ANALISIS DAN IMPLEMENTASI SISTEM MANAJEMEN KEAMANAN INFORMASI (SMKI) BERDASARKAN ISO/IEC 27001 PADA DIVISI TEKNOLOGI INFORMASI UNIVERSITAS HOGWARTS

Disusun Oleh:

Faza Adhima Putra 221011402177

Alfiana Supriyanti 221011401935

PROGRAM STUDI TEKNIKINFORMATIKA

FAKULTAS ILMU KOMPUTER

UNIVERSITAS PAMULANG

TANGERANG SELATAN

2025

DAFTAR ISI

BAB I

PENDAHULUAN

1.1 Latar Belakang

Dalam era digital yang semakin maju, informasi telah menjadi salah satu aset paling berharga bagi setiap organisasi, termasuk lembaga pendidikan tinggi. Universitas sebagai institusi penghasil ilmu pengetahuan dan pusat kegiatan akademik memiliki tanggung jawab besar dalam mengelola dan melindungi informasi yang mereka miliki. Informasi tersebut tidak hanya mencakup data akademik mahasiswa dan dosen, tetapi juga hasil penelitian, data administrasi, keuangan, sumber daya manusia, serta infrastruktur teknologi yang menopang kegiatan operasional kampus.

Seiring dengan transformasi digital di dunia pendidikan, hampir seluruh aktivitas kampus kini terintegrasi melalui sistem informasi berbasis teknologi. Proses pendaftaran mahasiswa, pengelolaan nilai, keuangan, hingga sistem pembelajaran daring (Learning Management System/LMS) semuanya berbasis digital dan terhubung dengan jaringan internet. Kemajuan ini membawa banyak manfaat — mulai dari efisiensi waktu, peningkatan aksesibilitas data, hingga kemudahan komunikasi antar-civitas akademika.

Namun, di sisi lain, kemajuan teknologi informasi juga membuka peluang munculnya berbagai ancaman keamanan informasi. Lembaga pendidikan tinggi kini menjadi salah satu target utama serangan siber, karena mengelola data dalam jumlah besar dan bernilai tinggi. Ancaman tersebut dapat berupa serangan malware, peretasan (hacking), phishing, ransomware, sabotase sistem, serta penyalahgunaan akses internal oleh pihak yang tidak berwenang. Selain ancaman eksternal, faktor internal seperti kelalaian pengguna, lemahnya pengaturan akses, dan kurangnya kesadaran terhadap keamanan siber juga menjadi penyebab utama terjadinya kebocoran data di lingkungan universitas.

Hasil riset global oleh IBM Security (2024) menunjukkan bahwa sektor pendidikan termasuk dalam lima besar sektor dengan tingkat kebocoran data tertinggi di dunia, dengan sekitar 25% insiden disebabkan oleh kesalahan manusia dan 30% diakibatkan oleh sistem yang tidak diperbarui secara rutin. Hal ini memperlihatkan bahwa keamanan informasi bukan hanya menjadi tanggung jawab tim teknis, tetapi merupakan tanggung jawab bersama seluruh elemen organisasi. Setiap individu di lingkungan universitas — mulai dari pimpinan, dosen, staf administrasi, hingga mahasiswa — memiliki peran penting dalam menjaga keamanan data dan integritas sistem akademik.

Universitas Hogwarts, sebagai salah satu universitas swasta terkemuka di Indonesia yang berfokus pada bidang teknologi, sains, dan bisnis digital, menghadapi tantangan yang sama dalam menjaga keamanan informasi di lingkungan kampus. Peningkatan jumlah mahasiswa,

dosen, dan proyek penelitian yang menggunakan sistem digital menyebabkan volume data yang dikelola semakin besar. Kondisi ini meningkatkan risiko terhadap kebocoran data, gangguan sistem, maupun serangan siber.

Beberapa insiden seperti percobaan akses ilegal terhadap sistem akademik, serangan phishing terhadap akun email dosen, serta gangguan jaringan akibat serangan DDoS (Distributed Denial of Service) pernah terjadi dan mengganggu operasional kampus untuk sementara waktu. Meskipun penanganan cepat telah dilakukan oleh Divisi Teknologi Informasi (IT Division), insiden tersebut menunjukkan perlunya pendekatan yang lebih sistematis, terukur, dan berkelanjutan dalam pengelolaan keamanan informasi universitas.

Untuk menjawab tantangan tersebut, Universitas Hogwarts berkomitmen untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan standar internasional ISO/IEC 27001:2022. Standar ini menyediakan kerangka kerja komprehensif bagi organisasi untuk menetapkan, mengimplementasikan, memelihara, dan terus meningkatkan sistem keamanan informasi secara berkelanjutan (*continuous improvement*).

ISO/IEC 27001 menekankan pada tiga pilar utama keamanan informasi, yaitu:

1. Kerahasiaan (Confidentiality) – memastikan bahwa informasi hanya dapat diakses oleh pihak yang memiliki otorisasi.
2. Integritas (Integrity) – menjamin bahwa data tetap akurat, lengkap, dan tidak diubah secara tidak sah.
3. Ketersediaan (Availability) – memastikan bahwa sistem dan informasi tersedia setiap saat saat dibutuhkan oleh pengguna yang berwenang.

Dengan penerapan ISO/IEC 27001, Universitas Hogwarts diharapkan dapat mengurangi risiko kebocoran data, meningkatkan keandalan sistem informasi akademik, serta memperkuat kepercayaan seluruh stakeholder seperti mahasiswa, dosen, mitra industri, dan pemerintah. Selain itu, penerapan standar ini juga mendukung kepatuhan universitas terhadap regulasi nasional, khususnya Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP), yang mewajibkan setiap lembaga untuk melindungi data pribadi individu dalam sistem mereka.

Implementasi SMKI berbasis ISO/IEC 27001 tidak hanya memberikan manfaat dalam aspek teknis, tetapi juga manfaat manajerial dan strategis. Melalui SMKI, universitas dapat:

- Menetapkan tanggung jawab keamanan informasi yang jelas antar-unit kerja.
- Membangun prosedur standar operasional (SOP) yang terdokumentasi dengan baik.
- Meningkatkan kesadaran dan kompetensi keamanan siber bagi seluruh pengguna sistem.

- Memastikan seluruh proses pengelolaan data sejalan dengan prinsip tata kelola yang baik (*good governance*).

Dengan latar belakang tersebut, penerapan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001 di Divisi Teknologi Informasi Universitas Hogwarts menjadi langkah strategis dan relevan untuk menjawab kebutuhan keamanan digital masa kini. Melalui tahapan analisis konteks organisasi, identifikasi risiko, pemilihan kontrol keamanan, dan penyusunan dokumen kebijakan serta prosedur, universitas diharapkan dapat membangun sistem keamanan informasi yang matang (*information security maturity*).

Pada akhirnya, penerapan SMKI ini akan memastikan bahwa seluruh data akademik, administratif, dan penelitian di Universitas Hogwarts dapat terlindungi dengan baik, mendukung terciptanya lingkungan pendidikan yang aman, terpercaya, dan berkelanjutan di era transformasi digital.

1.2 Tujuan

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) **berbasis** ISO/IEC 27001 di Universitas Hogwarts bertujuan untuk menciptakan tata kelola keamanan informasi yang terukur, terdokumentasi, dan berkelanjutan. Dalam konteks lembaga pendidikan tinggi, keamanan informasi memiliki peran strategis dalam memastikan bahwa seluruh proses akademik, administratif, dan penelitian berjalan dengan aman, efisien, serta sesuai dengan standar tata kelola teknologi informasi yang baik (*good IT governance*).

Keamanan informasi di lingkungan universitas tidak hanya berfokus pada perlindungan data dari ancaman eksternal seperti serangan siber, tetapi juga mencakup pengelolaan internal yang sistematis terhadap kebijakan, prosedur, serta perilaku pengguna dalam memanfaatkan sistem informasi kampus. Pendekatan menyeluruh ini diperlukan agar setiap unit di dalam organisasi memiliki tanggung jawab dan kesadaran yang sama terhadap pentingnya keamanan data.

Secara umum, tujuan utama dari analisis dan implementasi SMKI di Universitas Hogwarts adalah sebagai berikut:

1. Menganalisis konteks organisasi Divisi Teknologi Informasi (IT Division) – memahami kondisi internal dan eksternal yang memengaruhi keamanan informasi, termasuk aspek teknologi, kebijakan universitas, budaya kerja, serta regulasi nasional terkait perlindungan data pribadi dan keamanan siber.
2. Mengidentifikasi aset informasi penting yang dimiliki universitas, seperti data akademik, server pusat data, sistem informasi akademik (SIAKAD), jaringan kampus, sistem keuangan, serta data penelitian. Setiap aset akan diklasifikasikan berdasarkan nilai bisnis, sensitivitas, dan tingkat kritikalitasnya terhadap keberlangsungan operasional universitas.

3. Menentukan potensi ancaman dan kerentanan (vulnerability) yang dapat memengaruhi keamanan data, baik yang berasal dari luar organisasi (misalnya serangan malware, phishing, atau peretasan) maupun dari dalam organisasi (seperti kesalahan manusia, kelalaian prosedur, atau penyalahgunaan hak akses).
4. Melakukan penilaian risiko (risk assessment) terhadap setiap aset informasi dengan menilai tingkat dampak (*impact*) dan kemungkinan (*likelihood*) dari setiap ancaman yang teridentifikasi. Hasil analisis risiko ini akan menjadi dasar dalam menentukan prioritas tindakan mitigasi dan kontrol keamanan yang tepat guna mengurangi potensi kerugian informasi.
5. Merancang kerangka kontrol keamanan informasi berdasarkan *Annex A* dari ISO/IEC 27001:2022, yang mencakup aspek kebijakan, tanggung jawab keamanan, manajemen aset, kontrol akses, kriptografi, keamanan fisik, proteksi terhadap malware, keamanan jaringan, serta kepatuhan terhadap peraturan perundangan.
6. Menyusun dokumen-dokumen utama SMKI, seperti *Kebijakan Keamanan Informasi (Information Security Policy)*, *Tujuan Keamanan (Security Objectives)*, dan *Rencana Implementasi (Implementation Plan)*. Dokumen-dokumen tersebut berfungsi sebagai pedoman resmi dalam pelaksanaan, evaluasi, dan peningkatan sistem keamanan informasi universitas secara berkelanjutan.
7. Memberikan rekomendasi strategis bagi universitas dalam memperkuat budaya keamanan siber di seluruh lapisan civitas akademika melalui pelatihan, audit internal, dan program peningkatan kesadaran (*security awareness training*). Dengan langkah ini, universitas diharapkan dapat meminimalkan risiko kesalahan pengguna serta meningkatkan kesiapan dalam menghadapi ancaman digital.
8. Mempersiapkan universitas menuju sertifikasi ISO/IEC 27001, sebagai bukti bahwa sistem keamanan informasi Universitas Hogwarts telah memenuhi standar internasional. Sertifikasi ini tidak hanya menjadi simbol kepatuhan terhadap regulasi global, tetapi juga memperkuat reputasi universitas sebagai lembaga pendidikan tinggi yang profesional, modern, dan terpercaya dalam pengelolaan data dan sistem informasi.

Secara keseluruhan, penerapan SMKI berbasis ISO/IEC 27001 di Universitas Hogwarts bukan hanya ditujukan untuk memperoleh sertifikasi formal, melainkan untuk membangun budaya keamanan informasi (information security culture) yang melekat pada seluruh aktivitas kampus. Dengan budaya ini, setiap dosen, mahasiswa, dan tenaga kependidikan diharapkan memiliki tanggung jawab bersama dalam menjaga kerahasiaan, integritas, dan ketersediaan informasi universitas, serta menggunakan teknologi secara aman, etis, dan bertanggung jawab.

1.3 Ruang Lingkup

Ruang lingkup penerapan Sistem Manajemen Keamanan Informasi (SMKI) di Universitas Hogwarts difokuskan pada pengelolaan dan perlindungan seluruh informasi digital yang terkait dengan kegiatan akademik, penelitian, dan administrasi kampus. SMKI ini dikembangkan untuk

memastikan bahwa seluruh sistem informasi dan data yang digunakan oleh civitas akademika terlindungi dari ancaman, disalahgunakan, atau diakses oleh pihak yang tidak berwenang.

Sebagai lembaga pendidikan tinggi dengan jumlah pengguna yang besar dan aktivitas digital yang kompleks, Universitas Hogwarts memiliki berbagai sistem informasi dan aset data yang terhubung satu sama lain. Oleh karena itu, ruang lingkup SMKI mencakup proses, infrastruktur, manusia, serta kebijakan dan prosedur yang mendukung pengelolaan keamanan informasi di lingkungan kampus.

Adapun rincian ruang lingkup implementasi SMKI di Universitas Hogwarts adalah sebagai berikut:

1. Area Operasional dan Infrastruktur Teknologi Informasi

SMKI mencakup seluruh area operasional yang dikelola oleh Divisi Teknologi Informasi (IT Division), yang memiliki tanggung jawab terhadap penyediaan, pemeliharaan, dan keamanan infrastruktur teknologi universitas.

Cakupan infrastruktur meliputi:

- Server pusat data (data center) dan server cadangan (backup server) yang menampung seluruh sistem akademik, keuangan, dan administrasi.
- Jaringan lokal (LAN) dan jaringan nirkabel (Wi-Fi kampus) yang digunakan oleh mahasiswa, dosen, dan staf untuk aktivitas belajar mengajar dan komunikasi internal.
- Perangkat jaringan seperti router, switch, firewall, serta sistem *Intrusion Detection and Prevention (IDS/IPS)*.
- Perangkat endpoint (komputer, laptop, printer, scanner, dan perangkat mobile universitas) yang digunakan oleh pengguna sistem.
- Sistem penyimpanan cloud internal dan eksternal yang dikelola secara terpusat oleh Divisi IT.

Semua komponen infrastruktur tersebut menjadi bagian dari SMKI dan harus dikelola sesuai dengan kebijakan keamanan informasi universitas.

2. Sistem Informasi dan Aplikasi Akademik

SMKI mencakup pengelolaan dan perlindungan terhadap seluruh sistem dan aplikasi berbasis digital yang digunakan untuk mendukung kegiatan akademik dan administrasi kampus, antara lain:

- Sistem Informasi Akademik (SIAKAD) – mencakup data mahasiswa, jadwal kuliah, nilai, absensi, dan kegiatan perkuliahan.
- Learning Management System (LMS) – digunakan untuk pembelajaran daring dan penyimpanan materi kuliah digital.
- Portal Dosen dan Mahasiswa – digunakan untuk akses informasi akademik dan komunikasi resmi.
- Sistem Keuangan dan Sumber Daya Manusia (HRD) – mengelola data keuangan, gaji, dan administrasi pegawai.
- Sistem Penelitian dan Pengabdian – mencatat aktivitas riset dan publikasi ilmiah universitas.
- Layanan email institusional dan komunikasi digital yang digunakan oleh seluruh civitas akademika.

Setiap sistem tersebut wajib memenuhi standar keamanan minimum, termasuk penggunaan autentikasi ganda (*multi-factor authentication*), enkripsi data, serta audit log yang terdokumentasi.

3. Aset Informasi

Ruang lingkup SMKI juga meliputi seluruh aset informasi yang dikelola, disimpan, atau ditransmisikan oleh universitas, baik dalam bentuk digital maupun non-digital.

Aset informasi yang termasuk dalam cakupan SMKI antara lain:

- Data pribadi mahasiswa, dosen, dan staf (biodata, nilai, riwayat akademik, dan data kepegawaian).
- Data keuangan universitas dan laporan keuangan tahunan.
- Hasil penelitian, publikasi ilmiah, dan dokumen kerja sama.
- Dokumen kebijakan, arsip administratif, serta kontrak dengan pihak ketiga.
- Data jaringan dan log aktivitas pengguna yang berkaitan dengan keamanan siber.

Setiap aset informasi akan diklasifikasikan berdasarkan tingkat sensitivitas dan kepentingannya terhadap keberlangsungan operasional universitas. Aset dengan klasifikasi kritis akan diberikan perlindungan tambahan, seperti sistem backup terenkripsi dan kontrol akses terbatas.

4. Proses Manajemen Keamanan Informasi

Ruang lingkup SMKI mencakup seluruh proses manajemen keamanan yang dilakukan di universitas, antara lain:

- Kebijakan dan prosedur keamanan informasi – panduan tertulis mengenai tata kelola keamanan data dan sistem.
- Penilaian risiko (risk assessment) – proses identifikasi dan evaluasi risiko yang dapat memengaruhi aset informasi.
- Mitigasi dan pengendalian risiko (risk treatment) – penerapan kontrol teknis dan administratif untuk mengurangi dampak risiko.
- Manajemen insiden keamanan informasi – prosedur pelaporan, penanganan, dan pelaporan insiden siber.
- Proses audit internal dan review manajemen – untuk memastikan efektivitas penerapan SMKI dan peningkatan berkelanjutan (*continuous improvement*).

Dengan cakupan tersebut, universitas dapat mengelola risiko secara terukur dan memastikan bahwa seluruh langkah pengamanan berjalan sesuai dengan prinsip ISO/IEC 27001.

5. Sumber Daya Manusia dan Kepatuhan

SMKI di Universitas Hogwarts juga mencakup pengelolaan sumber daya manusia (SDM) yang memiliki akses terhadap sistem informasi universitas. Setiap dosen, staf, dan pihak ketiga (vendor) wajib:

- Menandatangani perjanjian kerahasiaan (non-disclosure agreement).
- Mengikuti pelatihan keamanan informasi yang diselenggarakan minimal dua kali dalam setahun.
- Mematuhi seluruh kebijakan keamanan data dan penggunaan sistem TI universitas.

Selain itu, SMKI juga memastikan kepatuhan universitas terhadap regulasi dan standar yang berlaku, antara lain:

- ISO/IEC 27001:2022 – standar internasional keamanan informasi.
- ISO/IEC 27002:2022 – panduan kontrol keamanan informasi.
- Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).
- Peraturan Menteri Pendidikan, Kebudayaan, Riset, dan Teknologi terkait keamanan siber dan perlindungan data di lembaga pendidikan.

6. Batasan dan Pengecualian

Untuk menjaga fokus penerapan, ruang lingkup SMKI tidak mencakup sistem atau aktivitas yang sepenuhnya dikelola oleh pihak eksternal tanpa kontrol langsung dari universitas. Misalnya, aplikasi pihak ketiga yang digunakan secara individu oleh dosen atau mahasiswa tanpa integrasi resmi ke sistem universitas.

Namun demikian, universitas tetap memiliki kebijakan umum untuk memastikan bahwa setiap penggunaan teknologi eksternal mematuhi prinsip keamanan informasi yang sejalan dengan kebijakan universitas.

BAB II

PROFIL ORGANISASI

2.1 Gambaran Umum Universitas Hogwarts

Universitas Hogwarts merupakan salah satu perguruan tinggi swasta yang berfokus pada pengembangan ilmu pengetahuan, teknologi, dan riset terapan. Berdiri sejak tahun 1987, universitas ini terus berkembang menjadi salah satu institusi pendidikan tinggi terkemuka di Indonesia yang berorientasi pada inovasi digital, penelitian unggulan, dan tata kelola akademik berbasis teknologi informasi.

Dalam menghadapi era transformasi digital, Universitas Hogwarts telah mengintegrasikan berbagai sistem berbasis teknologi untuk mendukung kegiatan akademik, administrasi, penelitian, dan pelayanan mahasiswa. Hampir seluruh proses di lingkungan kampus telah terdigitalisasi, mulai dari sistem penerimaan mahasiswa baru, keuangan, kepegawaian, hingga pembelajaran daring melalui platform e-learning yang terpusat.

Dengan jumlah mahasiswa lebih dari 15.000 orang dan lebih dari 1.200 dosen serta tenaga kependidikan, universitas ini mengelola volume data yang sangat besar setiap harinya. Oleh karena itu, pengelolaan keamanan informasi menjadi aspek yang sangat penting untuk memastikan seluruh data akademik, administrasi, dan penelitian tetap terlindungi, andal, dan hanya diakses oleh pihak yang berwenang.

Sebagai bagian dari upaya mewujudkan universitas yang modern dan berdaya saing tinggi, Universitas Hogwarts berkomitmen untuk menerapkan Sistem Manajemen Keamanan Informasi (SMKI) berbasis ISO/IEC 27001:2022 guna memperkuat tata kelola teknologi informasi dan membangun budaya keamanan data yang berkelanjutan.

2.2 Visi dan Misi Universitas Hogwarts

Visi:

“Menjadi universitas unggul dan berdaya saing global dalam bidang pendidikan, penelitian, dan inovasi teknologi yang berintegritas dan aman secara digital.”

Misi:

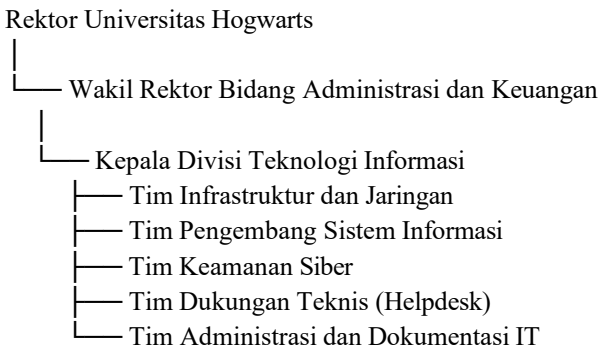
1. Menyelenggarakan pendidikan tinggi berkualitas dengan penerapan teknologi informasi yang efektif dan aman.
2. Mengembangkan penelitian dan inovasi yang mendukung kemajuan ilmu pengetahuan serta pembangunan nasional.

3. Membangun sistem manajemen universitas yang transparan, efisien, dan berorientasi pada keamanan informasi.
4. Meningkatkan kesadaran keamanan digital di seluruh lapisan civitas akademika.
5. Menjalin kerja sama dengan lembaga nasional dan internasional dalam pengembangan sistem keamanan informasi dan tata kelola data.

2.3 Struktur Organisasi Divisi Teknologi Informasi (IT Division)

Divisi Teknologi Informasi (IT Division) merupakan unit kerja yang berada di bawah koordinasi Wakil Rektor Bidang Administrasi dan Keuangan. Divisi ini memiliki peran strategis dalam mengelola infrastruktur teknologi universitas serta bertanggung jawab terhadap keamanan data, sistem jaringan, dan pengembangan aplikasi kampus.

Struktur organisasi Divisi IT Universitas Hogwarts terdiri dari beberapa bagian utama sebagai berikut:



a. Kepala Divisi Teknologi Informasi

Bertanggung jawab dalam perencanaan, pengawasan, dan pengendalian seluruh kegiatan Divisi IT, termasuk implementasi kebijakan keamanan informasi serta penerapan ISO/IEC 27001.

b. Tim Infrastruktur dan Jaringan

Menangani seluruh perangkat keras dan jaringan universitas, termasuk server utama, perangkat router, firewall, serta sistem Wi-Fi kampus. Tim ini memastikan ketersediaan layanan dan kestabilan jaringan selama 24 jam.

c. Tim Pengembang Sistem Informasi

Bertugas untuk mengembangkan dan memelihara sistem-sistem digital universitas seperti SIAKAD (Sistem Informasi Akademik), portal mahasiswa dan dosen, serta Learning Management System (LMS).

d. Tim Keamanan Siber (Cyber Security Team)

Fokus pada perlindungan data dan sistem dari ancaman keamanan, melakukan pemantauan aktivitas jaringan, serta menangani insiden keamanan siber. Tim ini juga melaksanakan penilaian risiko (risk assessment) dan audit keamanan (security audit) secara berkala.

e. Tim Dukungan Teknis (Helpdesk)

Memberikan layanan teknis kepada pengguna sistem universitas, baik dosen, staf, maupun mahasiswa. Selain itu, tim ini juga memberikan edukasi terkait penggunaan teknologi dan praktik keamanan digital yang baik.

f. Tim Administrasi dan Dokumentasi IT

Mengelola seluruh dokumen operasional Divisi IT, termasuk kebijakan, prosedur, laporan insiden, audit, serta dokumen SMKI.

2.4 Fungsi dan Tanggung Jawab Divisi IT

Divisi Teknologi Informasi Universitas Hogwarts memiliki fungsi utama sebagai berikut:

1. Mengelola infrastruktur teknologi informasi kampus, termasuk server, jaringan, dan perangkat digital.
2. Menyediakan sistem informasi terintegrasi untuk mendukung kegiatan akademik, penelitian, dan administrasi.
3. Menjaga keamanan data dan sistem informasi, serta mengelola kebijakan keamanan kampus berbasis ISO/IEC 27001.
4. Melakukan audit keamanan informasi dan evaluasi risiko secara berkala.
5. Memberikan dukungan teknis dan pelatihan keamanan siber kepada seluruh civitas akademika.
6. Menjalin kerja sama dengan pihak eksternal seperti penyedia layanan cloud, konsultan TI, dan auditor keamanan.

Dengan fungsi tersebut, Divisi IT menjadi tulang punggung keberhasilan transformasi digital universitas serta garda terdepan dalam menjaga keamanan sistem akademik.

2.5 Layanan Utama Divisi IT

Layanan yang dikelola oleh Divisi Teknologi Informasi Universitas Hogwarts meliputi:

1. **Manajemen Jaringan Kampus**
   Pengelolaan jaringan internet, LAN, dan Wi-Fi di seluruh area kampus agar selalu stabil, cepat, dan aman.
2. **Sistem Informasi Akademik (SIAKAD)**
   Aplikasi utama yang digunakan untuk mengelola data akademik, nilai, jadwal kuliah, serta kehadiran mahasiswa dan dosen.
3. **Learning Management System (LMS)**
   Platform pembelajaran daring yang digunakan dalam kegiatan perkuliahan jarak jauh dan penyimpanan materi digital.
4. **Manajemen Akun dan Autentikasi Pengguna**
   Mengelola sistem autentikasi berbasis *Single Sign-On (SSO)* dan *Multi-Factor Authentication (MFA)* untuk meningkatkan keamanan akses.
5. **Email Institusional dan Layanan Cloud**
   Menyediakan layanan email resmi universitas (@hogwarts.ac.id) dan sistem penyimpanan berbasis cloud untuk kolaborasi penelitian dan administrasi.
6. **Keamanan Siber dan Monitoring Sistem**
   Melakukan pemantauan aktivitas jaringan dan sistem universitas secara real-time untuk mendeteksi potensi ancaman siber.
7. **Manajemen Backup dan Disaster Recovery**
   Menyediakan sistem backup otomatis dan prosedur pemulihan bencana agar data tetap aman jika terjadi insiden.

2.6 Aset Informasi Penting

Universitas Hogwarts mengelola berbagai aset informasi penting yang menjadi dasar dalam pengambilan keputusan dan kegiatan operasional kampus. Berikut adalah klasifikasi aset informasi yang termasuk dalam lingkup keamanan informasi:

No.	Aset Informasi	Deskripsi dan Fungsi	Klasifikasi Keamanan
1	**Database Akademik**	Menyimpan data mahasiswa, dosen, nilai, jadwal kuliah, dan hasil belajar.	Sangat Rahasia
2	**Server Pusat Data (Data Center)**	Menjadi pusat penyimpanan seluruh sistem digital universitas.	Kritis
3	**Sistem Informasi Akademik (SIAKAD)**	Aplikasi inti untuk manajemen kegiatan akademik.	Kritis
4	**Learning Management System (LMS)**	Menyimpan materi kuliah, tugas, dan hasil evaluasi mahasiswa.	Rahasia

No.	Aset Informasi	Deskripsi dan Fungsi	Klasifikasi Keamanan
5	**Sistem Keuangan dan SDM**	Mengelola data keuangan, gaji, dan administrasi pegawai.	Rahasia
6	**Email dan Cloud Institusional**	Media komunikasi resmi antar-civitas akademika.	Rahasia
7	**Jaringan Kampus (LAN & Wi-Fi)**	Menghubungkan seluruh aktivitas digital di kampus.	Penting
8	**Backup dan Arsip Digital**	Menyimpan salinan data penting untuk pemulihan.	Kritis
9	**Perangkat Endpoint (Laptop, PC, Router)**	Sarana operasional pengguna dan jaringan kampus.	Penting
10	**Portal Penelitian dan Publikasi**	Menyimpan hasil riset dan publikasi ilmiah dosen.	Rahasia

Setiap aset informasi tersebut dilindungi melalui kebijakan keamanan yang sesuai dengan prinsip **Confidentiality, Integrity, dan Availability (CIA)**, sebagaimana yang diatur dalam ISO/IEC 27001.

2.7 Budaya dan Nilai Organisasi

Universitas Hogwarts meyakini bahwa keamanan informasi bukan hanya tanggung jawab teknis, tetapi juga budaya organisasi. Oleh karena itu, universitas menanamkan nilai-nilai berikut dalam setiap aktivitasnya:

1. **Integritas Data:** Setiap data akademik dan administratif harus dikelola dengan kejujuran dan tanggung jawab.
2. **Kerahasiaan:** Informasi pribadi civitas akademika wajib dijaga dari akses tidak sah.
3. **Profesionalisme:** Penggunaan teknologi informasi harus dilakukan dengan etika dan kepatuhan terhadap kebijakan universitas.
4. **Kepatuhan Hukum:** Setiap proses TI harus mematuhi peraturan perundangan nasional dan standar internasional.
5. **Keberlanjutan (Sustainability):** Penerapan SMKI dilakukan dengan pendekatan berkelanjutan agar mampu menyesuaikan diri terhadap perubahan teknologi dan ancaman baru.

Dengan fondasi budaya yang kuat, Universitas Hogwarts berkomitmen menjadi universitas modern yang aman secara digital, berdaya saing global, dan patuh terhadap standar tata kelola keamanan informasi internasional.

BAB III

ANALISIS KONTEKS ORGANISASI

Penerapan Sistem Manajemen Keamanan Informasi (SMKI) berdasarkan ISO/IEC 27001:2022 diawali dengan analisis konteks organisasi. Analisis ini bertujuan untuk memahami lingkungan internal dan eksternal Universitas Hogwarts yang dapat memengaruhi keberhasilan sistem manajemen keamanan informasi.

Konteks organisasi mencakup faktor-faktor seperti struktur organisasi, budaya kerja, kapasitas sumber daya manusia, kebijakan dan prosedur internal, hingga tuntutan pihak luar seperti peraturan pemerintah, perkembangan teknologi, serta ekspektasi stakeholder.

3.1 Konteks Internal

Faktor internal mencakup seluruh elemen di dalam Universitas Hogwarts yang berpengaruh langsung terhadap pengelolaan keamanan informasi, termasuk struktur organisasi, kebijakan TI, sumber daya manusia, serta infrastruktur digital.

No.	Isu Internal	Deskripsi Kondisi	Dampak terhadap Keamanan Informasi
1	**Kesadaran Keamanan Informasi yang Masih Rendah**	Sebagian besar staf dan dosen belum memahami sepenuhnya risiko siber seperti phishing, kebocoran data, atau penggunaan password lemah.	Potensi kesalahan manusia (*human error*) dan kebocoran data meningkat.
2	**Infrastruktur TI Belum Seragam**	Beberapa unit fakultas masih menggunakan sistem lokal yang tidak terintegrasi dengan pusat data universitas.	Menimbulkan celah keamanan dan kesulitan pemantauan sistem.
3	**Belum Ada SOP Keamanan yang Terintegrasi**	Prosedur keamanan data belum disusun secara formal dan terdokumentasi sesuai standar ISO.	Penanganan insiden keamanan menjadi tidak konsisten dan lambat.
4	**Pengelolaan Hak Akses yang Tidak Terstandar**	Beberapa akun pengguna tidak dinonaktifkan setelah pegawai atau mahasiswa keluar dari sistem.	Risiko akses ilegal dan penyalahgunaan akun meningkat.
5	**Keterbatasan Sumber Daya Keamanan Siber**	Tim keamanan TI hanya terdiri dari beberapa personel dengan beban kerja tinggi.	Penanganan ancaman siber tidak dapat dilakukan secara optimal.
6	**Tingkat Ketergantungan pada Sistem Digital yang Tinggi**	Hampir semua aktivitas kampus bergantung pada sistem akademik, keuangan, dan LMS.	Bila sistem terganggu, layanan akademik dan administrasi terhenti.
7	**Kurangnya Audit Internal Rutin**	Audit terhadap keamanan sistem belum dijadwalkan secara berkala.	Risiko keamanan tidak teridentifikasi secara cepat.

Analisis menunjukkan bahwa Universitas Hogwarts perlu memperkuat kesadaran keamanan informasi di seluruh lapisan organisasi serta membangun kebijakan dan SOP keamanan yang terdokumentasi agar lebih konsisten dan terukur.

3.2 Konteks Eksternal

Faktor eksternal mencakup kondisi di luar organisasi yang dapat memengaruhi keamanan informasi, seperti regulasi hukum, ancaman teknologi, serta kerja sama dengan pihak ketiga.

No.	Isu Eksternal	Deskripsi Kondisi	Dampak terhadap Keamanan Informasi
1	**Ancaman Siber Global (Phishing, Ransomware, DDoS)**	Perguruan tinggi sering menjadi target serangan karena menyimpan banyak data akademik dan penelitian.	Potensi gangguan operasional dan kehilangan data sensitif.
2	**Peraturan Perlindungan Data Pribadi (UU No. 27 Tahun 2022)**	Universitas wajib mematuhi regulasi terkait pengumpulan, penyimpanan, dan penggunaan data pribadi.	Diperlukan kepatuhan hukum yang ketat dan dokumentasi kebijakan privasi.
3	**Ketergantungan terhadap Vendor dan Cloud Pihak Ketiga**	Beberapa layanan cloud dan aplikasi kampus di-host oleh penyedia eksternal.	Risiko kebocoran data dan kontrol terbatas terhadap keamanan vendor.
4	**Perkembangan Teknologi yang Cepat**	Adanya adopsi sistem baru (AI, IoT, dan Big Data) menambah kompleksitas pengelolaan TI.	Diperlukan pembaruan kebijakan dan sistem keamanan secara berkelanjutan.
5	**Persaingan Reputasi antar Universitas**	Reputasi kampus dapat menurun jika terjadi kebocoran data atau serangan siber.	Keamanan informasi menjadi aspek strategis dalam citra publik universitas.
6	**Pandemi dan Digitalisasi Pendidikan**	Perpindahan aktivitas ke platform online meningkatkan paparan ancaman siber.	Universitas perlu memperkuat sistem keamanan e-learning dan akses jarak jauh.

Analisis eksternal menegaskan pentingnya implementasi ISO 27001 agar Universitas Hogwarts dapat mematuhi hukum, meningkatkan kepercayaan stakeholder, serta melindungi data akademik di tengah dinamika teknologi yang terus berkembang.

3.3 Analisis SWOT Keamanan Informasi

Sebagai bagian dari analisis konteks organisasi, berikut gambaran kekuatan (Strengths), kelemahan (Weaknesses), peluang (Opportunities), dan ancaman (Threats) yang berkaitan dengan keamanan informasi Universitas Hogwarts:

Aspek	Uraian
Strengths (Kekuatan)	- Infrastruktur TI kampus sudah terpusat di Data Center. - Memiliki Divisi IT khusus dengan tim pengembang dan keamanan. - Dukungan pimpinan terhadap pengembangan sistem keamanan.
Weaknesses (Kelemahan)	- Kesadaran keamanan informasi belum merata. - SOP dan kebijakan belum sepenuhnya terdokumentasi. - Audit keamanan belum berjalan rutin.
Opportunities (Peluang)	- Penerapan ISO 27001 dapat meningkatkan kepercayaan publik dan akreditasi kampus. - Potensi kerja sama riset keamanan dengan lembaga nasional/internasional. - Dukungan pemerintah terhadap transformasi digital pendidikan.
Threats (Ancaman)	- Meningkatnya serangan ransomware dan phishing.

Aspek	Uraian
	- Ketergantungan pada layanan cloud pihak ketiga. - Potensi kehilangan reputasi akibat insiden keamanan.

3.4 Analisis Pihak Berkepentingan (Stakeholder Analysis)

Stakeholder merupakan pihak-pihak yang memiliki kepentingan langsung maupun tidak langsung terhadap keamanan informasi universitas. Setiap stakeholder memiliki kebutuhan dan harapan yang berbeda terkait keamanan, integritas, dan ketersediaan informasi.

Pihak Berkepentingan	Kebutuhan/Harapan terhadap Keamanan Informasi	Tingkat Kepentingan
Rektor dan Pimpinan Universitas	Laporan keamanan yang akurat, kebijakan keamanan yang sesuai standar, dan keandalan sistem universitas.	Sangat Tinggi
Divisi IT	Dukungan sumber daya, kebijakan yang jelas, dan kontrol keamanan yang terstandar.	Sangat Tinggi
Dosen dan Tenaga Kependidikan	Akses mudah ke sistem akademik tanpa mengorbankan keamanan data.	Tinggi
Mahasiswa	Privasi data pribadi, nilai, dan aktivitas akademik yang terjamin.	Tinggi
Pemerintah dan Regulator (Kemendikbud & Kominfo)	Kepatuhan terhadap peraturan perlindungan data dan keamanan sistem pendidikan.	Sangat Tinggi
Vendor atau Mitra Teknologi	Kejelasan perjanjian keamanan (SLA) dan akses terbatas sesuai kontrak.	Menengah
Masyarakat dan Orang Tua Mahasiswa	Kepercayaan terhadap integritas data akademik dan reputasi universitas.	Tinggi

Hasil analisis menunjukkan bahwa kebutuhan keamanan informasi paling tinggi berasal dari pihak pimpinan universitas, regulator, dan Divisi IT, yang menjadi tiga aktor utama dalam keberhasilan implementasi SMKI.

3.5 Konteks Organisasi terhadap ISO/IEC 27001

Analisis konteks ini menjadi dasar dalam penerapan ISO/IEC 27001:2022, yang mensyaratkan organisasi untuk memahami faktor-faktor yang dapat memengaruhi tujuan SMKI.
Dalam konteks Universitas Hogwarts:

- **Faktor internal** menunjukkan perlunya peningkatan budaya keamanan dan dokumentasi kebijakan.
- **Faktor eksternal** menegaskan pentingnya kepatuhan hukum dan adaptasi terhadap ancaman digital baru.
- **Stakeholder** menuntut sistem yang tidak hanya aman tetapi juga efisien dan transparan.

Dengan memahami ketiga dimensi tersebut, universitas dapat menyusun kebijakan keamanan informasi yang relevan, realistis, dan selaras dengan tujuan strategis institusi.

3.6 Kesimpulan Analisis Konteks

Hasil analisis konteks organisasi menunjukkan bahwa Universitas Hogwarts berada pada tahap transisi menuju tata kelola keamanan informasi yang lebih matang. Tantangan terbesar yang dihadapi bukan hanya ancaman eksternal seperti serangan siber, tetapi juga faktor internal berupa rendahnya kesadaran pengguna terhadap praktik keamanan digital.

Penerapan SMKI berbasis ISO/IEC 27001 diharapkan mampu:

- Menstandarkan seluruh kebijakan dan prosedur keamanan informasi.
- Meningkatkan kesadaran seluruh civitas akademika terhadap pentingnya keamanan data.
- Memastikan kepatuhan universitas terhadap regulasi nasional dan internasional.

Dengan pemahaman konteks organisasi yang jelas, langkah selanjutnya adalah melakukan penilaian risiko keamanan informasi (Tahap 3**)** sebagai dasar penyusunan strategi pengendalian keamanan di lingkungan Universitas Hogwarts.

BAB IV

PENILAIAN RISIKO KEAMANAN INFORMASI

Penilaian risiko (Risk Assessment) merupakan tahap penting dalam penerapan Sistem Manajemen Keamanan Informasi (SMKI) karena menjadi dasar untuk menentukan langkah pengendalian (kontrol) yang tepat.

Dalam konteks Universitas Hogwarts, penilaian risiko dilakukan untuk mengidentifikasi dan mengevaluasi ancaman (threats), kerentanan (vulnerabilities), serta dampak (impact) terhadap aset informasi yang dikelola oleh universitas. Tujuannya adalah untuk memastikan bahwa setiap potensi ancaman dapat dikendalikan dengan cara yang efektif dan proporsional.

4.1 Metodologi Penilaian Risiko

Penilaian risiko di Universitas Hogwarts dilakukan menggunakan pendekatan kualitatif sesuai pedoman ISO/IEC 27005:2018, dengan langkah-langkah sebagai berikut:

1. **Identifikasi Aset Informasi**
   Menentukan aset penting yang menjadi objek perlindungan, seperti sistem akademik, server data, jaringan kampus, dan informasi pribadi mahasiswa.
2. **Identifikasi Ancaman dan Kerentanan**
   Menganalisis potensi ancaman (internal maupun eksternal) serta kelemahan yang dapat dimanfaatkan oleh pihak tidak berwenang.
3. **Penilaian Dampak (Impact Assessment)**
   Menilai sejauh mana konsekuensi yang mungkin terjadi apabila suatu ancaman terealisasi terhadap aset informasi tertentu.
4. **Penilaian Kemungkinan (Likelihood Assessment)**
   Mengukur peluang terjadinya ancaman berdasarkan kondisi nyata dan frekuensi kejadian sebelumnya.
5. **Evaluasi Risiko (Risk Level Evaluation)**
   Menentukan tingkat risiko berdasarkan kombinasi antara dampak dan kemungkinan terjadinya ancaman menggunakan skala berikut:

Tingkat Risiko (Risk Level)	Deskripsi
Rendah (Low)	Risiko kecil, dapat diterima dengan pemantauan minimal.
Sedang (Medium)	Risiko moderat, perlu tindakan pengendalian tambahan.
Tinggi (High)	Risiko signifikan, harus ditangani segera.
Sangat Tinggi (Critical)	Risiko kritis, membutuhkan tindakan mitigasi prioritas tinggi dan pemantauan ketat.

6. **Penentuan Strategi Penanganan (Risk Treatment Plan)**
   Menetapkan langkah mitigasi atau kontrol yang sesuai untuk mengurangi kemungkinan atau dampak risiko.

4.2 Identifikasi Risiko dan Aset Informasi

Berdasarkan hasil observasi dan analisis Divisi Teknologi Informasi Universitas Hogwarts, berikut ini adalah daftar aset informasi utama beserta ancaman, kerentanan, dan risiko yang mungkin terjadi.

No.	Aset Informasi	Ancaman	Kerentanan	Dampak Potensial	Kemungkinan Terjadi	Level Risiko	Tindakan Mitigasi / Kontrol yang Direkomendasikan
1	**Server Data (Data Center)**	Serangan malware dan ransomware	Server belum diperbarui & antivirus tidak aktif	Tinggi – Kehilangan data & gangguan layanan	Sedang	Tinggi	Instalasi antivirus terpusat, update patch rutin, pemantauan 24 jam
2	**Database Mahasiswa & Dosen**	Akses ilegal atau kebocoran data pribadi	Password lemah, belum ada MFA	Sangat Tinggi – Pelanggaran UU PDP, reputasi buruk	Tinggi	Kritis	Terapkan kebijakan password kuat, MFA, enkripsi database
3	**Sistem Akademik (SIAKAD)**	Manipulasi data nilai / jadwal	Audit log tidak aktif	Tinggi – Integritas data akademik terganggu	Sedang	Tinggi	Aktifkan audit log, backup harian terenkripsi, pembatasan hak akses admin
4	**Jaringan Kampus (LAN/Wi-Fi)**	Serangan DDoS / sniffing	Firewall tidak optimal, tidak ada segmentasi	Tinggi – Gangguan koneksi internet	Sedang	Tinggi	Upgrade firewall, implementasi IDS/IPS, segmentasi jaringan per fakultas
5	**Email Institusional**	Phishing / malware dari lampiran	Pengguna belum teredukasi, filter email minim	Sedang – Potensi pencurian kredensial	Tinggi	Tinggi	Filter spam & phishing, pelatihan kesadaran keamanan email
6	**Layanan Cloud & Backup Data**	Kebocoran data / kehilangan file	Backup manual, tidak terenkripsi	Tinggi – Kehilangan data riset & akademik	Sedang	Tinggi	Otomatisasi backup terenkripsi, audit integritas file, uji DRP berkala
7	**Laptop & Perangkat Staf IT**	Pencurian atau kehilangan perangkat	Tidak ada enkripsi disk / pelacakan perangkat	Sedang – Data internal bocor	Sedang	Sedang	Enkripsi perangkat (BitLocker), kebijakan Mobile Device Management
8	**Portal Penelitian & Publikasi**	Peretasan situs / manipulasi data	Patch keamanan tidak rutin	Sedang – Kredibilitas riset terganggu	Sedang	Sedang	Update sistem berkala, enkripsi koneksi HTTPS, audit akses admin
9	**Sistem Keuangan & SDM**	Serangan ransomware / insider threat	Hak akses tidak rutin diperbarui	Sangat Tinggi – Kerugian finansial / hukum	Rendah–Sedang	Tinggi	Audit hak akses, backup offline, pelatihan staf keuangan
10	**Vendor Cloud Eksternal**	Kebocoran data pihak ketiga	SLA tidak mencakup keamanan	Tinggi – Hilangnya kontrol data	Rendah	Sedang	Audit vendor, revisi kontrak SLA mencakup kepatuhan ISO 2700

4.3 Evaluasi Risiko

Berdasarkan hasil identifikasi, risiko-risiko pada aset dengan level tinggi hingga kritis perlu mendapat perhatian utama. Risiko tertinggi ditemukan pada database mahasiswa dan dosen, karena berisi data pribadi yang dilindungi oleh Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi (UU PDP).

Risiko lain yang cukup signifikan adalah serangan malware terhadap server data, phishing pada email dosen, dan serangan DDoS pada jaringan kampus.
Untuk setiap risiko tersebut, universitas harus menyiapkan langkah mitigasi yang sesuai baik dari sisi teknis, kebijakan, maupun sumber daya manusia.

4.4 Strategi Mitigasi dan Pengendalian Risiko

Berikut adalah rencana mitigasi dan kontrol keamanan informasi yang direkomendasikan untuk setiap risiko prioritas:

No.	Aset/Risiko Utama	Strategi Mitigasi (Risk Treatment Plan)	Tanggung Jawab
1	**Server Data**	- Instalasi antivirus terpusat dan update otomatis. - Implementasi sistem pemantauan server 24/7. - Penerapan patching berkala.	Tim Infrastruktur & Keamanan TI
2	**Database Mahasiswa & Dosen**	- Penerapan kebijakan password kuat dan autentikasi ganda (MFA). - Enkripsi data saat disimpan dan ditransmisikan. - Pembatasan hak akses berdasarkan jabatan.	Tim Keamanan Siber & DBA
3	**SIAKAD**	- Aktivasi audit log dan deteksi aktivitas anomali. - Backup harian terenkripsi. - Pembatasan akses admin.	Tim Pengembang Sistem & Keamanan TI
4	**Jaringan Kampus**	- Penambahan firewall dengan filtering canggih. - Segmentasi jaringan per fakultas. - Implementasi IDS/IPS untuk deteksi dini.	Tim Infrastruktur & Jaringan
5	**Email Dosen dan Staf**	- Implementasi filter spam dan phishing otomatis. - Pelatihan kesadaran keamanan siber (cyber awareness training).	Helpdesk & Tim Keamanan TI
6	**Backup dan Cloud Data**	- Backup otomatis dengan enkripsi AES-256. - Audit rutin integritas file backup. - Pengujian prosedur *disaster recovery* setiap semester.	Tim Infrastruktur & Backup
7	**Laptop Staf IT**	- Enkripsi seluruh perangkat dengan BitLocker atau sejenisnya. - Kebijakan keamanan perangkat mobile (MDM).	Tim Keamanan TI
8	**Vendor Cloud Eksternal**	- Revisi perjanjian SLA agar mencakup klausul keamanan data dan audit tahunan. - Pemeriksaan kepatuhan vendor terhadap ISO 27001.	Kepala Divisi IT & Tim Legal

4.5 Penilaian Residual Risk

Setelah penerapan kontrol, universitas perlu melakukan evaluasi ulang terhadap risiko residual, yaitu risiko yang masih tersisa setelah tindakan mitigasi dijalankan.
Hasil pengamatan menunjukkan bahwa dengan penerapan kontrol di atas, sebagian besar risiko dapat diturunkan menjadi level sedang atau rendah, kecuali pada area database akademik yang tetap memerlukan pemantauan ketat dan enkripsi berlapis.

BAB V

PEMILIHAN DAN RANCANGAN KONTROL KEAMANAN

Tahap ini bertujuan untuk menentukan kontrol keamanan informasi yang tepat berdasarkan hasil penilaian risiko pada Bab IV. Pemilihan kontrol mengacu pada **Annex A ISO/IEC 27001:2022**, yang berisi kontrol keamanan berbasis risiko untuk melindungi aset informasi organisasi.
Universitas Hogwarts memilih kontrol yang relevan dengan karakteristik lembaga pendidikan tinggi, tingkat risiko yang dihadapi, serta kemampuan sumber daya organisasi. Kontrol-kontrol ini dirancang untuk menjaga **kerahasiaan, integritas, dan ketersediaan (CIA)** informasi.

5.1 Dasar Pemilihan Kontrol

Pemilihan kontrol dilakukan berdasarkan:

1. Hasil penilaian risiko (risk assessment)
2. Tingkat kritikalitas aset informasi
3. Kesesuaian dengan proses bisnis universitas
4. Kepatuhan terhadap regulasi (UU PDP No. 27 Tahun 2022)
5. Rekomendasi Annex A ISO/IEC 27001:2022

5.2 Daftar Kontrol Keamanan yang Dipilih (Annex A)

Berikut adalah **minimal 10 kontrol keamanan** yang dipilih beserta alasan dan rencana implementasinya:

No	Kontrol ISO 27001:2022 (Annex A)	Deskripsi Kontrol	Alasan Pemilihan	Implementasi di Universitas Hogwarts
1	A.5.1 Kebijakan Keamanan Informasi	Menetapkan kebijakan keamanan formal	Belum ada kebijakan tertulis terintegrasi	Penyusunan dan pengesahan Kebijakan Keamanan Informasi oleh pimpinan
2	A.5.15 Kontrol Akses	Mengatur hak akses pengguna	Banyak akun aktif tidak terkelola	Role-Based Access Control (RBAC) & review akses berkala
3	A.5.16 Manajemen Identitas	Pengelolaan akun pengguna	Risiko akun tidak dinonaktifkan	Prosedur pembuatan & penghapusan akun terstandar
4	A.8.2 Hak Akses Istimewa	Pembatasan akses admin	Risiko penyalahgunaan admin	Dual control & logging aktivitas admin
5	A.8.7 Perlindungan Malware	Pencegahan malware & ransomware	Serangan malware pada server	Antivirus terpusat & update otomatis
6	A.8.9 Manajemen Konfigurasi	Pengelolaan konfigurasi sistem	Sistem tidak terdokumentasi	Dokumentasi baseline konfigurasi

No	Kontrol ISO 27001:2022 (Annex A)	Deskripsi Kontrol	Alasan Pemilihan	Implementasi di Universitas Hogwarts
7	A.8.12 Pencegahan Kebocoran Data	Perlindungan data sensitif	Risiko kebocoran data pribadi	Enkripsi data & DLP policy
8	A.8.16 Logging dan Monitoring	Pencatatan aktivitas sistem	Tidak ada audit log aktif	Centralized log & SIEM
9	A.5.30 Kesiapan Keamanan ICT	Kesiapan menghadapi insiden	Penanganan insiden belum baku	SOP Incident Response
10	A.5.31 Kepatuhan Hukum	Kepatuhan terhadap regulasi	Tuntutan UU PDP	Audit kepatuhan & dokumentasi hukum

5.3 Pernyataan Penerapan Kontrol (Statement of Applicability – SoA)

Pernyataan Penerapan (SoA) digunakan untuk mendokumentasikan:

- Kontrol yang diterapkan
- Alasan penerapan atau pengecualian
- Status implementasi kontrol

Universitas Hogwarts menetapkan bahwa **seluruh kontrol yang dipilih dalam Bab ini diterapkan**, karena seluruhnya relevan dengan risiko keamanan informasi yang telah diidentifikasi.

BAB VI

RANCANGAN DOKUMEN UTAMA SMKI

6.1 Kebijakan Keamanan Informasi (Information Security Policy)

Tujuan Kebijakan:
Menetapkan komitmen Universitas Hogwarts dalam melindungi informasi dari ancaman internal dan eksternal.

Ruang Lingkup:
Berlaku untuk seluruh civitas akademika, staf, vendor, dan pihak ketiga yang memiliki akses ke sistem informasi universitas.

Prinsip Kebijakan:
1. Menjaga kerahasiaan data akademik dan pribadi
2. Menjamin integritas informasi
3. Menyediakan ketersediaan sistem informasi
4. Mematuhi peraturan perundangan yang berlaku
5. Menerapkan pendekatan berbasis risiko.

Tanggung Jawab:
- Rektor: Penanggung jawab tertinggi SMKI
- Kepala Divisi IT: Implementasi dan pengawasan
- Pengguna: Kepatuhan terhadap kebijakan keamanan.

6.2 Tujuan Keamanan Informasi (Information Security Objectives)

Tujuan keamanan informasi Universitas Hogwarts adalah:
1. Mengurangi insiden keamanan informasi sebesar ≥ 50% dalam satu tahun
2. Menjamin ketersediaan sistem akademik minimal 99%
3. Memastikan 100% staf IT mengikuti pelatihan keamanan siber
4. Menerapkan MFA pada seluruh sistem kritis
5. Memastikan kepatuhan penuh terhadap UU PDP

Setiap tujuan diukur melalui **Key Performance Indicator (KPI)** dan dievaluasi secara berkala.

6.3 Rencana Implementasi SMKI (Implementation Plan)

Tahap	Aktivitas	Penanggung Jawab	Waktu
1	Pembentukan Tim SMKI	Rektor & Divisi IT	Bulan 1
2	Penyusunan kebijakan & SOP	Tim SMKI	Bulan 2
3	Implementasi kontrol teknis	Tim IT	Bulan 3–4
4	Pelatihan & sosialisasi	HR & IT	Bulan 4
5	Audit internal SMKI	Auditor Internal	Bulan 5
6	Tinjauan manajemen	Pimpinan	Bulan 6

BAB VII

KESIMPULAN DAN REKOMENDASI

7.1 Kesimpulan

Berdasarkan hasil analisis dan simulasi penerapan ISO/IEC 27001:2022, dapat disimpulkan bahwa:

1. Universitas Hogwarts memiliki aset informasi yang sangat kritis dan bernilai tinggi
2. Risiko utama berasal dari kebocoran data, malware, dan kesalahan manusia
3. Penerapan SMKI mampu meningkatkan keamanan sistem secara terstruktur
4. Kontrol Annex A yang dipilih relevan dan sesuai dengan kebutuhan organisasi
5. SMKI membantu universitas dalam memenuhi kepatuhan hukum dan meningkatkan kepercayaan stakeholder.

7.2 Rekomendasi

Untuk peningkatan berkelanjutan, direkomendasikan agar Universitas Hogwarts:

1. Melakukan audit internal SMKI minimal 1 kali setahun
2. Meningkatkan program pelatihan keamanan siber
3. Mengembangkan sistem monitoring keamanan berbasis SIEM
4. Melakukan evaluasi vendor TI secara berkala
5. Menyiapkan roadmap sertifikasi ISO/IEC 27001 resmi

DAFTAR PUSTAKA

ISO/IEC 27001:2022 – Information Security Management Systems

ISO/IEC 27002:2022 – Information Security Controls

ISO/IEC 27005:2018 – Information Security Risk Management

Undang-Undang Nomor 27 Tahun 2022 tentang Perlindungan Data Pribadi

BSI Group. (2022). *Implementing ISO/IEC 27001*