DOI: https://doi.org/10.62017/jpmi

Penyusunan Sertifikasi ISO 27001 Di PT. Pundi Mas Berjaya

Haeruddin *[1]
Stefanus Eko Prasetyo [2]
Ari Wahyuni Kaharuddin [3]

[1,2,3] Universitas Internasional Batam
*e-mail: haeruddin@uib.edu[1], stefanus.eko@uib.edu[2], ariwahyunik043@gmail.com[3]

Abstrak

Persiapan untuk sertifikasi ISO 27001 di PT Pundi Mas Berjaya merupakan proses yang melibatkan pemahaman mendalam tentang persyaratan standar, penyusunan SOP yang terstruktur, penilaian risiko yang cermat, kolaborasi antar departemen, dan dokumentasi yang teliti. Hasil dari persiapan ini menunjukkan komitmen perusahaan dalam meningkatkan keamanan informasi secara menyeluruh. Saran yang diambil adalah untuk terus berkomitmen pada peningkatan kontinu dalam manajemen keamanan informasi, sesuai dengan prinsip-prinsip ISO 27001. Dengan demikian, persiapan ini bukan hanya memenuhi persyaratan formal, tetapi juga membawa dampak positif dalam memperkuat keamanan informasi di PT Pundi Mas Berjaya.

***Kata kunci**: ISO 2700, Risk Assessment, SOP*

Abstract

The preparation for ISO 27001 certification at PT Pundi Mas Berjaya is a process that involves a deep understanding of the standard's requirements, structured SOP development, careful risk assessment, interdepartmental collaboration, and meticulous documentation. The outcome of this preparation demonstrates the company's commitment to enhancing information security comprehensively. The recommendation is to maintain a continuous commitment to improving information security management, in accordance with ISO 27001 principles. Thus, this preparation not only meets formal requirements but also positively impacts the strengthening of information security at PT Pundi Mas Berjaya.

***Keywords**: ISO 2700, Risk Assessment, SOP*

PENDAHULUAN

Dalam era digital yang sedang berkembang ini, perusahaan IT seperti PT. Pundi Mas Berjaya memiliki tanggung jawab yang semakin meningkat untuk melindungi data dan informasi yang mereka kelola. Untuk mencapai tingkat keamanan yang maksimal, sertifikasi ISO 27001 menjadi fondasi yang sangat penting. ISO/IEC 27001 merupakan standar internasional yang menetapkan persyaratan untuk membangun, menerapkan, memelihara, dan terus meningkatkan sistem manajemen keamanan informasi (ISMS) dalam suatu organisasi, serta bertujuan untuk melindungi informasi dengan mengelola risiko keamanan informasi (Culot et al. 2021). Standar internasional ini memberikan panduan bagi perusahaan IT, termasuk PT. PMB, dalam membangun, menerapkan, dan memelihara sistem manajemen keamanan informasi yang kuat.

Sertifikasi ISO 27001 bukan hanya standar formal, tetapi telah menjadi titik pusat dalam strategi keamanan informasi perusahaan modern. Sebagai standar yang diakui secara global, ISO 27001 menunjukkan komitmen perusahaan terhadap perlindungan data, keandalan sistem, dan keamanan informasi secara menyeluruh. Dalam konteks PT. PMB, sertifikasi ini menjadi bukan hanya kebutuhan, tetapi juga diferensiasi yang kuat dalam membangun kepercayaan pelanggan dan mitra bisnis, terutama di tengah meningkatnya ancaman keamanan cyber.

PT. PMB, yang didirikan pada tahun 2014 sebagai penyedia solusi perangkat lunak terkemuka, memiliki peran penting dalam mengintegrasikan teknologi informasi terbaru dalam berbagai bidang bisnis. Solusi berbasis layanan yang ditawarkan oleh perusahaan ini mencakup industri properti, otomotif, transportasi, pengiriman makanan, pengiriman barang, dan e-commerce. Melalui model pengembangan on-site dan off-site, PT. PMB mampu merancang solusi-solusi inovatif yang memungkinkan bisnis menghadapi era digital (pmberjaya.com 2024).

DOI: https://doi.org/10.62017/jpmi

Dengan dukungan tim yang kuat dan kapasitas yang mampu menangani proyek-proyek besar, PT. PMB menegaskan komitmennya untuk memberikan pelayanan terbaik kepada setiap pelanggan. Kunci keberhasilan perusahaan ini terletak pada kemampuan adaptasi terhadap berbagai kebutuhan sistem informasi komputer, menciptakan solusi terdepan dalam manajemen kualitas, manajemen proyek, infrastruktur TI, dan aspek lainnya. Hal ini bertujuan untuk menciptakan kepuasan maksimal bagi para klien, sejalan dengan komitmen PT. PMB dalam memberikan pelayanan terpadu.

Pelayanan terpadu yang ditawarkan oleh PT. PMB dirancang untuk memberikan akses yang mudah melalui berbagai platform, termasuk website responsif, situs mobile, dan aplikasi mobile. Dengan demikian, perusahaan ini mendukung optimalisasi aktivitas bisnis pelanggan dan memastikan pengalaman yang lancar dan efisien dalam penggunaan solusi-solusi yang mereka tawarkan. Dalam konteks keseluruhan ini, sertifikasi ISO 27001 menjadi fondasi yang kuat bagi keamanan informasi PT. PMB, memastikan bahwa solusi-solusi yang ditawarkan tidak hanya inovatif tetapi juga aman dan dapat diandalkan.

METODE

A. Metode Penelitian

Pada bagian ini, peneliti menggunakan metode deskriptif untuk menguraikan secara rinci langkah-langkah yang terlibat dalam penyusunan SOP, analisis risiko, dan dokumentasi pendukung. Metode deskriptif digunakan untuk menggambarkan secara sistematis dan faktual mengenai fakta-fakta dan sifat hubungan antar fenomena yang diselidiki (Dr. Muhammad Ramdhan 2021). Dalam konteks penelitian ini, metode deskriptif bertujuan untuk menguraikan langkah-langkah yang dilakukan oleh PT. PMB dalam penyusunan SOP, analisis risiko, dan dokumentasi pendukung untuk sertifikasi ISO 27001.

B. Tahapan Penelitian

1. Tahap Perencanaan

   Dalam tahap ini, dilakukan diskusi internal dengan melibatkan manajemen dan pemangku kepentingan untuk mengidentifikasi kebutuhan perusahaan. Ruang lingkup ditetapkan pada area kunci seperti pengelolaan SDM, pengembangan perangkat lunak, keamanan jaringan, pemeliharaan peralatan, manajemen disaster recovery, manajemen akses, dan backup data perusahaan.
2. Tahap Persiapan

   Tahap persiapan dimulai dengan pengumpulan informasi melalui wawancara dengan karyawan yang terlibat langsung dalam proses operasional, observasi langsung terhadap pelaksanaan proses operasional di lapangan, dan peninjauan dokumen internal seperti kebijakan perusahaan, panduan kerja, dan catatan operasional.
3. Tahap Pelaksanaan

   Pada tahap ini, penulis menyusun Standar Operasional Prosedur (SOP), melakukan konsultasi, dan revisi melalui diskusi dengan pemangku kepentingan. Analisis risiko mencakup identifikasi risiko melalui wawancara, observasi, dan dokumen perusahaan, mengidentifikasi ancaman seperti malware dan pelanggaran data, serta mengevaluasi dampak dan kemungkinan risiko. Tindakan pengendalian risiko termasuk teknologi keamanan seperti anti-malware, firewall, kontrol akses, serta prosedur keamanan fisik dan pelatihan. Dokumen pendukung QMS mencakup proses untuk memenuhi standar kualitas, kebijakan, prosedur, dan audit internal. ISMS mencakup kebijakan keamanan informasi, prosedur dan kontrol, serta evaluasi risiko berkala. ITSM mencakup rencana layanan TI, desain yang efisien dan efektif, serta implementasi dan pengelolaan sesuai standar.

DOI: https://doi.org/10.62017/jpmi

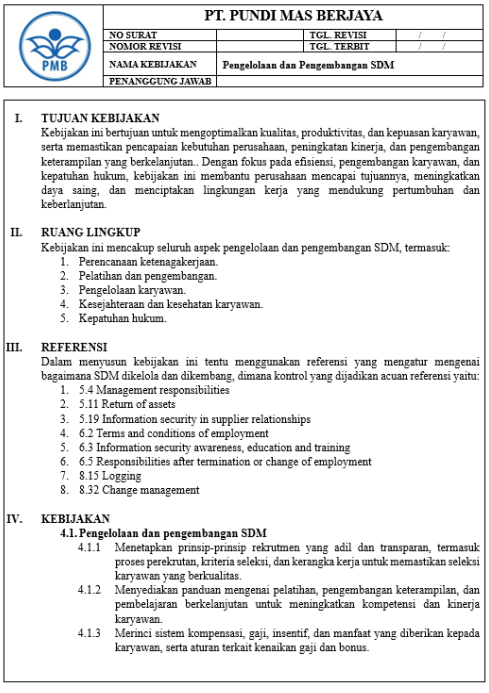
HASIL DAN PEMBAHASAN

A. Penyusunan SOP

Sebagai bagian dari persiapan untuk mendapatkan sertifikasi ISO 27001, PT. PMB perlu menyusun SOP perusahaan. SOP ini merupakan serangkaian panduan tertulis yang memastikan operasi dan proses dalam suatu organisasi dilakukan secara efisien, konsisten, dan terkontrol. SOP bertujuan untuk mengurangi kesalahan, menyelesaikan masalah dengan efektif, melindungi tenaga kerja, dan menetapkan standar kerja agar target tercapai dan kualitas pekerjaan meningkat (Muhaling et al. 2021). Oleh karena itu, tugas saya di sini adalah melakukan penyusunan SOP yang sesuai dengan kebutuhan dan praktik terbaik perusahaan. SOP ini akan menjadi panduan bagi karyawan PT. PMB dalam melaksanakan berbagai tugas dan proses operasional, khususnya terkait dengan manajemen keamanan informasi. Dengan menyusun SOP yang komprehensif dan tepat, diharapkan perusahaan dapat memenuhi persyaratan sertifikasi ISO 27001 dengan baik. Proses penyusunan SOP ini melibatkan pengumpulan informasi terperinci tentang berbagai proses dan kebijakan yang ada di perusahaan, serta konsultasi dengan berbagai pemangku kepentingan. Dengan demikian, SOP yang dihasilkan akan mencerminkan praktik terbaik dan kebutuhan aktual PT. PMB dalam menjaga keamanan informasi dan memenuhi standar internasional yang ditetapkan oleh ISO 27001. Tujuan akhirnya adalah agar PT. PMB dapat mengimplementasikan SOP ini dengan efektif dan efisien, sehingga membantu memperkuat sistem manajemen keamanan informasi perusahaan secara keseluruhan. Adapun SOP yang disusun sebagai berikut.

1. SOP Pengelolaan dan Pengembangan SDM

   Pengelolaan dan Pengembangan SDM merupakan serangkaian proses dan praktik yang digunakan oleh organisasi untuk mengelola, mempertahankan, mengembangkan, dan memaksimalkan potensi karyawan. Tujuannya yaitu untuk menciptakan lingkungan kerja yang efisien, produktif, dan berkelanjutan, sambil memastikan pertumbuhan dan perkembangan karyawan yang sejalan dengan tujuan strategis organisasi.



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Pengelolaan dan Pengembangan SDM		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini bertujuan untuk mengoptimalkan kualitas, produktivitas, dan kepuasan karyawan, serta memastikan pencapaian kebutuhan perusahaan, peningkatan kinerja, dan pengembangan keterampilan yang berkelanjutan.. Dengan fokus pada efisiensi, pengembangan karyawan, dan kepatuhan hukum, kebijakan ini membantu perusahaan mencapai tujuannya, meningkatkan daya saing, dan menciptakan lingkungan kerja yang mendukung pertumbuhan dan keberlanjutan.

II. RUANG LINGKUP

Kebijakan ini mencakup seluruh aspek pengelolaan dan pengembangan SDM, termasuk:

1. Perencanaan ketenagakerjaan.
2. Pelatihan dan pengembangan.
3. Pengelolaan karyawan.
4. Kesejahteraan dan kesehatan karyawan.
5. Kepatuhan hukum.

III. REFERENSI

Dalam menyusun kebijakan ini tentu menggunakan referensi yang mengatur mengenai bagaimana SDM dikelola dan dikembang, dimana kontrol yang dijadikan acuan referensi yaitu:

1. 5.4 Management responsibilities
2. 5.11 Return of assets
3. 5.19 Information security in supplier relationships
4. 6.2 Terms and conditions of employment
5. 6.3 Information security awareness, education and training
6. 6.5 Responsibilities after termination or change of employment
7. 8.15 Logging
8. 8.32 Change management

IV. KEBIJAKAN

4.1. Pengelolaan dan pengembangan SDM

4.1.1 Menetapkan prinsip-prinsip rekrutmen yang adil dan transparan, termasuk proses perekrutan, kriteria seleksi, dan kerangka kerja untuk memastikan seleksi karyawan yang berkualitas.

4.1.2 Menyediakan panduan mengenai pelatihan, pengembangan keterampilan, dan pembelajaran berkelanjutan untuk meningkatkan kompetensi dan kinerja karyawan.

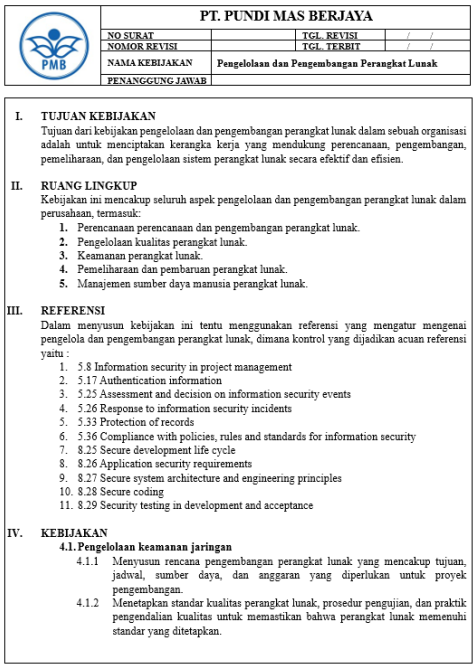
4.1.3 Merinci sistem kompensasi, gaji, insentif, dan manfaat yang diberikan kepada karyawan, serta aturan terkait kenaikan gaji dan bonus.

Gambar 1. SOP Pengelolaan dan Pengembangan SDM

DOI: https://doi.org/10.62017/jpmi

2. SOP Pengelolaan dan Pengembangan Perangkat Lunak

Pengelolaan dan Pengembangan perangkat lunak merupakan proses merancang, membuat, menguji, dan memelihara program komputer atau aplikasi perangkat lunak. Tujuannya yaitu untuk menciptakan solusi perangkat lunak yang memenuhi kebutuhan pengguna atau organisasi. Proses pengelolaan dan pengembangan perangkat lunak melibatkan sejumlah tahap dan aktivitas yang terstruktur untuk mencapai tujuan yang diinginkan.



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Pengelolaan dan Pengembangan Perangkat Lunak		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Tujuan dari kebijakan pengelolaan dan pengembangan perangkat lunak dalam sebuah organisasi adalah untuk menciptakan kerangka kerja yang mendukung perencanaan, pengembangan, pemeliharaan, dan pengelolaan sistem perangkat lunak secara efektif dan efisien.

II. RUANG LINGKUP

Kebijakan ini mencakup seluruh aspek pengelolaan dan pengembangan perangkat lunak dalam perusahaan, termasuk:

1. Perencanaan perencanaan dan pengembangan perangkat lunak.
2. Pengelolaan kualitas perangkat lunak.
3. Keamanan perangkat lunak.
4. Pemeliharaan dan pembaruan perangkat lunak.
5. Manajemen sumber daya manusia perangkat lunak.

III. REFERENSI

Dalam menyusun kebijakan ini tentu menggunakan referensi yang mengatur mengenai pengelola dan pengembangan perangkat lunak, dimana kontrol yang dijadikan acuan referensi yaitu :

1. 5.8 Information security in project management
2. 5.17 Authentication information
3. 5.25 Assessment and decision on information security events
4. 5.26 Response to information security incidents
5. 5.33 Protection of records
6. 5.36 Compliance with policies, rules and standards for information security
7. 8.25 Secure development life cycle
8. 8.26 Application security requirements
9. 8.27 Secure system architecture and engineering principles
10. 8.28 Secure coding
11. 8.29 Security testing in development and acceptance

IV. KEBIJAKAN

4.1. Pengelolaan keamanan jaringan

4.1.1 Menyusun rencana pengembangan perangkat lunak yang mencakup tujuan, jadwal, sumber daya, dan anggaran yang diperlukan untuk proyek pengembangan.

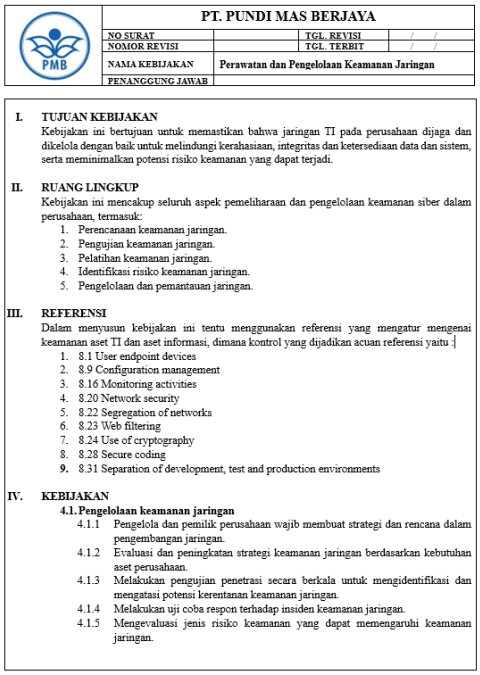
4.1.2 Menetapkan standar kualitas perangkat lunak, prosedur pengujian, dan praktik pengendalian kualitas untuk memastikan bahwa perangkat lunak memenuhi standar yang ditetapkan.

Gambar 2. SOP Pengelolaan dan Pengembangan Perangkat Lunak

3. SOP Perawatan dan Pengelolaan Keamanan Jaringan

Prosedur perawatan dan pengelolaan keamanan jaringan merupakan panduan resmi yang menjaga keandalan, ketersediaan, dan keamanan jaringan komputer. Tujuan dari pembuatan SOP ini yaitu menjaga ketersediaan jaringan komputer yang tinggi dan memastikan operasional yang aman.

DOI: https://doi.org/10.62017/jpmi



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Perawatan dan Pengelolaan Keamanan Jaringan		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini bertujuan untuk memastikan bahwa jaringan TI pada perusahaan dijaga dan dikelola dengan baik untuk melindungi kerahasiaan, integritas dan ketersediaan data dan sistem, serta meminimalkan potensi risiko keamanan yang dapat terjadi.

II. RUANG LINGKUP

Kebijakan ini mencakup seluruh aspek pemeliharaan dan pengelolaan keamanan siber dalam perusahaan, termasuk:

1. Perencanaan keamanan jaringan.
2. Pengujian keamanan jaringan.
3. Pelatihan keamanan jaringan.
4. Identifikasi risiko keamanan jaringan.
5. Pengelolaan dan pemantauan jaringan.

III. REFERENSI

Dalam menyusun kebijakan ini tentu menggunakan referensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan referensi yaitu :

1. 8.1 User endpoint devices
2. 8.9 Configuration management
3. 8.16 Monitoring activities
4. 8.20 Network security
5. 8.22 Segregation of networks
6. 8.23 Web filtering
7. 8.24 Use of cryptography
8. 8.28 Secure coding
9. 8.31 Separation of development, test and production environments

IV. KEBIJAKAN

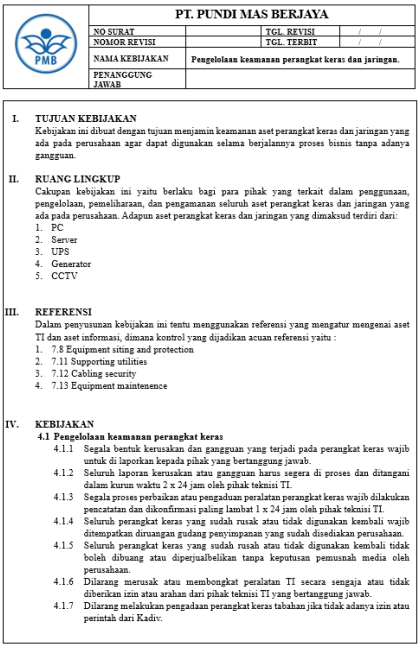
4.1. Pengelolaan keamanan jaringan

4.1.1 Pengelola dan pemilik perusahaan wajib membuat strategi dan rencana dalam pengembangan jaringan.
4.1.2 Evaluasi dan peningkatan strategi keamanan jaringan berdasarkan kebutuhan aset perusahaan.
4.1.3 Melakukan pengujian penetrasi secara berkala untuk mengidentifikasi dan mengatasi potensi kerentanan keamanan jaringan.
4.1.4 Melakukan uji coba respon terhadap insiden keamanan jaringan.
4.1.5 Mengevaluasi jenis risiko keamanan yang dapat memengaruhi keamanan jaringan.

Gambar 3. SOP Perawatan dan Penglolaan Keamanan Jaringan

4. SOP Pemeliharaan Peralatan dan Ketersediaan Sarana Pendukung

Prosedur pemeliharaan peralatan dan ketersediaan sarana pendukung merupakan prosedur yang memastikan semua peralatan dapat digunakan tanpa ada kerusakan dan gangguan, sehingga proses bisnis dapat terus berjalan dengan baik. Tujuan dari SOP ini yaitu memastikan semua peralatan dapat digunakan, penjadwalan pemeliharaan peralatan dapat berjalan dengan baik, serta ketersediaan sarana pendukung peralatan dapat tersedia dalam setiap proses bisnis perusahaan.



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Pengelolaan keamanan perangkat keras dan jaringan.		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin keamanan aset perangkat keras dan jaringan yang ada pada perusahaan agar dapat digunakan selama berjalannya proses bisnis tanpa adanya gangguan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi para pihak yang terkait dalam penggunaan, pengelolaan, pemeliharaan, dan pengamanan seluruh aset perangkat keras dan jaringan yang ada pada perusahaan. Adapun aset perangkat keras dan jaringan yang dimaksud terdiri dari:

1. PC
2. Server
3. UPS
4. Generator
5. CCTV

III. REFERENSI

Dalam penyusunan kebijakan ini tentu menggunakan referensi yang mengatur mengenai aset TI dan aset informasi, dimana kontrol yang dijadikan acuan referensi yaitu :

1. 7.8 Equipment siting and protection
2. 7.11 Supporting utilities
3. 7.12 Cabling security
4. 7.13 Equipment maintenence

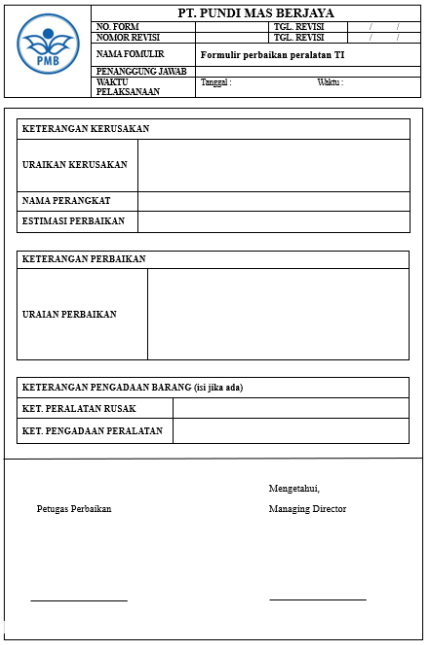
IV. KEBIJAKAN

4.1 Pengelolaan keamanan perangkat keras

4.1.1 Segala bentuk kerusakan dan gangguan yang terjadi pada perangkat keras wajib untuk di laporkan kepada pihak yang bertanggung jawab.
4.1.2 Seluruh laporan kerusakan atau gangguan harus segera di proses dan ditangani dalam kurun waktu 2 x 24 jam oleh pihak teknisi TI.
4.1.3 Segala proses perbaikan atau pengaduan peralatan perangkat keras wajib dilakukan pencatatan dan dikonfirmasi paling lambat 1 x 24 jam oleh pihak teknisi TI.
4.1.4 Seluruh perangkat keras yang sudah rusak atau tidak digunakan kembali wajib ditempatkan diruangan gudang penyimpanan yang sudah disediakan perusahaan.
4.1.5 Seluruh perangkat keras yang sudah rusah atau tidak digunakan kembali tidak boleh dibuang atau diperjualbelikan tanpa keputusan pemusnah media oleh perusahaan.
4.1.6 Dilarang merusak atau membongkat peralatan TI secara sengaja atau tidak diberikan izin atau arahan dari pihak teknisi TI yang bertanggung jawab.
4.1.7 Dilarang melakukan pengadaan perangkat keras tabahan jika tidak adanya izin atau perintah dari Kadiv.

Gambar 4. SOP Pengelolaan Keamanan Perangkat Keras dan Jaringan

DOI: https://doi.org/10.62017/jpmi



PT. PUNDI MAS BERJAYA			
NO. FORM		TGL. REVISI	/ /
NOMOR REVISI		TGL. REVISI	/ /
NAMA FOMULIR	Formulir perbaikan peralatan TI		
PENANGGUNG JAWAB			
WAKTU PELAKSANAAN	Tanggal :	Waktu :	

KETERANGAN KERUSAKAN	
URAIKAN KERUSAKAN	
NAMA PERANGKAT	
ESTIMASI PERBAIKAN	

KETERANGAN PERBAIKAN	
URAIAN PERBAIKAN	

KETERANGAN PENGADAAN BARANG (isi jika ada)	
KET. PERALATAN RUSAK	
KET. PENGADAAN PERALATAN	

Petugas Perbaikan

Mengetahui,
Managing Director

Gambar 5. Formulir Perbaikan Peralatan TI

PT. PUNDI MAS BERJAYA			
NO. FORM		TGL. REVISI	/ /
NOMOR REVISI		TGL. REVISI	/ /
NAMA FOMULIR	Formulir pemeliharaan Peralatan TI		
PENANGGUNG JAWAB			
WAKTU PELAKSANAAN	Tanggal :	Waktu :	

KETERANGAN PERANGKAT	
JENIS PERANGKAT TI	
JUMLAH PERANGKAT	

KETERANGAN PEMELIHARAAN	
URAIAN PEMELIHARAAN	

KONDISI PERANGKAT	
URAIAN KONDISI PERANGKAT	

Petugas Perbaikan

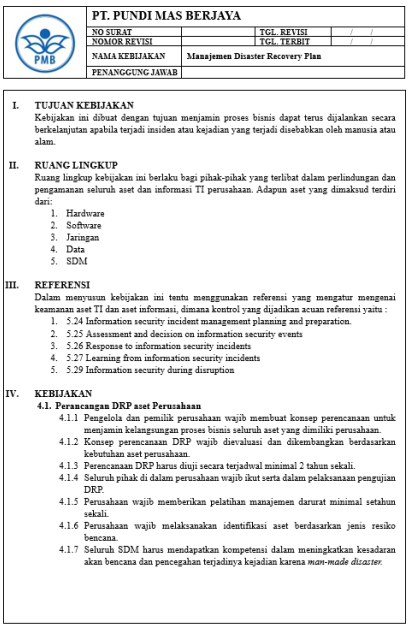
Mengetahui,
Managing Director

Gambar 6. Formulir Pemeliharaan Peralatan TI

5. SOP Manajemen Disaster Recovery Plan

Prosedur manajemen disaster recovery plan merupakan prosedur yang memastikan bahwa suatu perusahaan memiliki rencanan yang tersruktur dan efektif untuk mengidentifikasi, mengevaluasi, serta mengelola resiko yang berkaitan dengan pemulihan sistem setelah terjadinya bencana atau insiden. Tujuannya untuk melindungi keberlanjutan operasional perusahaan, melindungi data dan sumber daya, serta mengurangi risiko dan kerentanan yang dapat muncul selama insiden.

DOI: https://doi.org/10.62017/jpmi



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Manajemen Disaster Recovery Plan		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan menjamin proses bisnis dapat terus dijalankan secara berkelanjutan apabila terjadi insiden atau kejadian yang terjadi disebabkan oleh manusia atau alam.

II. RUANG LINGKUP

Ruang lingkup kebijakan ini berlaku bagi pihak-pihak yang terlibat dalam perlindungan dan pengamanan seluruh aset dan informasi TI perusahaan. Adapun aset yang dimaksud terdiri dari:

1. Hardware
2. Software
3. Jaringan
4. Data
5. SDM

III. REFERENSI

Dalam menyusun kebijakan ini tentu menggunakan referensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan referensi yaitu :

1. 5.24 Information security incident management planning and preparation.
2. 5.25 Assessment and decision on information security events
3. 5.26 Response to information security incidents
4. 5.27 Learning from information security incidents
5. 5.29 Information security during disruption

IV. KEBIJAKAN

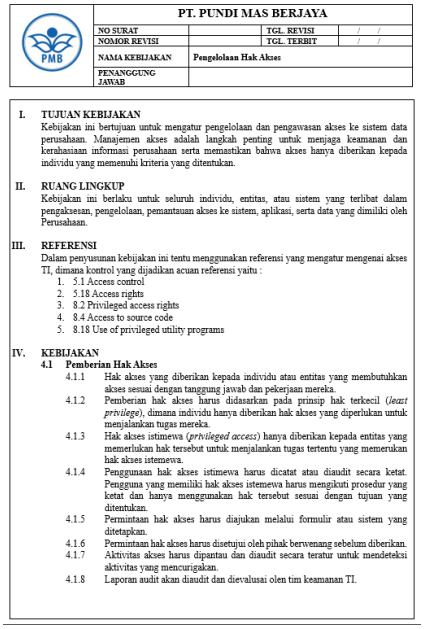
4.1. Perancangan DRP aset Perusahaan

4.1.1 Pengelola dan pemilik perusahaan wajib membuat konsep perencanaan untuk menjamin kelangsungan proses bisnis seluruh aset yang dimiliki perusahaan.
4.1.2 Konsep perencanaan DRP wajib dievaluasi dan dikembangkan berdasarkan kebutuhan aset perusahaan.
4.1.3 Perencanaan DRP harus diuji secara terjadwal minimal 2 tahun sekali.
4.1.4 Seluruh pihak di dalam perusahaan wajib ikut serta dalam pelaksanaan pengujian DRP.
4.1.5 Perusahaan wajib memberikan pelatihan manajemen darurat minimal setahun sekali.
4.1.6 Perusahaan wajib melaksanakan identifikasi aset berdasarkan jenis resiko bencana.
4.1.7 Seluruh SDM harus mendapatkan kompetensi dalam meningkatkan kesadaran akan bencana dan pencegahan terjadinya kejadian karena *man-made disaster.*

Gambar 7. SOP Manajemen Disaster Recovery Plan

6. SOP Manajemen Akses

Proses manajemen akses merupakan prosedur yang memastikan perusahaan memiliki pedoman dalam kontrol manajemen hak akses sesuai dengan kebijakan dan aturan yang ada, terutama di dalam Data Center. Tujuan dari SOP ini adalah untuk memastikan bahwa hak akses diberikan dengan benar sesuai dengan tugas dan tanggung jawab pengguna, menjaga keamanan informasi, meminimalkan risiko pelanggaran keamanan, dan memenuhi persyaratan kepatuhan dan regulasi yang berlaku.



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Pengelolaan Hak Akses		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini bertujuan untuk mengatur pengelolaan dan pengawasan akses ke sistem data perusahaan. Manajemen akses adalah langkah penting untuk menjaga keamanan dan kerahasiaan informasi perusahaan serta memastikan bahwa akses hanya diberikan kepada individu yang memenuhi kriteria yang ditentukan.

II. RUANG LINGKUP

Kebijakan ini berlaku untuk seluruh individu, entitas, atau sistem yang terlibat dalam pengaksesan, pengelolaan, pemantauan akses ke sistem, aplikasi, serta data yang dimiliki oleh Perusahaan.

III. REFERENSI

Dalam penyusunan kebijakan ini tentu menggunakan referensi yang mengatur mengenai akses TI, dimana kontrol yang dijadikan acuan referensi yaitu :

1. 5.1 Access control
2. 5.18 Access rights
3. 8.2 Privileged access rights
4. 8.4 Access to source code
5. 8.18 Use of privileged utility programs

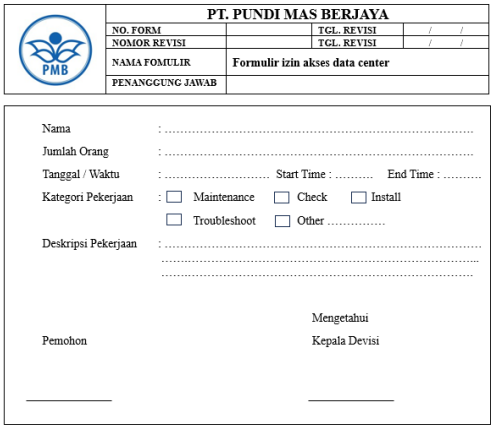
IV. KEBIJAKAN

4.1 Pemberian Hak Akses

4.1.1 Hak akses yang diberikan kepada individu atau entitas yang membutuhkan akses sesuai dengan tanggung jawab dan pekerjaan mereka.
4.1.2 Pemberian hak akses harus didasarkan pada prinsip hak terkecil (*least privilege*), dimana individu hanya diberikan hak akses yang diperlukan untuk menjalankan tugas mereka.
4.1.3 Hak akses istimewa (*privileged access*) hanya diberikan kepada entitas yang memerlukan hak tersebut untuk menjalankan tugas tertentu yang memerukan hak akses istemewa.
4.1.4 Penggunaan hak akses istimewa harus dicatat atau diaudit secara ketat. Pengguna yang memiliki hak akses istemeva harus mengikuti prosedur yang ketat dan hanya menggunakan hak tersebut sesuai dengan tujuan yang ditentukan.
4.1.5 Permintaan hak akses harus diajukan melalui formulir atau sistem yang ditetapkan.
4.1.6 Permintaan hak akses harus disetujui oleh pihak berwenang sebelum diberikan.
4.1.7 Aktivitas akses harus dipantau dan diaudit secara teratur untuk mendeteksi aktivitas yang mencurigakan.
4.1.8 Laporan audit akan diaudit dan dievalusai olen tim keamanan TI.

Gambar 8. SOP Pengelolaan Hak Akses

DOI: https://doi.org/10.62017/jpmi



PT. PUNDI MAS BERJAYA			
NO. FORM		TGL. REVISI	/ /
NOMOR REVISI		TGL. REVISI	/ /
NAMA FOMULIR	Formulir izin akses data center		
PENANGGUNG JAWAB			

Nama : .....

Jumlah Orang : .....

Tanggal / Waktu : ..... Start Time : ..... End Time : .....

Kategori Pekerjaan : ☐ Maintenance ☐ Check ☐ Install
☐ Troubleshoot ☐ Other .....

Deskripsi Pekerjaan : .....
.....
.....

Mengetahui

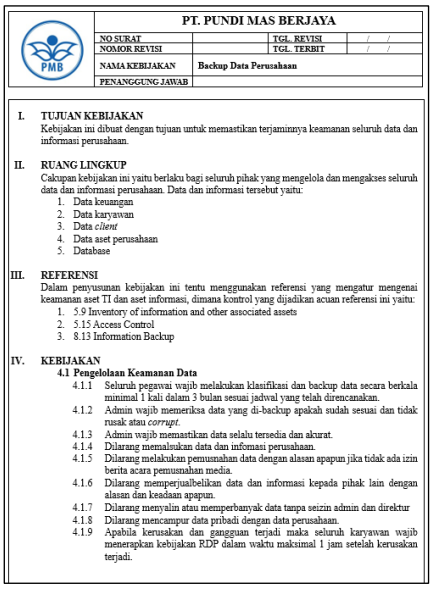
Pemohon Kepala Devisi

_____ _____

Gambar 9. Formulir Izin Akses Data Center

7. SOP Backup Data Perusahaan

Backup data perusahaan adalah tindakan mencadangkan salinan data dan informasi yang penting yang disimpan di dalam sistem komputer atau server perusahaan. Tujuan utama dari backup data adalah untuk melindungi data dari kerusakan, kehilangan, atau bencana, sehingga memastikan kelangsungan operasional, mengurangi risiko kehilangan data berharga, dan memungkinkan pemulihan cepat dalam situasi darurat.



PT. PUNDI MAS BERJAYA			
NO SURAT		TGL. REVISI	/ /
NOMOR REVISI		TGL. TERBIT	/ /
NAMA KEBIJAKAN	Backup Data Perusahaan		
PENANGGUNG JAWAB			

I. TUJUAN KEBIJAKAN

Kebijakan ini dibuat dengan tujuan untuk memastikan terjaminnya keamanan seluruh data dan informasi perusahaan.

II. RUANG LINGKUP

Cakupan kebijakan ini yaitu berlaku bagi seluruh pihak yang mengelola dan mengakses seluruh data dan informasi perusahaan. Data dan informasi tersebut yaitu:

1. Data keuangan
2. Data karyawan
3. Data *client*
4. Data aset perusahaan
5. Database

III. REFERENSI

Dalam penyusunan kebijakan ini tentu menggunakan referensi yang mengatur mengenai keamanan aset TI dan aset informasi, dimana kontrol yang dijadikan acuan referensi ini yaitu:

1. 5.9 Inventory of information and other associated assets
2. 5.15 Access Control
3. 8.13 Information Backup

IV. KEBIJAKAN

4.1 Pengelolaan Keamanan Data

4.1.1 Seluruh pegawai wajib melakukan klasifikasi dan backup data secara berkala minimal 1 kali dalam 3 bulan sesuai jadwal yang telah direncanakan.
4.1.2 Admin wajib memeriksa data yang di-backup apakah sudah sesuai dan tidak rusak atau *corrupt*.
4.1.3 Admin wajib memastikan data selalu tersedia dan akurat.
4.1.4 Dilarang memalsukan data dan informasi perusahaan.
4.1.5 Dilarang melakukan pemusnahan data dengan alasan apapun jika tidak ada izin berita acara pemusnahan media.
4.1.6 Dilarang memperjualbelikan data dan informasi kepada pihak lain dengan alasan dan keadaan apapun.
4.1.7 Dilarang menyalin atau memperbanyak data tanpa seizin admin dan direktur
4.1.8 Dilarang mencampur data pribadi dengan data perusahaan.
4.1.9 Apabila kerusakan dan gangguan terjadi maka seluruh karyawan wajib menerapkan kebijakan RDP dalam waktu maksimal 1 jam setelah kerusakan terjadi.

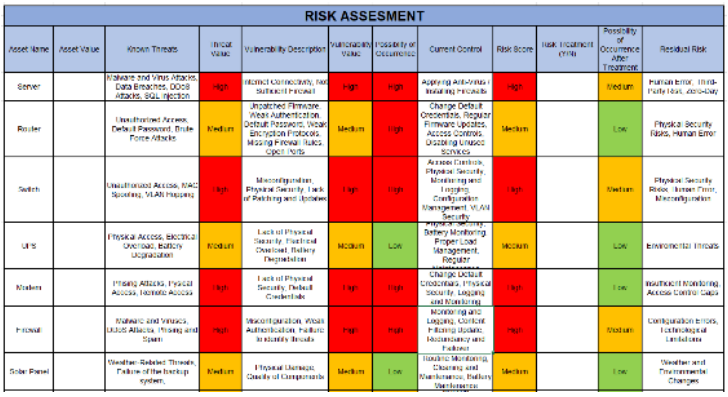
Gambar 10. SOP Backup Data Perusahaan

B. Analisis Risk Assessment

Risk assessment merupakan proses sistematis untuk mengidentifikasi, mengevaluasi, dan menganalisis potensi risiko yang terkait dengan suatu aktivitas atau proyek. Tahapan-tahapan dalam risk assessment meliputi identifikasi risiko, evaluasi terhadap dampak dan kemungkinan terjadinya risiko, serta analisis terhadap faktor-faktor yang mempengaruhi risiko tersebut. Tujuannya adalah untuk menetapkan langkah-langkah pengendalian risiko yang sesuai guna mengurangi dampak negatif yang mungkin timbul. Dengan melakukan risk assessment secara teratur, sebuah organisasi dapat memahami dan mengelola risiko-risiko yang mereka hadapi dalam rangka mencapai tujuan mereka (Hegde and Rokseth 2020).

DOI: https://doi.org/10.62017/jpmi

Adapun hasil dari analisis risk assessment pada PT. PMB akan memberikan gambaran yang jelas mengenai risiko-risiko yang diidentifikasi, evaluasi dampak dan kemungkinan terjadinya risiko tersebut, serta rekomendasi untuk langkah-langkah pengendalian risiko yang efektif.



RISK ASSESMENT											
Asset Name	Asset Value	Known Threats	Threat Value	Vulnerability Description	Vulnerability Value	Possibility of Occurrence	Current Control	Risk Score	Risk Treatment (RTR)	Possibility Occurrence After Treatment	Residual Risk
Server		Malware and Virus Attacks, Data Breaches, DDOS Attacks, SQL Injection	High	Incorrect Connectivity, Not Subscribe Firewall	High	High	Applying Anti-Virus / Installing Firewalls	High		Medium	Human Error, Third-Party Risk, Zero-Day
Router		Unauthorized Access, Default Password, Brute Force Attacks	Medium	Unpatched Firmware, Weak Authentication, Default Password, Weak Encryption Protocols, Missing Firewall Rules, Open Ports	Medium	High	Change Default Credentials, Regular Firmware Updates, Access Control, Disabling Unused Services	Medium		Low	Physical Security Risks, Human Error
Switch		Unauthorized Access, MAC Spoofing, VLAN Hopping	High	Misconfiguration, Physical Security, Lack of Patching and Updates	High	High	Access Controls, Physical Security, Monitoring and Logging, Configuration Management, VLAN Security	High		Medium	Physical Security Risks, Human Error, Misconfiguration
UPS		Physical Access, Electrical Overload, Battery Degradation	Medium	Lack of Physical Security, Electrical Overload, Battery Degradation	Medium	Low	Physical Security, Battery Monitoring, Proper Load Management, Regular	Medium		Low	Environmental Threats
Modem		Phising Attacks, Physical Access, Remote Access	High	Lack of Physical Security, Default Credentials	High	High	Change Default Credentials, Physical Security, Logging and Monitoring	High		Low	Insufficient Monitoring, Access Control Gaps
Firewall		Malware and Viruses, DDoS Attacks, Phising and Spam	High	Misconfiguration, Weak Authentication, Failure to Identify Threats	High	High	Monitoring and Logging, Content Filtering Updates, Redundancy and Failover	High		Medium	Configuration Errors, Technological Limitations
Solar Panel		Weather-Related Threats, Failure of the backup system,	Medium	Physical Damage, Quality of Components	Medium	Low	Routine Monitoring, Cleaning and Maintenance, Battery Maintenance	Medium		Low	Weather and Environmental Changes

Gambar 11. Hasil Analisis Risk Assessment

Dari gambar yang disajikan, terlihat bahwa gambar tersebut merupakan hasil identifikasi terhadap sejumlah potensi ancaman yang mungkin mengarah pada kerugian terhadap aset-aset yang dimiliki oleh PT. PMB. Selain itu, gambar tersebut juga memberikan penjelasan terkait dengan berbagai langkah pengendalian yang telah diterapkan untuk mengurangi risiko-risiko yang teridentifikasi tersebut.

Dalam konteks manajemen risiko, identifikasi ancaman merupakan langkah awal yang penting untuk memahami potensi gangguan atau kerugian yang mungkin dihadapi oleh suatu organisasi. Gambar tersebut memberikan gambaran yang jelas mengenai jenis-jenis ancaman yang dihadapi oleh PT. PMB, seperti serangan malware, pelanggaran data, akses tidak sah, dan lain sebagainya. Hal ini memungkinkan perusahaan untuk mengambil langkah-langkah pencegahan yang tepat guna mengurangi potensi dampak negatif yang mungkin timbul.

Selain identifikasi ancaman, gambar tersebut juga menggambarkan sejumlah kontrol yang telah diterapkan oleh PT. PMB sebagai langkah-langkah mitigasi risiko. Kontrol-kontrol ini meliputi berbagai langkah teknis, seperti penggunaan perangkat lunak anti-malware, firewall, dan kontrol akses, serta langkah-langkah non-teknis seperti prosedur keamanan fisik dan kesadaran pelatihan karyawan. Penggunaan kontrol-kontrol ini diharapkan dapat mengurangi probabilitas terjadinya ancaman serta mengurangi dampaknya jika ancaman tersebut terjadi.

Secara keseluruhan, gambar tersebut merupakan alat yang efektif dalam membantu PT. PMB dalam mengidentifikasi dan mengelola risiko-risiko yang terkait dengan aset-aset mereka. Dengan pemahaman yang lebih baik mengenai ancaman yang dihadapi dan langkah-langkah pengendalian yang telah diterapkan, perusahaan dapat meningkatkan kemampuannya untuk melindungi aset-aset mereka serta mencapai tujuan bisnis mereka dengan lebih aman dan efisien.

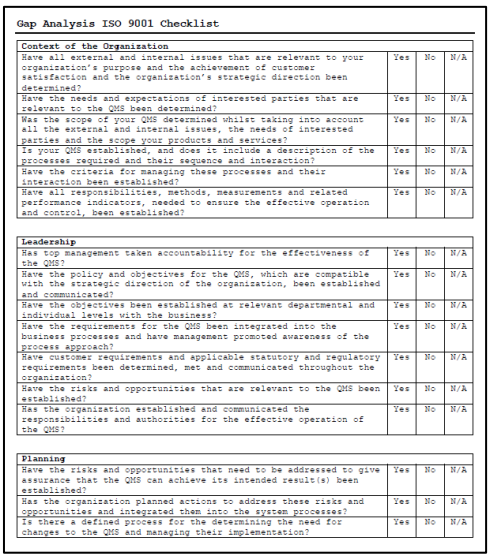
C. Dokumen Pendukung QMS, ISMS, ITSM

1. Dokumen Pendukung QMS

   Sistem Manajemen Kualitas (QMS), dikenal juga sebagai Quality Management System, adalah sebuah kerangka kerja yang diterapkan oleh organisasi untuk mengelola dan meningkatkan mutu produk atau layanan yang mereka sediakan. QMS melibatkan penetapan proses-proses, kebijakan, dan prosedur-prosedur yang dirancang khusus untuk memastikan bahwa produk atau layanan memenuhi standar kualitas yang telah ditetapkan. Dengan adopsi QMS, organisasi dapat secara sistematis mengidentifikasi, menganalisis, dan memperbaiki proses-proses yang ada guna meningkatkan kepuasan pelanggan dan efisiensi operasional. Penting untuk dicatat bahwa implementasi QMS sering kali merujuk pada standar internasional seperti ISO 9001, yang memberikan

DOI: https://doi.org/10.62017/jpmi

panduan terstandarisasi bagi organisasi dalam menerapkan prinsip-prinsip QMS (Ummu 2023). Selain itu, QMS juga merupakan salah satu dokumen pendukung yang penting dalam memenuhi persyaratan untuk pengajuan sertifikasi ISO 27001, sebuah langkah yang ingin diambil oleh PT Pundi Mas Berjaya. Berikut merupakan Gap Analysis Checklist yang ada pada ISO 9001.



Gap Analysis ISO 9001 Checklist

Context of the Organization			
Have all external and internal issues that are relevant to your organization's purpose and the achievement of customer satisfaction and the organization's strategic direction been determined?	Yes	No	N/A
Have the needs and expectations of interested parties that are relevant to the QMS been determined?	Yes	No	N/A
Was the scope of your QMS determined whilst taking into account all the external and internal issues, the needs of interested parties and the scope your products and services?	Yes	No	N/A
Is your QMS established, and does it include a description of the processes required and their sequence and interaction?	Yes	No	N/A
Have the criteria for managing these processes and their interaction been established?	Yes	No	N/A
Have all responsibilities, methods, measurements and related performance indicators, needed to ensure the effective operation and control, been established?	Yes	No	N/A

Leadership			
Has top management taken accountability for the effectiveness of the QMS?	Yes	No	N/A
Have the policy and objectives for the QMS, which are compatible with the strategic direction of the organization, been established and communicated?	Yes	No	N/A
Have the objectives been established at relevant departmental and individual levels with the business?	Yes	No	N/A
Have the requirements for the QMS been integrated into the business processes and have management promoted awareness of the process approach?	Yes	No	N/A
Have customer requirements and applicable statutory and regulatory requirements been determined, met and communicated throughout the organization?	Yes	No	N/A
Have the risks and opportunities that are relevant to the QMS been established?	Yes	No	N/A
Has the organization established and communicated the responsibilities and authorities for the effective operation of the QMS?	Yes	No	N/A

Planning			
Have the risks and opportunities that need to be addressed to give assurance that the QMS can achieve its intended result(s) been established?	Yes	No	N/A
Has the organization planned actions to address these risks and opportunities and integrated them into the system processes?	Yes	No	N/A
Is there a defined process for the determining the need for changes to the QMS and managing their implementation?	Yes	No	N/A

Gambar 12. Template Checklist QMS

2. Dokumen Pendukung ISMS

ISMS, atau Sistem Manajemen Keamanan Informasi, merupakan kerangka kerja yang digunakan oleh organisasi untuk mengelola keamanan informasi secara menyeluruh. Ini melibatkan penetapan kebijakan, prosedur, dan kontrol keamanan informasi untuk melindungi informasi dari ancaman dan risiko. Tujuannya adalah untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi serta mengurangi risiko keamanan informasi yang mungkin dihadapi oleh organisasi (Susanto and Almunawar 2018). Implementasi ISMS sering didasarkan pada standar internasional seperti ISO/IEC 27001. Berikut merupakan ISMS ISO 27001 checklist sebagai dokumen pendukung syarat pengajuan sertifikasi untuk PT. PMB.

DOI: https://doi.org/10.62017/jpmi

ISO 27001:2022 Checklist		
Clause 4 : Context of the organization		
4.1 Understanding the organization and its context		
Has the organization determined external and internal issues that are relevant to your purpose and that affected its ability to achieve the intended outcomes of your information security management system?		
4.2 Understanding the needs and expectations of interested parties		
Has the organization determined the interested parties that are relevant to the information security Management System?		
Has the organization determined the relevant requirements of these interested parties?		
Has the organization determined which of these requirements will be addressed through the information security management system?		
4.3 Determining the scope of the Information Security management system		
Has the organization established the boundaries and applicability of the information security management system to establish its scope?		
When determining the scope of the information security management system has the organization considered the external and internal issues referred to clause 4.1 and also considered the relevant ISMS requirements of interested parties as referred in clause 4.2?		
While determining the scope, has the organization determined the interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations?		
Is the organization's scope made available as a Documented		

Gambar 13. Template Checklist ISMS

3. Dokumen Pendukung ITSM

ITSM, atau Manajemen Layanan Teknologi Informasi, adalah kerangka kerja yang digunakan untuk merencanakan, merancang, mengimplementasikan, dan mengelola layanan TI dalam sebuah organisasi. Tujuannya adalah untuk meningkatkan kualitas layanan TI, memastikan kepuasan pengguna, dan meningkatkan efisiensi operasional. Dengan menerapkan ITSM, organisasi dapat mengoptimalkan penggunaan sumber daya TI, mengurangi waktu tidak aktif sistem, dan merespons kebutuhan bisnis secara lebih baik (Serrano et al. 2021). Kerangka kerja ITSM sering didasarkan pada standar industri seperti ITIL (Information Technology Infrastructure Library). Berikut dokumen pendukung Information Technology Service Management (ITSM) dari PT. PMB.

Information Technology Service Management (ITSM) from PT. Pundi Mas Berjaya proposal	
Section	**Details/Description**
Introduction	Our organization, Cloudbank, is a leading provider of cloud hosting services, specializing in secure and scalable solutions for businesses of all sizes in Batam. With a commitment to excellence and innovation, we are seeking proposals for an IT Service Management (ITSM) solution to enhance our service delivery capabilities.
	The purpose of this RFP is to identify a qualified vendor to provide an integrated ITSM solution that aligns with our cloud hosting services, streamlining processes, ensuring efficient incident resolution, and improving overall service quality.
Project Overview	Project scope: The project involves the implementation of a robust ITSM solution tailored to our cloud hosting services. The scope includes incident, problem, and change management, service request and catalog management, knowledge management, and comprehensive reporting and analytics.
	Project Goals: Our primary objectives for this project include improving service response times, enhancing customer satisfaction, and ensuring the seamless integration of the ITSM solution as well as reasonable price with our existing cloud hosting infrastructure.
Proposal Requirements	Company Overview: We invite vendors to provide a detailed overview of their company, including its history, size, core competencies, and experience in delivering ITSM solutions.
	Relevant Experience and Case Studies: Please share examples of your company's relevant experience, particularly instances where your ITSM solution has been successfully implemented in conjunction with cloud hosting services.
	Proposed Solution: Vendors should outline their proposed ITSM solution, emphasizing its adaptability to our cloud hosting environment and its capacity to meet our specific service management needs.
	Implementation Timeline and Methodology: Provide a detailed timeline for the implementation of the ITSM solution, along with an explanation of the methodology you will
	Pricing and Licensing: Please submit a comprehensive breakdown of pricing, licensing details, and any additional costs associated with the proposed ITSM solution.
Technical Requirements	Integration with Existing Systems: The ITSM solution must seamlessly integrate with our existing systems (e.g. LDAP and IT Asset Management (ITAM) tools).
	Support for Multiple Platforms: Ensure that the ITSM solution supports multiple platforms, with a particular emphasis on compatibility with our cloud hosting environment.
	Mobile Access and Support: The solution should provide secure and user-friendly mobile access to support our on-the-go teams.
	Customization Options: Detail the level of customization the ITSM solution offers, allowing us to tailor it to our specific cloud hosting service requirements.
	Customization, Security, and Compliance Features: The ITSM solution is expected to excel in both customization and security aspects. It must allow for a high degree of customization, enabling seamless adaptation to our unique cloud hosting service requirements. This includes the ability to tailor workflows, forms, and user interfaces to align with our specific business processes. Simultaneously, the solution should prioritize security and compliance, incorporating robust access controls, encryption mechanisms, and strict adherence to industry standards like GDPR and HIPAA. In addition, the inclusion of comprehensive audit trails and reporting functionalities is crucial to ensure continuous compliance with regulatory requirements. This integrated approach ensures that the ITSM solution not only meets our specific operational needs but also establishes a secure and compliant foundation for our

Gambar 14. Dokumen ITSM

Bagian hasil penelitian memuat hasil analisis uji hipotesis yang dapat menyertakan tabel, grafik, dan sebagainya. Pembahasan memuat interpretasi dan evaluasi terhadap hasil penelitian, serta ulasan berbagai permasalahan terkait yang dipandang dapat memengaruhi hasil penelitian. Deskripsi pada bagian ini menitikberatkan pada analisis

secara kritis secara substansial terhadap hasil penelitian, selain itu ditambahkan juga kelemahan dalam penelitian.

KESIMPULAN

Persiapan sertifikasi ISO 27001 di PT Pundi Mas Berjaya menunjukkan komitmen perusahaan terhadap keamanan informasi, dengan fokus pada perlindungan data melalui penyusunan SOP, penilaian risiko, dan pengumpulan dokumen pendukung. Menggunakan kerangka kerja ISMS dan QMS, perusahaan memastikan standar keamanan informasi dan manajemen kualitas terpenuhi. Kolaborasi antara berbagai departemen dan pemangku kepentingan menunjukkan komitmen seluruh organisasi. Sertifikasi ini akan meningkatkan kredibilitas PT. PMB di mata pelanggan dan mitra bisnis dengan memenuhi standar internasional perlindungan data.

DAFTAR PUSTAKA

Culot, Giovanna, Guido Nassimbeni, Matteo Podrecca, and Marco Sartor. 2021. "The ISO/IEC 27001 Information Security Management Standard: Literature Review and Theory-Based Research Agenda." *TQM Journal* 33(7):76–105.

Dr. Muhammad Ramdhan, S. Pd. ,. M. M. 2021. *METODE PENELITIAN*. Vol. vol.1. edited by A. A. Effendy. Surabaya: Cipta Media Nusantara.

Hegde, Jeevith, and Børge Rokseth. 2020. "Applications of Machine Learning Methods for Engineering Risk Assessment – A Review." *Safety Science* 122(October 2019):104492. doi: 10.1016/j.ssci.2019.09.015.

Muhaling, A. R., I D Palandeng, J S B Sumarauw, Oleh :. Anjas, Rovian Muhaling, Indrie D Palandeng, Jacky S B Sumarauw, Jurusan Manajemen, Fakultas Ekonomi, and Dan Bisnis. 2021. "IMPLEMENTASI STANDAR OPERASIONAL PROSEDUR (SOP) LAYANAN PADA PT. TASPEN (PESERO) CABANG MANADO IMPLEMENTATION OF STANDARD OPERATING PROCEDURES (SOP) SERVICES IN PT. TASPEN (PERSERO) CABANG MANADO." 9:572–81.

pmberjaya.com. 2024. "PT. Pundi Mas Berjaya About Us." Retrieved July 30, 2024 (https://www.pmberjaya.com/#about_us).

Serrano, João, João Faustino, Daniel Adriano, Rúben Pereira, and Miguel Mira da Silva. 2021. "An It Service Management Literature Review: Challenges, Benefits, Opportunities and Implementation Practices." *Information (Switzerland)* 12(3).

Susanto, H., and M. N. Almunawar. 2018. *Information Security Management Systems: A Novel Framework and Software as a Tool for Compliance with Information Security Standard*. Apple Academic Press.

Ummu. 2023. "Mengenal Quality Management System (QMS): Pengertian Hingga Implementasi Di Perusahaan." *Idmetafora*. Retrieved February 17, 2024 (https://idmetafora.com/id/blog/read/3954/Mengenal-Quality-Management-System-QMS-Pengertian-hingga-Implementasi-di-Perusahaan.html).