., Vigna, G., Kruegel, C., Kemmerer, R., A. (2004). A comprehensive approach to intrusion detection alert correlation. IEEE Transactions on Dependable and Secure Computing, Vol. 1, NO. 3.

Verma, J. P., Agrawal, S., Patel, B., & Patel, A. (2016). Big data analytics: Challenges and applications for text, audio, video, and social media data, *Int. J. on Soft Comput.,*

Artif. Intell. and Appl. (IJSCAI), vol. 5, no. 1, pp. 41-51, 2016.

Vishik, C., Rajan, A., Ramming, C., Grawrock, D., & Walker, J. (2011). Defining Trust Evidence: Research Directions. Proceedings of the Seventh Annual Workshop on Cyber Security and Information Intelligence Research (CSIIRW '11), Frederick T. Sheldon, Robert Abercrombie, and Axel Krings, eds. (ACM: New York).

Vishik, C., Sheldon, F., & Ott, D,. (2013). Economic Incentives for Cybersecurity: Using Economics to Design Technologies Ready for Deployment. *ISSE 2013 Securing Electronic Business Processes*, eds. Helmut Reimer, Norbert Pohlmann and Wolfgang Schneider (Springer Vieweg, 2013), 133-147.

Webb, L. R. (2012). Business intelligence in audit. International Journal of Business Intelligence Research, 3(3), 42–53.

Whitman, M. E., & Mattord, H. J. (2014). Information Security: A Comprehensive Handbook.

William, R. C., & Bellovin, S. M. (2003). Firewalls and Internet Security: Repelling the Wily Hacker. Addison-Wesley Professional Computing Series.

Wong, M. W. (2007). Cyber-trespass and 'unauthorized access' as legal mechanisms of access control: Lessons from the US experience. *International Journal of Law and Information Technology, 15*(1), 90-128.

Wong, S., & Venkatraman, S. (2015). Financial accounting fraud detection using business intelligence. Asian Economic and Financial Review, 5(11), 1187-1207.

Xu, G., Ren, Y., Li, H., Liu, D., Dai, Y., & Yang, K. "Cryptmdb: A Practical Encrypted Mongodb Over Big Data. Communications (ICC), 2017 IEEE International Conference on, pp. 1–6.

Yao, Y., Zhang, L., Yi, J., Peng, Y., Hu, W., & Shi, L. (2016). A Framework For Big Data Security Analysis And The Semantic Technology. *IT Convergence and Security (ICITCS), 2016 6th International Conference on*, pp. 1–4.

Zorabedian, J. (2019). "Cybercriminals Spoof Major Accounting and Payroll Firms in Tax Season Malware Campaigns." *Security Inteligence*, 2019/04/08. https://securityintelligence.com/cybercriminals-spoof-major- accounting-and-payroll-firms-in-tax-season-malware-campaigns/. Accessed June 18, 2020.

Zraqat, O. M. (2020). The moderating role of business intelligence in the impact of big data on financial reports quality in Jordanian Telecom Companies. Modern Applied Science, 14(2), 71-85.

Zuca, M., & Tinta, A. (2018). The contribution of computer assisted auditing techniques (CAAT) and of the business intelligence instruments in financial audit. Academic Journal of Economic Studies, 4(1), 183-191.

*Sin*Di era digital yang bergerak cepat, audit pajak menghadapi tantangan baru yang kompleks dan dinamis, khususnya dari perspektif keamanan siber. Monograf ini membahas pentingnya integrasi keamanan siber dalam proses audit pajak, menyoroti bagaimana teknologi informasi dan komunikasi telah mengubah lanskap keamanan dan manajemen data dalam audit pajak. Dengan meningkatnya insiden keamanan siber, perlindungan data sensitif dan sistem informasi menjadi prioritas utama dalam memastikan integritas dan kepercayaan publik dalam proses audit. Monograf ini mengeksplorasi bagaimana Compliance Risk Management (CRM), Big Data Analytics (BDA), dan Business Intelligence (BI) dapat dilindungi dari risiko keamanan siber dan dimanfaatkan untuk meningkatkan efisiensi dan efektivitas audit pajak. Melalui analisis literatur dan studi kasus, monograf ini mengidentifikasi dan mengevaluasi strategi mitigasi untuk mengatasi tantangan keamanan siber, serta merumuskan rekomendasi kebijakan untuk mengembangkan kerangka kerja keamanan siber yang berorientasi pada hasil analitik dari BDA, BI, dan CRM.

Monograf ini juga menyelidiki bagaimana sistem Business Development Analytics (BDA) dan Business Intelligence (BI) saat ini dilindungi dari risiko keamanan siber, serta mengidentifikasi potensi kerentanan yang dimanfaatkan dalam audit pajak. Pengembangan strategi mitigasi BDA, BI, dan CRM untuk meningkatkan keamanan siber dan integritas audit pajak menjadi fokus utama, dengan tujuan membangun kepercayaan publik dan meningkatkan efisiensi operasional dalam audit pajak. Dengan memahami dampak isu keamanan siber terhadap kinerja audit pajak, monograf ini menyediakan wawasan berharga tentang pentingnya teknologi canggih dan keamanan siber dalam era konektivitas. Integrasi efektif antara audit pajak dan keamanan siber memungkinkan otoritas pajak untuk melindungi data finansial dan memastikan kepatuhan terhadap beragam regulasi dan standar keamanan, memperkuat integritas dan kepercayaan publik dalam proses audit pajak. Dengan pendekatan multidisiplin dan analisis, monograf ini menggarisbawahi perlunya strategi responsif dan adaptif dalam cybersecurity untuk menanggapi kompleksitas dan dinamisme lingkungan teknologi yang terus berkembang. Dalam menghadapi ancaman siber yang meningkat, pembauran komponen siber dan fisik dalam audit pajak global memerlukan kolaborasi antar-agensi dan investasi yang signifikan dalam inovasi keamanan siber untuk meningkatkan efisiensi audit pajak.

Profil Penulis

Siti Kurnia Rahayu
DPK di UNIKOM Bandung

2024

UNIKOM
UNIKOM PRESS

ISBN 978-602-18602-7-4

9 786021 860274