e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

URGENSI PENERAPAN ISO 27001 PADA PERBANKAN SYARIAH DI INDONESIA

Abdul Rahman[1], Fachrurozi[2], Safitri[3]
Sekolah Tinggi Agama Islam Binamadani[1,2,3]
Ashrafalirahman2019@gmail.com[1], fachrurozi504@gmail.com[2], safitri@stai-binamadani.ac.id[3]

ABSTRAK

Penelitian ini bertujuan untuk mengelaborasi pentingnya penerapan ISO 27001 tentang sistem manajemen keamanan informasi untuk kalangan industri perbankan syariah di Indonesia. Implementasi ISO 27001 pada industri perbankan syariah sangatlah penting agar industri yang sedang berkembang pesat di Indonesia ini bisa mengantisipasi dan terhindar dari bahaya serangan *cyber* yang tentunya akan merugikan banyak pihak utamanya nasabah dari bank syariah itu sendiri. Penelitian ini berjenis kualitatif dengan menggunakan pendekatan studi pustaka. Sumber data penelitian ini menggunakan sumber data primer dan sekunder yang terdiri dari artikel, buku dan dokumen terkait perbankan syariah serta ISO 27001. Hasil penelitian ini menunjukan, bahwa: 1) Penerapan ISO 27001 tentang sistem manajemen keamanan informasi bagi industri perbankan syariah di Indonesia sangatlah penting dalam menjaga imunitas sistem keamanan informasi di bank syariah; 2) Melalui pendekatan berbasis risiko, bank syariah dapat melindungi aset informasi, menjaga keamanan fisik dan personel, serta mengelola akses ke sistem informasi; 3) ISO 27001 mendorong pengawasan dan perbaikan terus-menerus dan dengan mengimplementasikan standar ini bank syariah dapat meningkatkan keamanan informasi dan melindungi informasi penting mereka dengan lebih efektif; 4) Bank syariah yang mematuhi standar yang diakui secara internasional ini menunjukkan dedikasinya dalam melindungi data sensitif dan menjaga kepatuhan terhadap peraturan, serta menanamkan kepercayaan pada klien dan pemangku kepentingan.

Kata Kunci: *Perbankan Syariah, ISO 27001, Sistem Manajemen, Keamanan Informasi*

Abstract: *This study aims to elaborate the importance of implementing ISO 27001 on information security management system for the Islamic banking industry in Indonesia. The implementation of ISO 27001 in the Islamic banking industry is very important so that this rapidly growing industry in Indonesia can anticipate and avoid the danger of cyber attacks which will certainly harm many parties, especially customers of Islamic banks themselves. Penelitian ini berjenis kualitatif dengan menggunakan pendekatan studi pustaka. Sumber data penelitian ini menggunakan sumber data primer dan sekunder yang terdiri dari artikel, buku dan dokumen terkait perbankan syariah serta ISO 27001. Hasil penelitian ini menunjukan, bahwa: 1) The implementation of ISO 27001 on information security management system for the Islamic banking industry in Indonesia is very important in maintaining the immunity of information security systems in Islamic banks; 2) Through a risk-based approach, Islamic banks can protect information assets, maintain physical and personnel security, and manage access to information systems; 3) ISO 27001 encourages continuous supervision and improvement and by implementing this standard Islamic banks can improve information security and protect their important information more effectively; 4) Islamic banks that adhere to these internationally recognized standards demonstrate their dedication to protecting sensitive data and maintaining regulatory compliance, as well as instilling trust in clients and stakeholders*.

Keywords: *Islamic Banking, ISO 27001, Management System, Information Security*

PENDAHULUAN

Industri perbankan syariah memainkan peran penting dalam perekonomian nasional, oleh karenanya beragam strategi dilakukan banyak pihak utamanya pemerintah dalam hal ini otoritas jasa keuangan dalam mengembangkan industri tersebut. Sebagaimana diungkap otoritas jasa keuangan bahwa perkembangan industri

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

perbankan syariah di Indonesia begitu impresif yang mencapai rata-rata pertumbuhan aset lebih dari 65% pertahun dalam lima tahun terakhir.[1]

Perkembangan tersebut perlu dibarengi dengan perhatian serius terhadap ketahanan keamanan data dan informasi yang menjadi faktor kritis bagi perbankan syariah utamanya di era digital seperti saat ini. Terlebih lagi ancaman keamanan *cyber* semakin meningkat, dengan serangan terbaru terhadap Bank Syariah Indonesia (BSI) yang menjadi sorotan publik.[2] Namun di sisi lain kejadian ini memperkuat argumen pentingnya implementasi standar keamanan informasi seperti ISO 27001 dalam industri perbankan syariah di Indonesia.

Teknologi informasi kini telah berkembang dengan pesat dan telah membawa dunia memasuki era informasi yang serba cepat dan akurat. Tentu dengan cepat tersebarnya informasi ke jenjang dunia, keamanan dan kerahasiaan dari sebuah data pun patut untuk diperhatiakan. Keamanan informasi yang dimaksud dapat berupa data konsumen, data perusahaan, maupun data dari sebuah bank. Apabila data nasabah dari sebuah bank disalahgunakan, maka tidak hanya nasabah yang merugi, tetapi kualitas dari bank tersebut juga akan diragukan oleh nasabah lain. Maka dari itu keamanan dari data perlu untuk dijaga kerahasiaannya agar tidak disalahgunakan.[3]

Sebagai tulang punggung sistem keuangan global, sektor perbankan menghadapi banyak tantangan dalam melindungi data sensitif dan memastikan keamanan informasi. ISO 27001 menawarkan kerangka kerja komprehensif untuk membangun, menerapkan, memelihara, dan terus meningkatkan Sistem Manajemen Keamanan Informasi (ISMS) bank. Dengan mengikuti sertifikasi yang diakui secara internasional ini, bank syariah dapat memperkuat pertahanan mereka terhadap ancaman dunia maya, menunjukkan komitmen untuk melindungi informasi pelanggan, dan menjaga kepatuhan terhadap peraturan.

ISO 27001 mengatasi tantangan keamanan unik pada sektor perbankan melalui pendekatan berbasis risiko, memungkinkan bank untuk mengidentifikasi dan memprioritaskan potensi ancaman. Kerangka kerja ekstensif ini mencakup aspek-aspek penting seperti manajemen aset, kontrol akses, dan perencanaan respons insiden. Menerapkan langkah-langkah ini dalam ISMS mereka memungkinkan lembaga keuangan untuk memitigasi risiko secara efektif, meningkatkan postur keamanan informasi secara keseluruhan, dan memastikan kepatuhan terhadap peraturan industri.

Komponen utama ISO 27001 adalah penekanannya pada perbaikan berkelanjutan dan audit rutin, untuk memastikan bank tetap waspada dalam upaya keamanan informasi mereka. Pendekatan dinamis ini menumbuhkan budaya ketahanan, memungkinkan lembaga keuangan beradaptasi terhadap ancaman yang muncul dan kemajuan teknologi sambil tetap menjaga langkah-langkah keamanan yang kuat. Oleh karena itu, ISO 27001 merupakan kerangka kerja yang sangat diperlukan bagi sektor perbankan, yang menyediakan alat yang diperlukan untuk menjaga data sensitif dan menjunjung tinggi kepercayaan nasabah di dunia yang semakin digital.[4]

---

[1] Lihat: https://ojk.go.id/id/kanal/syariah/Pages/Perbankan-Syariah.aspx. Juga: https://ojk.go.id/id/kanal/syariah/tentang-syariah/ Pages/Perbankan-Syariah.aspx. Diakses pada Tanggal 2 Januari 2024.

[2] Lihat: https://www.bbc.com/indonesia/articles/cn01gdr7eero. Diakses pada Tanggal 5 Januari 2024.

[3] Aan Ansori, "Sistem Informasi Perbankan Syariah", *Jurnal Banque Syar'i,* Vol. 4 No. 1 Juli-Desember 2018, h. 183. DOI: 10.32678/bs.v4i2.1131

[4] Lihat: https://www.isms.online/sectors/iso-27001-for-the-banking-sector/. Diakses pada tanggal 5 Januari 2024.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

Lembaga keuangan yang menggunakan kerangka ISO 27001 telah mengalami peningkatan signifikan dalam langkah-langkah keamanan informasi mereka, yang secara efektif melindungi data sensitif pelanggan. Penerapan standar yang kuat ini akan meningkatkan postur keamanan mereka dan menunjukkan dedikasi mereka dalam menjaga kepercayaan klien dan mematuhi peraturan industri yang ketat. Ketergantungan sektor perbankan pada ISO 27001 menunjukkan komitmennya untuk menjaga lingkungan yang aman di tengah lanskap digital yang terus berkembang dan dipenuhi ancaman siber. Dengan adanya penerapan standar ISO 27001, perusahaan dalam hal ini bank syariah dapat menghidari kemungkinan besar ancaman keamanan seperti tindak perusakan atau terorisme, kebakaran, pencurian, *hacking*, dan kesalahan penggunaan informasi.

METODE PENELITIAN

Metode yang digunakan dalam penelitian ini adalah metode kualitatif deskriptif dengan pendekatan studi pustaka (*library research*). Oleh sebab itu, kajian dari penelitian ini didasari pada tinjauan literatur serta referensi-referensi terkait yang relevan dengan objek penelitian ini. Objek penelitian yang dimaksud berupa buku-buku dan artikel jurnal terkait perbankan syariah, ISO 27001 dan sistem manajemen keamanan informasi serta sumber-sumber pendukung lainnya. Dengan penggunaan metode ini, dapat diperoleh pemahaman yang mendalam dan komprehensif mengenai pentingnya penerapan ISO 27001 tentang sistem manajemen keamanan informasi pada industri perbankan syariah di Indonesia. Sehingga penelitian ini diharapkan bisa berkontribusi baik secara praktis maupun teoritis.

HASIL DAN PEMBAHASAN

Konsep Sistem Manajemen Keamanan Informasi

Sistem Manajemen Keamanan Informasi Atau *Information Security Management System* (ISMS) adalah pendekatan terstruktur untuk mengelola data sensitif, melindunginya dari akses, pengungkapan, atau penghancuran yang tidak sah. Di sektor perbankan, penerapan SMKI mengatasi potensi risiko dan kerentanan sekaligus memastikan kepatuhan terhadap peraturan dan menumbuhkan budaya ketahanan terhadap ancaman dunia maya yang terus berkembang. Berdasarkan penilaian risiko, implementasi kebijakan, dan perbaikan berkelanjutan, SMKI berfungsi sebagai landasan keamanan informasi.

Membangun SMKI dalam perbankan memerlukan perencanaan dan pelaksanaan yang cermat. Peran kunci seperti manajemen puncak, petugas keamanan informasi, dan manajer risiko berkolaborasi untuk mengidentifikasi risiko, mengembangkan kebijakan, menerapkan kontrol, dan memantau kemajuan sambil memastikan perbaikan berkelanjutan. Sejalan dengan standar ISO 27001 dalam upaya penanganan maupun pengendalian terhadap keamanan informasi, kiranya harus mempertimbangkan tiga aspek penting dalam keamanan informasi (*Confidentiality*, *Integrity*, *Availability*), yaitu: 1) *Confidentiality* (kerahasiaan). Merupakan aspek yang memastikan bahwa informasi hanya dapat diakses oleh orang yang berwenang; 2) *Integrity* (integritas). Merupakan aspek yang menjamin tidak adanya pengubahan data tanpa seizin pihak yang berwenang, menjaga

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

keakuratan dan keutuhan informasi; 3) *Availability* (ketersediaan). Merupakan aspek yang memberi jaminan atas ketersediaan data saat dibutuhkan, kapanpun dan dimanapun. [5]

Sejarah berdirinya *Information Security Management System* (ISMS) dimulai pada tahun 1995 ketika *British Standards Institution* (BSI) memperkenalkan standar pertama untuk pengelolaan keamanan informasi, yaitu BS 7799. Standar ini awalnya diterapkan oleh organisasi di Inggris untuk meningkatkan keamanan informasi mereka, dan kemudian menyebar ke seluruh dunia.

Pada tahun 2000, BS 7799 diterbitkan sebagai standar internasional ISO/IEC 17799, yang kemudian diperbarui pada tahun 2005 menjadi ISO/IEC 27001.[6] Standar ini memberikan kerangka kerja sistematis untuk mengelola keamanan informasi dalam suatu organisasi, termasuk identifikasi risiko, perlindungan terhadap risiko, dan penilaian terhadap efektivitas pengelolaan keamanan informasi. Sejak itu, ISMS telah berkembang menjadi suatu standar internasional yang diakui secara global, dan banyak organisasi di seluruh dunia menerapkannya untuk mengelola keamanan informasi mereka. Standar ini terus diperbarui dan ditingkatkan untuk mengikuti perkembangan teknologi dan tantangan keamanan informasi yang terus berubah.

Dalam beberapa tahun terakhir, ISMS telah menjadi semakin penting dalam era digital dan di tengah meningkatnya serangan siber. Organisasi yang ingin menjaga keamanan informasi mereka dan memenuhi persyaratan kepatuhan hukum dan regulasi, seringkali menggunakan ISMS sebagai kerangka kerja untuk mengelola keamanan informasi mereka. ISMS biasanya melibatkan proses siklus PDCA (*Plan-Do-Check-Act*) untuk memastikan bahwa kebijakan keamanan informasi yang diterapkan dalam organisasi efektif dan terus ditingkatkan. Dalam melaksanakan ISMS, organisasi harus mempertimbangkan risiko keamanan informasi yang mungkin terjadi dan mengambil langkah-langkah untuk mengurangi atau menghilangkan risiko tersebut.

ISO 27001 adalah standar internasional untuk ISMS yang memberikan kerangka kerja dan persyaratan yang harus dipenuhi oleh organisasi dalam mengelola keamanan informasi. Selain itu, ada juga standar dan kerangka kerja lainnya seperti NIST, COBIT, dan ITIL yang dapat digunakan untuk mengelola keamanan informasi dalam sebuah organisasi.[7] ISO 20071 ISO/IEC 27001 merupakan standar keamanan informasi yang menggantikan BS-7799:2 dan diterbitkan pada bulan Oktober 2005 *oleh International Organization for Standarization* dan *International Electrotechnical Commission.* ISO 27001 berisi spesifikasi atau persyaratan yang harus dipenuhi dalam membangun Sistem Manajemen Keamanan Informasi (SMKI).

Standar ini bersifat independen terhadap produk teknologi informasi, mensyaratkan penggunaan pendekatan manajemen berbasis risiko, dan dirancang untuk menjamin agar kontrol-kontrol keamanan yang dipilih mampu melindungi aset informasi dari berbagai risiko dan memberi keyakinan tingkat keamanan bagi pihak yang berkepentingan. Standar ini mengadopsi "*Plan-Do-Check-Act*" (PDCA) model, yang

[5] Lihat: https://www.djkn.kemenkeu.go.id/kanwil-jakarta/baca-artikel/16304/Information-Security-Management-System-ISMS. Diakses pada tanggal 20 Januari 2024.

[6] Fine Ermana, dkk, "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM", *Jurnal Sistem Informasi dan Komputer Akuntansi*, Vol. 1 No. 1 2012, h. 1-8.

[7] Chalifa Chazar, "Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005", *Jurnal Informasi*, Vol. VII No. 2 November 2015, h. 48-57.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

digunakan untuk mengatur semua proses SMKI. Penerapan model PDCA juga akan mencerminkan prinsip-prinsip sebagaimana diatur dalam Pedoman OECD yang mengatur keamanan sistem informasi dan jaringan. Standar ini memberikan model untuk menerapkan prinsipprinsip dalam pedoman yang mengatur penilaian risiko, desain keamanan dan implementasi, manajemen keamanan dan penilaian ulang.

ISO 27001 memiliki sebelas klausul kontrol keamanan (*security control*), 39 objektif control (*control objectives*) dan 133 kontrol keamanan/*control (controls*). Sebelas klausul kontrol keamanannya adalah sebagai berikut: 1) Kebijakan keamanan informasi; 2) Organisasi keamanan informasi; 3) Manajemen aset; 4) Sumber daya manusia menyangkut keamanan informasi; 5) Keamanan fisik dan lingkungan; 6) Komunikasi dan manajemen operasi; 7) Akses control; 8) Pengadaan/akuisisi, pengembangan dan pemeliharaan sistem informasi; 9) Pengelolaan insiden keamanan informasi; 10) Manajemen kelangsungan usaha (business continuity management); 11) Kepatuhan.[8]

Konsep Penerapan ISO 27001 Pada Bank Syariah

ISO adalah singkatan dari "*International Standard Organization*", ISO adalah entitas global yang didirikan pada tahun 1946. Delegasi dari 25 negara berkumpul untuk memastikan bahwa batas nasional tidak mengganggu kemampuan untuk mengembangkan teknologi yang andal. Saat ini, ISO menyatukan dewan standardisasi dari 166 negara dan melapor ke pemerintah pusat di Swiss.

ISO mengatur hampir semua standarisasi kegiatan industri industri, perusahaan dari lingkup terkecil hingga keamanan dan perlindungan data yang terkait dengan kehidupan.[9] Jika dalam hal keamanan IT, sertifikasi ISO 27001 adalah salah satu standar internasional yang paling dihormati. Nama lengkap ISO 27001 adalah "ISO/IEC 27001:2013" dan direvisi pada tahun 2017 dan 2022 bekerja sama dengan badan sertifikasi lain yang disebut Komisi *Elektroteknik Internasional* (IEC).[10]

ISO 27001 adalah standar internasional yang mengatur cara-cara perlindungan informasi penting dalam sebuah organisasi termasuk di dunia perbankan syariah. Standar ini membantu organisasi dalam mengidentifikasi, menganalisis, dan mengelola risiko terkait keamanan informasi dengan cara yang sistematis. Standar ini melibatkan pembangunan, penerapan, pemeliharaan, dan perbaikan terus-menerus dari Sistem Manajemen Keamanan Informasi (SMKI) dalam sebuah perbankan syariah. SMKI ini mencakup kebijakan, prosedur, pemantauan, pengukuran, dan penilaian risiko.

Penerapan standar ISO 27001 mendorong untuk menggunakan pendekatan berbasis risiko dalam mengelola keamanan informasi. Hal ini melibatkan identifikasi risiko, penilaian risiko, dan pengembangan langkah-langkah pengendalian untuk mengurangi atau menghilangkan risiko yang teridentifikasi. Standar ini juga menekankan pentingnya

[8] Margo Utomo, dkk, "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I", *Jurnal Teknik ITS*, Vol. 1 No. 1 September 2012, h. 288-293. DOI: 10.12962/j23373539.v1i1.900

[9] Fitroh, dkk, "Pentingnya Implementasi ISO 27001 dalam Manajemen Keamanan: Sistematika Review", *Prosiding Seminar Nasional Sains dan Teknologi*, *Fakultas Teknik Universitas Muhammadiyah Jakarta*, 1-2 November 2017, h. 1-6. https://jurnal.umj.ac.id/index.php/semnastek/article/view/1916/1568

[10] Yohan Adhi Styoutomo & Yova Ruldeviyani, "Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution", *CommIT Journal*, Vol. 17 No. 2 2023, h. 133-149. DOI:10.21512/commit.v17i2.8272

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

melindungi aset informasi dalam perbankan syariah, misalnya data pelanggan, kekayaan intelektual, dan informasi rahasia, menjaga keamanan fisik, keamanan personel, serta mengelola akses ke sistem informasi. ISO 27001 juga mendorong bank syariah untuk melakukan pengawasan dan peningkatan terus-menerus dalam manajemen keamanan informasi. Bank syariah diharapkan melakukan audit internal, mengevaluasi kepatuhan terhadap kebijakan dan prosedur, serta melaksanakan tindakan perbaikan yang diperlukan.[11]

Di antara fungsi dari penerapan ISO 27001 pada bank syariah adalah: 1) Merumuskan persyaratan keamanan dan tujuan serta memastikan bahwa pendanaan risiko keamanan dikelola secara efektif dan memastikan kepatuhan terhadap hukum dan peraturan yang ada; 2) Kerangka proses untuk pelaksanaan dan manajemen kontrol dan memastikan tujuan keamanan secara spesific dari suatu organisasi; 3) Identifikasi dan klarifikasi proses SMKI yang ada serta menentukan status kegiatan manajemen keamanan informasi; 4) Menentukan tingkat kepatuhan terhadap kebijakan, arahan dan standar yang diadopsi oleh organişasi; 5) Memberikan informasi yang relevan tentang keamanan informasi dan kebijakan keamanan informasi, arahan, standar dan prosedur untuk mitra dan organisasi lain untuk alasan operasional atau komersial.[12]

Kemudian dari segi keuntungan yang akan didapat dari implementasi ISO 27001 pada perbankan syariah adalah: 1) Perlindungan Terhadap Ancaman *Cyber.* Implementasi ISO 27001 membantu lembaga keuangan dalam mengidentifikasi, mengkategorikan, dan mengelola risiko yang terkait dengan keamanan informasi. Dengan adanya kerangka kerja yang kokoh, bank dapat mengambil tindakan pencegahan yang tepat dan melindungi diri dari serangan *cyber* yang merugikan. 2) Peningkatan Kepercayaan Nasabah. Keamanan informasi adalah hal yang sangat penting bagi nasabah di sektor perbankan. Dengan memiliki sertifikasi ISO 27001, bank dapat membuktikan komitmen mereka terhadap keamanan data nasabah. Ini membantu membangun kepercayaan nasabah dan memberikan keunggulan kompetitif di pasar yang semakin ketat. 3) Kepatuhan Terhadap Regulasi. Industri perbankan tunduk pada berbagai peraturan dan regulasi yang mengatur pengelolaan keamanan informasi. Implementasi ISO 27001 membantu bank memenuhi persyaratan hukum dan peraturan yang berlaku, seperti Perlindungan Data Pribadi atau Regulasi Perlindungan Data Umum. Dengan demikian, bank dapat menghindari sanksi hukum dan denda yang mungkin timbul akibat ketidakpatuhan.

Kendala penerapan ISO 27001 pada perbankan syariah yang sering ditemui adalah:

a) Biaya. Mengadopsi kerangka ISO 27001 dapat menjadi proses yang menghabiskan banyak waktu dan sumber daya. Hal ini dapat mencakup biaya pelatihan personel, pelaksanaan penilaian, dan penerapan pengendalian baru.
b) Kompleksitas. Kerangka kerja ISO 27001 bersifat komprehensif, sehingga membuatnya rumit untuk dipahami dan diterapkan. Hal ini dapat menjadi tantangan tersendiri bagi perbankan yang memiliki sumber daya dan keahlian terbatas.

[11] Mardhi Yudi & Djajasukma Tjahjadi, "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001", *Jurnal Penelitian Ilmu Komputer, System Embedded & Logic*, Vol. 6 No. 1 2018, h. 95-104. DOI:10.33558/piksel.v6i1.1404

[12] Arya Pratama Damanik, dkk, "Implementasi ISO 27001:2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA", *Jurnal Jurnal Sains Dan Teknologi (JSIT),* Vol. 3 No. 1 2023, h. 68-73. DOI:10.47233/jsit.v3i1.488

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

c) Ketidakfleksibelan. Kerangka kerja ISO 27001 adalah standar preskriptif, yang berarti kerangka tersebut menentukan pengendalian spesifik yang harus diterapkan oleh perbankan. Hal ini mungkin tidak fleksibel bagi bank yang memiliki persyaratan keamanan unik atau yang ingin menyesuaikan kontrolnya dengan kebutuhan bisnis spesifiknya.
d) Dapat memakan waktu dan sumber daya yang intensif. Penerapan kerangka ISO 27001 dapat menjadi proses yang kompleks dan memakan waktu, memerlukan alokasi sumber daya yang signifikan untuk menerapkan dan memelihara pengendalian yang diperlukan.
e) Memerlukan pemeliharaan berkelanjutan. Kerangka kerja ISO 27001 didasarkan pada siklus PDCA, yang berarti bahwa organisasi harus terus meninjau dan memperbarui pengendalian mereka untuk memastikan bahwa pengendalian tersebut efektif dan selaras dengan praktik terbaik terkini. Hal ini memerlukan pemeliharaan dan sumber daya yang berkelanjutan.

Tujuan dan Manfaat Penerapan ISO 27001 Pada Perbankan Syariah

Implementasi ISO 27001 ini bertujuan untuk memberikan gambaran implementasi sistem manajemen keamanan informasi berstandar internasional kepada bank syariah agar dapat mempelajari dan mencoba mengimplementasikannya. Implementasi ISO 27001 pada kegiatannya juga mencoba melakukan kegiatan audit terhadap semua aspek terkait, seperti: kondisi jaringan komputer lokal, policy, manajemen SDM, organisasi keamanan informasi, dan lain-lain.[13]

Organisasi ISO menciptakan ISO 27001 untuk melawan serangan cyber yang semakin canggih terhadap sistem informasi. Untuk melindungi data pribadi yang sensitif, perusahaan perlu mematuhi seperangkat standar keamanan yang ketat. Peraturan keamanan informasi yang muncul juga telah memicu adopsi ISO 27001. Undang-undang seperti *Health Insurance Portability and Accountability Act* (HIPAA) di Amerika Serikat dan *General Data Protection Regulation* (GDPR) di Uni Eropa dan Undang-Undang Perlindungan Data Pribadi di Indonesia yang juga memberlakukan hukuman yang ketat untuk pelanggaran data yang dapat dicegah. Mereka yang tidak mematuhinya juga menghadapi biaya penalti yang sangat tinggi.

Manfaat dari standar ISO 27001 adalah memastikan bahwa organisasi memiliki kontrol yang memadai terkait keamanan informasi, menunjukkan tata kelola yang baik dalam penanganan dan pengamanan informasi, dan adanya mekanisme untuk mengukur berhasil atau tidaknya kontrol pengamanan. Manfaat lainnya adalah adanya review yang independen terkait ISMS dengan adanya audit setiap tahun. Selain itu, citra perusahaan akan menjadi lebih baik, karena sertifikasi dikeluarkan oleh badan sertifikasi yang formal. Selain itu, ISO 27001 juga bermanfaat membantu bank dalam menjalankan perbaikan yang berkesinambungan dalam pengelolaan keamanan informasi, dan meningkatkan efektivitas dan keandalan pengamanan informasi.[14]

[13] Yuni Cintia, dkk, "Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001: 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi", *Jurnal Sistem Informasi Bisnis,* Vol. 6 No. 1 2016, h. 38-45. https://doi.org/10.21456/vol6iss1pp38-45

[14] Fitroh, dkk, "Pentingnya Implementasi ISO 27001 dalam Manajemen Keamanan: Sistematika Review", ..., h.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

Berikut manfaat lain dari adanya penerapan ISO 27001:

a) Memberi pemahaman yang lebih baik mengenai aset informasi dan proses manajemen keamanan informasi yang diperlukan.
b) Membantu memberikan pemahaman pentingnya keamanan informasi pada karyawan, stakeholder dan masyarakat umum.
c) Membantu mengarahkan implementasi sistem manajemen keamanan informasi berdasarkan kepada pertimbangan manajemen risiko.
d) Mendukung organisasi dengan memberi kerangka kerja (panduan) proses untuk mengimplementasikan dan melakukan manajemen serta kontrol terhadap keamanan informasi agar dapat menjamin bahwa objek-objek keamanan tertentu telah dicapai.
e) Membantu organisasi untuk menjaminkan risiko keamanan dapat dikendalikan dengan biaya terkontrol dan dengan feedback yang menguntungkan.
f) Meningkatkan keyakinan terhadap organisasi karena telah mematuhi undang-undang, peraturan-peraturan negara, dengan menjamin kualitas informasi dan pelayanan.
g) Mempersilakan auditor internal maupun external untuk memastikan bahwa organisasi telah mematuhi aturan-aturan, memiliki arah pengembangan Manajemen dan standard-standard yang dilaksanakan.[15]

ISO 27001 Merupakan Simbol untuk kualitas dan keamanan. Penetapan ISO 27001akan menunjukkan kepada pelanggan-pelanggan, partner anda dan pihak pemerintah bahwa kualitas pelayanan dan keamanan yang baik dalam proses bisnis anda telah dikendalikan dengan benar, hal ini dapat menjadi publikasi yang sangat positif bagi organisasi untuk meraih kepercayaan stake holder.

Urgensi Implementasi ISO 27001 Pada Perbankan Syariah

Pentingnya ISO 27001 di sektor perbankan syariah terletak pada kerangka komprehensifnya untuk mengelola risiko keamanan informasi dan memastikan kepatuhan terhadap peraturan. ISO 27001 sangat penting dalam memitigasi risiko dunia maya yang spesifik pada sektor perbankan, seperti penipuan keuangan dan pelanggaran data. Pendekatan berbasis risiko memungkinkan bank syariah untuk secara sistematis mengidentifikasi kerentanan, menetapkan kontrol yang kuat, dan membangun ketahanan terhadap ancaman dunia maya yang terus berkembang. Kepatuhan terhadap ISO 27001 meningkatkan postur keamanan bank syariah dan berfungsi sebagai simbol kepercayaan dan kredibilitas bagi nasabah, regulator, dan pemangku kepentingan lainnya.

Mengadopsi standar yang diakui secara internasional ini memungkinkan bank syariah untuk menavigasi lanskap digital dan peraturan yang kompleks ini, melindungi data sensitif, menjaga kepercayaan pelanggan, tetap mematuhi hukum dan peraturan, dan pada akhirnya memperkuat reputasi mereka sebagai lembaga aman yang mampu mengatasi ancaman dunia maya dan tantangan industri yang muncul.

Penerapan ISO 27001 ke sektor perbankan syariah melibatkan penyesuaian prinsip dan kontrol untuk mengatasi tantangan spesifik industri, seperti persyaratan peraturan yang ketat, lingkungan transaksional yang kompleks, dan kebutuhan perlindungan data yang berisiko tinggi. Dengan menyesuaikan kerangka ISMS agar sejalan dengan tuntutan unik ini, bank dapat secara efektif mengelola risiko keamanan informasi sekaligus menjaga

[15] Sisca, "Implementasi ISO 27001 Pada Pengelolaan Sistem Informasi Nilai Pelajaran Siswa Di SMKN 4 Bandar Lampung", *Jurnal Teknologi Terkini*, Vol. 2 No. 7 2022, h. 1-11.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

kepercayaan nasabah dan memastikan kepatuhan dalam lanskap digital yang berkembang pesat dan penuh dengan ancaman dunia maya.

Menavigasi lanskap keamanan informasi unik di sektor perbankan memerlukan pendekatan yang disesuaikan dengan penerapan ISO 27001. Mengintegrasikan ISO 27001 dengan peraturan dan standar perbankan terkait lainnya, seperti Standar Keamanan Data Industri Kartu Pembayaran (PCI DSS) dan Peraturan Perlindungan Data Umum (GDPR), menciptakan kerangka keamanan informasi yang komprehensif dan kohesif untuk lembaga keuangan.[16] Pendekatan yang selaras ini memungkinkan bank untuk secara efektif mengatasi tantangan-tantangan spesifik industri sambil menjaga kepatuhan di berbagai bidang peraturan, sehingga pada akhirnya meningkatkan ketahanan mereka terhadap ancaman dunia maya dalam lanskap digital yang semakin kompleks.

Bank syariah dapat menyesuaikan ISO 27001 dengan kebutuhan unik mereka dengan mengikuti beberapa langkah utama:[17] *Pertama,* Pahami konteksnya. Dapatkan pemahaman mendalam tentang kebutuhan dan tantangan spesifik dalam sektor perbankan. Pertimbangkan ancaman spesifik industri terhadap keamanan informasi, seperti serangan siber, pencurian identitas, dan aktivitas penipuan. Langkah ini membantu menentukan ruang lingkup dan tujuan Sistem Manajemen Keamanan Informasi (SMKI).

Kedua, Definisikan kepemimpinan dan komitmen. Dapatkan dukungan dan komitmen dari manajemen puncak di bank. Tentukan peran dan tanggung jawab, alokasikan sumber daya yang diperlukan, dan tetapkan kebijakan keamanan informasi. Menyelaraskan kebijakan dengan tujuan bisnis dan menunjukkan komitmen yang kuat terhadap perbaikan berkelanjutan. *Ketiga,* Penilaian risiko. Melakukan penilaian risiko komprehensif untuk mengidentifikasi risiko terhadap keamanan informasi. Sertakan semua potensi ancaman dan kerentanan, seperti serangan malware, penipuan internal, dan teknik rekayasa sosial.

Keempat, Menerapkan pengendalian. Berdasarkan penilaian risiko, pilih dan terapkan pengendalian yang tepat untuk mengelola dan memitigasi risiko yang teridentifikasi. Manfaatkan pengendalian yang direkomendasikan dalam Lampiran ISO 27001 dan pertimbangkan pengendalian tambahan yang relevan dengan sektor perbankan, seperti langkah-langkah untuk perbankan online yang aman, mekanisme otentikasi yang kuat, dan enkripsi data. *Kelima,* Pelatihan dan kesadaran. Memberikan pelatihan komprehensif kepada pegawai bank tentang kebijakan, prosedur, dan pengendalian SMKI. Tekankan pentingnya mematuhi protokol keamanan, menangani data pelanggan dengan aman, dan menjaga kerahasiaan. Langkah ini penting untuk memitigasi risiko yang terkait dengan ancaman orang dalam dan serangan rekayasa sosial.

Keenam, Pemantauan dan tinjauan. Secara teratur memantau dan meninjau kinerja SMKI. Melakukan audit internal, tinjauan manajemen, dan pemantauan berkelanjutan terhadap insiden keamanan. Hal ini membantu memastikan efektivitas SMKI yang berkelanjutan dan memungkinkan identifikasi area untuk perbaikan dan remediasi.

[16] Shobur Abdusalam & Ratih Titi Komala Sari, "Teknologi Komunikasi dan Informatika, Implementasi Algoritma Brute Force dan Algoritma Simon Pada Aplikasi Task Management System dengan Pengujian ISO 27001", *Jurnal Penelitian dan Pembelajaran Informatika*, Vol. 7 No. 1 2022, h. 115-165. DOI:10.29100/jipi.v7i1. 2444

[17] Naniek Utami Handayani, dkk, "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001", *TEKNIK*, Vol. 39 No. 2 2018, h. 78–85. DOI: https://doi.org/10.14710/teknik.v39i2.15918

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

Ketujuh, Sertifikasi. Setelah SMKI diterapkan dan beroperasi secara efektif, pertimbangkan untuk mencari sertifikasi ISO 27001 dari lembaga sertifikasi yang memiliki reputasi baik. Sertifikasi ini memvalidasi komitmen bank terhadap keamanan informasi dan memberikan jaminan kepada pemangku kepentingan, termasuk nasabah dan otoritas pengatur.

Dengan mengikuti langkah-langkah ini dan menyesuaikannya dengan kebutuhan serta keadaan spesifik sektor perbankan syariah, lembaga keuangan dapat berhasil mengadaptasi ISO 27001 dengan persyaratan industri, memperkuat keamanan informasi, dan menunjukkan komitmen teguh untuk melindungi data keuangan sensitif.[18] Berikut beberapa tahap dalam penerapan ISO 27001 yang dapat direalisasikan ke dalam dunia perbankan, yaitu:

1) Analisis risiko. Identifikasi dan evaluasi risiko keamanan informasi yang mungkin dihadapi oleh bank syariah. Hal ini melibatkan penilaian terhadap kerentanan, ancaman potensial, dan dampak yang mungkin terjadi. Dengan pemahaman yang mendalam tentang risiko, bank syariah dapat merancang langkah-langkah mitigasi yang efektif.
2) Kebijakan keamanan informasi. Pembuatan kebijakan dan prosedur yang jelas untuk mengatur pengelolaan keamanan informasi di seluruh organisasi. Hal ini meliputi kebijakan penggunaan kata sandi yang kuat, pengaturan akses, dan kebijakan penggunaan perangkat seluler yang aman.
3) Pelatihan dan kesadaran karyawan. Mengedukasi dan melibatkan karyawan dalam upaya keamanan informasi. Melalui pelatihan yang tepat, karyawan dapat memahami pentingnya keamanan informasi, tindakan yang harus diambil untuk melindungi data, dan bagaimana melaporkan kejadian keamanan yang mencurigakan.
4) Audit internal dan pemantauan. Melakukan audit internal secara berkala untuk memastikan kepatuhan terhadap kebijakan keamanan informasi. Pemantauan terus-menerus terhadap sistem keamanan juga penting untuk mendeteksi aktivitas mencurigakan dan serangan potensial.
5) Pemulihan bencana dan rencana keberlanjutan bisnis. Menyusun rencana pemulihan bencana yang efektif dan rencana keberlanjutan bisnis untuk mengatasi kemungkinan insiden keamanan yang dapat mengganggu operasional bank. Ini termasuk cadangan data yang teratur, pengujian rencana pemulihan bencana, dan pemulihan sistem dalam waktu yang minimal.[19]

Pentingnya Kepatuhan ISO 27001 Pada Perbankan Syariah

Di sektor perbankan syariah, kepatuhan sangat penting untuk memastikan keamanan informasi dan menjaga kepercayaan nasabah. Persyaratan peraturan mengharuskan kepatuhan yang ketat terhadap standar seperti ISO 27001, yang memberikan perlindungan kuat untuk data sensitif dan memitigasi potensi risiko. Dengan mengikuti pedoman ini, bank syariah menunjukkan komitmen mereka terhadap lingkungan yang aman dalam menghadapi ancaman yang terus berkembang.

[18] Siti Alvi Sholikhatin, dkk, "Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto)", *Jurnal IT CIDA*, Vol. 4 No. 1 Juni 2018, h. 1-9.

[19] Badan Standardisasi Nasional, *Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan*, Jakarta; BSN, 2016.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

Kepatuhan terhadap ISO 27001 menumbuhkan kepercayaan di antara pelanggan dan pemangku kepentingan dengan menawarkan pendekatan yang transparan dan sistematis terhadap manajemen keamanan informasi.[20] Bank syariah yang mematuhi standar yang diakui secara internasional ini menunjukkan dedikasinya dalam melindungi data sensitif dan menjaga kepatuhan terhadap peraturan, serta menanamkan keandalan pada klien dan pemangku kepentingan. Hal ini memperkuat reputasi bank sebagai institusi aman yang menavigasi lanskap digital yang kompleks dari ancaman dunia maya.

Memasukkan kepatuhan ISO 27001 memungkinkan lembaga keuangan untuk mengadopsi pendekatan proaktif terhadap mitigasi risiko dan mencegah pelanggaran keamanan atau insiden kehilangan data. Dengan menerapkan standar ini, bank syariah dapat secara sistematis mengidentifikasi kerentanan, memprioritaskan ancaman, dan menetapkan kontrol yang kuat untuk melindungi informasi sensitif sekaligus menumbuhkan budaya ketahanan. Kepatuhan terhadap ISO 27001 memberdayakan bank syariah untuk menavigasi lanskap digital yang rumit dengan percaya diri sambil menjunjung tinggi kepercayaan pelanggan dan persyaratan peraturan.

KESIMPULAN

Penerapan ISO 27001 yang merupakan standar internasional yang membantu organisasi melindungi informasi penting secara sistematis pada bank syariah adalah sebuah keharusan di era digitalisasi informasi seperti saat ini. Banyak keuntungan dan manfaat yang akan didapat oleh industri perbankan syariah di Indoensia dengan menerapkan standar ISO 27001 ini. Di antaranya: 1) Standar ini akan mendorong pengembangan Sistem Manajemen Keamanan Informasi (SMKI) yang ada pada bank syariah dan pengelolaan risiko yang terkait; 2) melalui pendekatan berbasis risiko bank syariah dapat melindungi aset informasi, menjaga keamanan fisik dan personel, serta mengelola akses ke sistem informasi; 3) ISO 27001 juga mendorong pengawasan dan perbaikan terus-menerus sehingga dengan mengimplementasikan standar ini, bank syariah dapat meningkatkan keamanan informasi dan melindungi informasi penting mereka dengan lebih efektif. Dalam menerapkan ISO 27001 pada bank syariah diperlukan beberapa tahapan yang harus dilalui, yakni: analisis risiko, kebijakan keamanan informasi, pelatihan dan kesadaran karyawan, audit internal dan pemantauan, pemulihan bencana dan rencana keberlanjutan bisnis.

DAFTAR PUSTAKA

Abdusalam, Shobur & Ratih Titi Komala Sari. (2022). "Teknologi Komunikasi dan Informatika, Implementasi Algoritma Brute Force dan Algoritma Simon Pada Aplikasi Task Management System dengan Pengujian ISO 27001", *Jurnal Penelitian dan Pembelajaran Informatika* 7 (1): 115-165. DOI:10.29100/jipi.v7i1. 2444

Ansori, Aan (2018). "Sistem Informasi Perbankan Syariah", *Jurnal Banque Syar'I* 4 (1): 183. DOI: 10.32678/bs.v4i2.1131

[20] Chalifa Chazar, "Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005", *Jurnal Informasi*, Vol. VII No. 2 November 2015, h. 48-57.

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

Badan Standardisasi Nasional, *Teknologi Informasi-Teknik Keamanan-Sistem Manajemen Keamanan Informasi-Persyaratan*, Jakarta; BSN, 2016.

Chazar, Chalifa. (2015). "Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005", *Jurnal Informasi* VII (2): 48-57.

Chazar, Chalifa. (2015). "Standar Manajemen Keamanan Sistem Informasi Berbasis ISO 27001:2005", *Jurnal Informasi* VII (2): 48-57.

Cintia, Yuni, dkk. (2016). "Analisis Sistem Manajemen Keamanan Informasi Menggunakan ISO/IEC 27001: 2013 Serta Rekomendasi Model Sistem Menggunakan Data Flow Diagram pada Direktorat Sistem Informasi Perguruan Tinggi", *Jurnal Sistem Informasi Bisnis* 6 (1): 38-45. https://doi.org/10.21456 /vol6iss1pp38-45

Damanik, Arya Pratama, dkk. (2023). "Implementasi ISO 27001:2013 Dalam Pengamanan Sistem Informasi Pada Yayasan Pendidikan Islam ANNUR PRIMA", *Jurnal Jurnal Sains Dan Teknologi (JSIT)* 3 (1): 68-73. DOI:10.47233/jsit.v3i1.488

Ermana, Fine, dkk. (2012). "Audit Keamanan Sistem Informasi Berdasarkan Standar ISO 27001 Pada PT. BPR JATIM", *Jurnal Sistem Informasi dan Komputer Akuntansi* 1 (1): 1-8.

Fitroh, dkk. (2017). "Pentingnya Implementasi ISO 27001 dalam Manajemen Keamanan: Sistematika Review", *Prosiding Seminar Nasional Sains dan Teknologi*, *Fakultas Teknik Universitas Muhammadiyah Jakarta*, 1-2 November: 1-6. https://jurnal.umj.ac.id/ index. php/ semnastek/article/view/1916/1568

Handayani, Naniek Utami , dkk. (2018). "Penilaian Risiko Sistem Informasi Fakultas Teknik Universitas Diponegoro Menggunakan Metode Failure Mode Effect And Analysis Berbasis Framework ISO 27001", *TEKNIK* 39 (2): 78–85. DOI: https://doi.org/10.14710/ teknik.v39i2.15918

Sholikhatin, Siti Alvi , dkk. (2018). "Analisis Keamanan Sistem Informasi Dengan ISO 27001 (Studi Kasus: Sistem Informasi Akademik Universitas Muhammadiyah Purwokerto)", *Jurnal IT CIDA* 4 (1): h. 1-9.

Sisca. (2022). "Implementasi ISO 27001 Pada Pengelolaan Sistem Informasi Nilai Pelajaran Siswa Di SMKN 4 Bandar Lampung", *Jurnal Teknologi Terkini* 2 (7): 1-11.

Styoutomo, Yohan Adhi & Yova Ruldeviyani. (20230. "Information Security Awareness Raising Strategy Using Fuzzy AHP Method with HAIS-Q and ISO/IEC 27001:2013: A Case Study of XYZ Financial Institution", *CommIT Journal* 17 (2): 133-149. DOI:10. 21512/commit.v17i2.8272

Utomo, Margo, dkk. (2012). "Pembuatan Tata Kelola Keamanan Informasi Kontrol Akses Berbasis ISO/IEC 27001:2005 Pada Kantor Pelayanan Perbendaharaan Surabaya I", *Jurnal Teknik ITS* 1 (1): 2012, h. 288-293. DOI: 10.12962/j23373539.v1i1.900

Yudi, Mardhi & Djajasukma Tjahjadi. (2018). "Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001", *Jurnal Penelitian Ilmu Komputer, System Embedded & Logic* 6 (1): 95-104. DOI:10.33558 /piksel.v6i1.1404

e-ISSN 2686-5998
p-ISSN 2621-12X
https://stai-binamadani.e-journal.id/madanisyariah

https://ojk.go.id/id/kanal/syariah/Pages/Perbankan-Syariah.aspx

https://ojk.go.id/id/kanal/syariah/tentang-syariah/Pages/Perbankan-Syariah.aspx

https://www.bbc.com/indonesia/articles/cn01gdr7eero

https://www.djkn.kemenkeu.go.id/kanwil-jakarta/baca-artikel/16304/Information-Security-Manage ment-System-ISMS. Diakses pada tanggal 20 Januari 2024.

https://www.isms.online/sectors/iso-27001-for-the-banking-sector/. Diakses pada tanggal 5 Januari 2024.