**Analysis Of Information Technology Security Management SIASAT UKSW Using ISO/IEC 27001:2013**

Andeka Rocky Tanaamah1, Friska Juliana Indira2

*Abstract*— IT security management is very necessary for organizations to see the risks and opportunities that occur because they will greatly affect the ongoing business processes in the organization. The Satya Wacana Academic Information System or more often called SIASAT is an IT component that plays very important role in the running of core business processes at Satya Wacana Christian University under the control of the Information Systems and Technology Bureau. At this time the implementation of SIASAT has been going well, but there are still some obstacles in it. Lack of human resources is one of the findings and one of the biggest risks because it affects the use of infrastructure and information security. This research was conducted using the international standard ISO/IEC 27001:2013 which prioritizes information security by taking a planning clause which focuses on risk assessment. From the results of this study, 9 recommendations were given, some of which are the most important of which are the creation of separate standard operating procedure documents for SIASAT which were previously still affiliated with the Academic Administration Bureau, distributing job descriptions and providing clear and documented access rights for everyone. It is hoped that this research can reduce the risks that occur and can be considered for making improvements to improve academic services in the future.

**Keyword**— Information Technology, Information System, Information Security Management, ISO/IEC 27001:2013.

1. Introduction

Pada era sekarang ini peran Teknologi Informasi (TI) sangat penting dalam sebuah organisasi dalam mendukung berjalannya kegiatan bisnis. Masalah yang berkaitan dengan keamanan informasi sering kali kurang mendapatkan perhatian, sedangkan hal tersebut termasuk bagian yang terpenting dari penerapan teknologi informasi. Semakin banyak dilakukan pengiriman dan pemanfaatan data internal antar organisasi pada jaringan terbuka akan meningkatkan risiko informasi tersebut menjadi terpapar [1]. Keamanan Informasi diartikan sebagai proses melindungi informasi dan aset informasi, untuk menjaga kerahasiaan, integritas, dan ketersediaan informasi [2]. Kerahasiaan adalah istilah yang digunakan untuk mencegah pengungkapan informasi kepada pihak yang tidak berwenang. Integritas berarti data tidak dapat dimodifikasi. Ketersediaan diartikan bahwa informasi harus dapat diakses kapan dan dimana pun data diperlukan oleh pengguna berwenang [3].

1,2 Jurusan Sistem Informasi, Fakultas Teknologi Informasi, Universitas Kristen Satya Wacana, Jln. Diponegoro No. 51-60, Salatiga, 50711, INDONESIA (phone: 0298-321 212; fax: 0298-324197; e-mail: 1atanaamah@uksw.edu, 2682015002@student.uksw.edu )

Faktanya, saat ini keamanan informasi merupakan masalah utama bagi sebuah bisnis. Sebuah survei menunjukkan bahwa risiko tersebut berlaku untuk badan publik dan perusahaan swasta, informasi yang berupa kertas dan elektronik, dari kegagalan melindungi data langsung atau kegagalan untuk membuang informasi arsip dapat timbul dari tindakan yang di sengaja maupun tidak di sengaja [4]. Manajemen risiko di definisikan sebagai proses identifikasi terhadap kerentanan dan ancaman dalam sebuah kerangka kerja suatu organisasi, serta akan menghasilkan beberapa pengukuran untuk meminimalkan dampaknya terhadap sumber daya informasi [5].

Salah satu perguruan tinggi yang sudah sadar akan penerapan TI sebagai kebutuhan penting dalam berjalannya kegiatan akademik adalah Universitas Kristen Satya Wacana (UKSW). Dikelola oleh Biro Teknologi dan Sistem Informasi (BTSI) merupakan sebuah Biro yang berada di bawah Pembantu Rektor I UKSW bertanggung jawab mengembangkan dan melayani kebutuhan civitas akademika dalam bidang teknologi informasi, sistem informasi, multimedia (termasuk di dalamnya mengembangkan modul pengajaran) dan fasilitas pengajaran [6]. Teknologi informasi yang telah diterapkan dan dimanfaatkan tersebut salah satunya adalah Sistem Informasi Akademik Satya Wacana atau lebih dikenal dengan istilah SIASAT yang merupakan sistem informasi berbasis mobile web yang terintegrasi oleh beberapa layanan di dalamnya untuk mempermudah dan mendukung kegiatan akademik di lingkungan Universitas Kristen Satya Wacana. Saat ini SIASAT merupakan salah satu bagian paling penting yang wajib digunakan dalam kegiatan akademik baik oleh dosen maupun mahasiswa. Layanan yang disediakan untuk dosen berupa jadwal mengajar, perwalian, serta input nilai. Sedangkan layanan yang disediakan untuk mahasiswa berupa registrasi ulang, registrasi matakuliah, requestmata kuliah, kartu studi dan hasil studi, jadwal kuliah, transkrip nilai, informasi tagihan semester, pendaftaran skripsi/tesis, serta informasi peminjaman buku.

Sebagai Biro yang menyediakan layanan berupa sistem informasi dan teknologi informasi kepada pengguna civitas akademika, BTSI bertanggung jawab atas keamanan data dan informasi yang dikelola salah satunya pada SIASAT. Seiring dengan penerapannya, kelemahan dan ancaman yang muncul pada sistem dapat mengganggu jalannya proses akademik yang sedang berlangsung. Ancaman tersebut dapat muncul dari luar maupun dalam sistem itu sendiri. Sering ditemui kasus terkait keamanan informasi seperti hilangnya data mahasiswa saat proses registrasi mata kuliah, tentunya sangat merugikan mahasiswa karena berpengaruh dalam proses perkuliahan untuk satu semester ke depan. Peretasan akun mahasiswa sehingga mahasiswa yang berkaitan tidak dapat masuk kedalam akunnya sendiri juga masih sering dijumpai. Server yang sering down saat proses registrasi mata kuliah juga merupakan hal yang sering dikeluhkan oleh mahasiswa sampai sekarang masih terjadi.

Penelitian yang pernah dilakukan sebelumnya, Akademi Yaman untuk studi pascasarjana (YAGS) menggunakan penerapan standar ISO/IEC 27001:2013 untuk mengetahui tingkat kematangan keamanan informasi. Hasil penelitian tersebut menunjukkan tingkat kematangan berada pada level 2. Nilai gap antara nilai tingkat kematangan saat ini dengan tingkat nilai kematangan yang diharapkan adalah 3.19. Artinya, banyak kelemahan kontrol yang ada, kebijakan dan prosedur keamanan terkait harus dikembangkan dan sistem dan budaya manajemen keamanan harus diterapkan [7]. Pada penelitian lain, ISO/IEC 27001:2013 juga digunakan untuk melakukan implementasi tata kelola keamanan informasi arsip digital pemerintah yang berbasis cloud computing pada Arsip Nasional Republik Indonesia untuk mengurangi dampak dari risiko terjadinya kehilangan integritas, kerahasiaan, dan ketersediaan dari sebuah informasi [8]. Begitu juga dengan penelitian pada kasus penerapan Radio Frequency Identification (RFID) di FTI-UKSW masih ditemukan keamanan pada Laboratorium terkait dengan Standar Operasional Prosedur (SOP) yang belum terdokumentasi sehingga ISO 27001:2013 yang berfokus pada domain Kebijakan Keamanan Informasi yang diperlukan sebagai arahan dan dukungan manajemen dalam penerapan keamanan informasi [9]. DPTSI-ITS juga melakukan perancangan dokumen SMKI berdasarkan ISO/IEC 27001:2013 dan melakukan manajemen risiko keamanan informasi berdasarkan ISO/IEC 27005:2013 dengan hasil penelitian didapatkan 60 risiko yang tidak diterima dari total 228 risiko teridentifikasi [10].

Mengacu pada pemahaman di atas, maka penelitian ini bertujuan menganalisis manajemen keamanan teknologi informasi pada Sistem Informasi Akademik Satya Wacana (SIASAT) dengan menggunakan ISO/IEC 27001:2013 untuk melihat kondisi dengan melakukan penilaian risiko dan peluang agar mengetahui seberapa besar dampaknya terhadap lembaga. ISO/IEC 27001:2013 dipilih karena merupakan standar internasional yang secara khusus mengedepankan faktor keamanan informasi yang memiliki 10 klausul serta memiliki daftar kontrol yang tepat untuk dijadikan panduan penilaian [11]. Berdasarkan kebutuhan yang diperlukan pada penelitian ini, dari 10 klausul yang tersedia peneliti berfokus pada klausul Perencanaan sebagai panduan untuk melakukan penilaiain risiko. Dengan dilakukannya penelitian ini, diharapkan dapat melihat seberapa baik layanan TI yang sudah diberikan, mengetahui sejauh mana ancaman dan peluang risiko yang terjadi, serta hasil penilaian ini dapat digunakan pada saat pengambilan kebijakan dalam menangani risiko untuk meningkatkan kinerja pelayanan oleh BTSI sebagai biro penyedia layanan yang bertanggung jawab.

1. Metode Penelitian
   1. *Metode Pengumpulan Data*

Fokus utama dari penelitian ini adalah untuk melihat penerapan SIASAT di lingkungan akademik serta sejauh mana manajemen keamanan informasi diterapkan sesuai dengan standar ISO/IEC 27001:2013. Penelitian ini dilakukan menggunakan metode kualitatif dengan melakukan wawancara bersama sumber – sumber yang berkaitan dengan SIASAT agar dapat penulis dapat menggali informasi apa saja yang akan dijadikan bahan penelitian. Wawancara dilakukan bersama dengan dua narasumber yaitu Kepala BTSI UKSW dan Kepala Bagian Sistem Informasi BTSI UKSW. Dalam melakukan wawancara, ISO/IEC 27001:2013 digunakan sebagai panduan untuk menyusun daftar pertanyaan. ISO/IEC 27001:2013 juga dipilih karena merupakan standar yang tepat dalam memberikan gambaran tentang apa saja yang harus dilakukan oleh organisasi dalam mengimplementasikan konsep risk assesment dan penanganan kendali keamanan informasi yang dapat disesuaikan dengan kebutuhan organisasi [12]. Standar ini mengadopsi model “Plan-Do-Check-Act” (PDCA) yang melibatkan tahapan identifikasi risiko yang harus diketahui dengan baik, kemudian menganalisa dampak dari risiko yang terjadi, melakukan evaluasi dan memberikan penanggulangan terhadap risiko tersebut dengan keluaran berbentuk dokumen temuan dan rekomendasi [13].

* 1. *Tahapan Penelitian*

Fig. 1 Research Stages Diagram.

Tahapan penelitian ini diawali dengan melakukan studi awal pada Biro Teknologi dan Sistem Informasi (BTSI) UKSW dengan melihat visi, misi, dan alur kerja sistem. Tahapan awal penelitian ini dimulai dengan melakukan studi literatur dengan mempelajari buku, artikel, jurnal dan karya ilmiah yang berkaitan dengan analisis manajemen keamanan informasi. Studi awal dengan melihat visi, misi, dan alur kerja SIASAT juga dilakukan untuk mendapatkan pengetahuan lebih dalam terkait dengan objek studi penelitian. Dilanjutkan dengan tahapan kedua melakukan identifikasi masalah. Proses dalam mengidentifikasi masalah dilakukan untuk melihat permasalahan yang pernah terjadi pada SIASAT sekaligus untuk melakukan penyusunan daftar pertanyaan wawancara berdasarkan panduan dari ISO/IEC 27001:2013 yang berfokus pada klausul Perencanaan yang di dalamnya berfokus pada tindakan untuk menangani risiko dan peluang, serta sasaran keamanan informasi dan perencanaan sesuai dengan fokus penelitian.

Setelah dilakukan identifikasi masalah dan penyusunan daftar pertanyaan wawancara, tahapan ketiga dilanjutkan dengan melakukan pengambilan data dengan menjalankan wawancara dengan narasumber yang berkaitan. Proses wawancara dibantu dengan alat perekam suara sebagai bukti yang dapat dipertanggung jawabkan serta mendukung proses berjalannya penelitian ini. Pada tahapan keempat dari hasil wawancara yang telah dilakukan, diolah menjadi sebuah data yang merupakan identifikasi risiko dan temuan – temuan masalah yang terjadi di SIASAT. Risiko diukur dengan berdasarkan dampak atau pengaruh yang ditimbulkan terhadap kemungkinan terjadinya risiko [14]. Sehingga, temuan – temuan masalah tersebut bisa diberikan rekomendasi untuk perbaikan dan juga dapat ditarik kesimpulan dari hasil penelitian.

1. Hasil Dan Pembahasan

Berdasarkan hasil wawancara yang dilakukan dengan key informant*,* ditemukan beberapa risiko dan peluang pada SIASAT UKSW yang dijabarkan dalam Tabel I:

Table I  
Identification Findings Of Risk And Opportunities In SIASAT UKSW

|  |  |  |  |
| --- | --- | --- | --- |
| **Code** | **Type** | **Findings** | **Cause** |
| R 1 | Risk | Belum adanya dokumen Standard Operating Procedure (SOP) khusus yang dimiliki untuk SIASAT. | Selama ini SOP SIASAT mengikuti SOP yang dimiliki oleh Biro Administrasi dan Registrasi (BARA). |
| R 2 | Risk | Hak akses setiap user dan tiap bagian tidak terdokumentasi secara jelas. | Administrator tunggal BTSI harus memberikan ijin kepada user untuk melakukan akses pada kebutuhan – kebutuhan tertentu. |
| R 3 | Risk | Belum adanya dokumen control access untuk SIASAT. | Belum ada sumber daya manusia yang ditunjuk khusus untuk melakukan dokumentasi secara rinci. |
| R 4 | Risk | Belum ada pembagian job description untuk setiap bagian yang terdokumentasi dengan jelas. | Terbatasnya sumber daya manusia yang dapat dipercaya dan memiliki kemampuan untuk bertanggung jawab memegang kendali di SIASAT. |
| R 5 | Risk | Kerusakan Infrastruktur TI. | Bencana alam yang tidak terduga dapat merusak beberapa infrastruktur TI yang ada. |
| R 6 | Risk | Server mengalami down*.* | Koneksi jaringan yang terganggu dari pihak ketiga pemberi layanan. |
| R 7 | Risk | Peretasan akun SIASAT mahasiswa oleh mahasiswa lainnya. | Kelalaian mahasiswa dalam melakukan proses log in dan log out, serta tidak merubah password template dari BTSI sesuai dengan anjuran. |
| P1 | Opportunity | BTSI memiliki infrastruktur TI yang sudah memenuhi kualifikasi dan spesifikasi. | Memiliki hubungan kerjasama yang baik dengan vendor – vendor pemberi layanan serta memiliki dana yang cukup untuk merealisasikan permintaan kebutuhan yang sesuai dengan hasil rapat kerja bersama dengan stakeholder. |
| R 8 | Risk | Keamanan Ruang Server | Akses keluar masuk ruang server masih belum dibatasi, khususnya untuk pihak – pihak yang memiliki kewenangan khusus di luar pihak BTSI masih diperbolehkan masuk. |

1. Risk Identification and Inherent Risk

Mengacu pada panduan standar ISO/IEC 27001:2013 dijelaskan bahwa risiko dan peluang harus dijabarkan menjadi kategori risiko, jenis, penyebab dan konsekuensi. Setelah melakukan identifikasi risiko dan peluang yang dimiliki SIASAT UKSW, maka pada Tabel II akan dijabarkan proses penilaian kriteria. Tujuan dilakukan penjabaran ini untuk melihat lebih dalam tentang identifikasi dari risiko dan peluang, serta menilai seberapa besar risiko dan peluang dengan dilakukannya proses analisa inherent risk yang meliputi penilaian likelihood terjadinya risiko, penilaian consequences terjadinya risiko, dan tingkat risiko. Penilaian inherent risk dilakukan untuk mengetahui sejauh mana risiko dan peluang yang terjadi digunakan untuk mengukur dampak baik maupun buruk pada pelayanan kegiatan akademik di Universitas.

1. Likelihood Assesment

Penilaian Kemungkinan merupakan tahapan penting dalam menentukan jangka waktu dari sebuah risiko atau peluang yang terjadi yang dilakukan dengan cara melihat kembali apa saja penyebab risiko dan peluang teknologi informasi. Pengukuran pada Penilaian Kemungkinan dibagi menjadi 5 kategori pengukuran kualitatif yaitu, Almost Certain (sekali atau lebih dalam satu tahun), Likely (sekali dalam dua tahun), Moderate (sekali dalam 5 tahun), Unlikely (sekali dalam sepuluh tahun), dan Rare (sekali dalam lima puluh tahun). Dari hasil identifikasi temuan risiko sebelumnya, maka dapat dilakukan Penilaian Kemungkinan berdasarkan risiko dan peluang di SIASAT UKSW yang dijabarkan pada Tabel II:

Table II  
Likelihood Assessment Result

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Identification** | | | **Inherent Risk** |
| **Code** | **Categories** | **Consequences** | **Likelihood Assesment** |
| R 1 | Infrastructure | Tidak ada standarisasi khusus dalam skema penggunaan, penanggung jawab, hingga perawatan SIASAT. | Almost Certain |
| R 2 | Infrastructure | Mengakibatkan kerugiaan khususnya secara materi yang dapat menganggu jalannya proses bisnis. | Unlikely |
| R 3 | Infrastructure | Proses registrasi mata kuliah akan terganggu. | Likely |
| R 4 | Infrastructure | Performa layanan dapat terus ditingkatkan. | Almost Certain |
| R 5 | Human Resource | Beberapa hal kecil yang seharusnya menjadi job description dari masing – masing bagian akan bergantung pada Administrator. | Almost Certain |
| R 6 | Human Resource | Kesulitan untuk mencari tau job description dan hak akses setiap orang secara jelas ketika diperlukan. | Almost Certain |
| R 7 | Human Resource | Beberapa orang melakukan job description ganda sehingga mengganggu produktifitas pada job description utamanya. | Almost Certain |
| P 1 | Software | Tersendatnya proses registrasi mata kuliah yang akan merugikan mahasiswa itu sendiri. | Almost Certain |
| R 8 | Hardware Security | Kemungkinan terjadinya penyalahgunaan kepentingan oleh pihak – puhak yang tidak bertanggung jawab. | Moderate |

1. Consequences Assesment

Setelah Likelihood Assesment dilakukan, selanjutnya masuk ke tahapan Consequences Assesment. Perbedaan dari dua penilaian ini adalah likelihood assesment berbicara tentang jangka waktu sedangkan consequences assesment mengukur mengenai dampak kerugiannya secara materi. Namun, kedua hal ini saling berkaitan dimana likelihood assesment dapat mempengaruhi consequences assesment yang muncul dari risiko dan peluang yang terjadi. Tingkat penilaian konsekuensi dibedakan menjadi 5 kategori penilaian yaitu, Catastrophic (kerugian lebih dari $10 juta), Major (kerugian antara $5 – $10 juta), Moderate (kerugiaan antara $1 – $5 juta), Minor (kerugiaan antara $100 ribu – $1 juta), dan Insignificant (kerugiaan kurang dari $100 ribu).

Hasil dari Consequences Assesment risiko dan peluang yang dimiliki SIASAT UKSW dijabarkan pada Tabel III:

Table III  
Consequences Assesment Result

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Identification** | | | **Inherent Risk** | |
| **Code** | **Categories** | **Consequences** | **Likelihood Assesment** | **Consequences Assesment** |
| R 1 | Infrastructure | Tidak ada standarisasi khusus dalam skema penggunaan, penanggung jawab, hingga perawatan SIASAT. | Almost Certain | Catastrophic |
| R 2 | Infrastructure | Mengakibatkan kerugiaan khususnya secara materi yang dapat menganggu jalannya proses bisnis. | Unlikely | Catastrophic |
| R 3 | Infrastructure | Proses registrasi mata kuliah akan terganggu. | Likely | Moderate |
| R 4 | Infrastructure | Performa layanan dapat terus ditingkatkan. | Almost Certain | Catastrophic |
| R 4 | Human Resource | Beberapa hal kecil yang seharusnya menjadi job descriptiondari masing – masing bagian akan bergantung pada Administrator. | Almost Certain | Major |
| R 5 | Human Resource | Kesulitan untuk mencari tau job description dan hak akses setiap orang secara jelas ketika diperlukan. | Almost Certain | Minor |
| R 6 | Human Resource | Beberapa orang melakukan job description ganda sehingga mengganggu produktifitas pada job descriptionutamanya. | Almost Certain | Minor |
| P 1 | Software | Tersendatnya proses registrasi mata kuliah yang akan merugikan mahasiswa itu sendiri. | Almost Certain | Minor |
| R 7 | Hardware Security | Kemungkinan terjadinya penyalahgunaan kepentingan oleh pihak – puhak yang tidak bertanggung jawab. | Moderate | Minor |

1. Risk Level Assesment

Penilaian tingkat risiko dilakukan sebagai pengukuran tingkat risiko dan peluang yang terdapat pada SIASAT UKSW agar dijadikan perhatian penting oleh manajemen terkait. Penilaian tingkat risiko dibedakan menjadi 4 tingkatan yaitu Extreme Risk (memerlukan tindakan segera), High Risk (memerlukan perhatian manajemen senior), Moderate Risk (manajemen penanggung jawab spesifik), Low Risk (dikelola dengan prosedur rutin). Dari hasil penilaian tingkat risiko ini dapat digunakan dalam menentukan siapa saja pemilik risiko yang bertanggung jawab untuk melakukan evaluasi risiko dan peluang. Risk Matrix digunakan untuk memudahkan proses penilaian tingkat risiko yang dijabarkan pada Tabel IV, yang berpacu pada hasil dari Likelihood Assesment dan Consequences Assesment yang sudah dilakukan sebelumnya.

Table Iv  
Risk Matrix

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Consequences** | **Likelihood** | | | | |
| Almost Certain | Likely | Moderate | Unlikely | Rare |
| Insignificant | **H** | **H** | **E** | **E** | **E** |
| Minor | **M** | **H** | **H** | **E** | **E** |
| Moderate | **L** | **M** | **H** | **E** | **E** |
| Major | **L** | **L** | **M** | **H** | **E** |
| Catastrophic | **L** | **L** | **M** | **H** | **H** |

Hasil dari identifikasi Likelihood Assesment dan Consequences Assesment yang terjadi, maka dapat dilakukan penilaian tingkat risiko berdasarkan matriks risiko untuk mendapatkan hasil penilaian keseluruhan yang disajikan pada Tabel V:

Table V  
Overall Assesment Result

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk Identification** | | | **Inherent Risk** | | |
| **Code** | **Categories** | **Consequences** | **Likelihood Assesment** | **Consequences Assesment** | **Tingkat Risiko** |
| R 1 | Infrastructure | Tidak ada standarisasi khusus dalam skema penggunaan, penanggung jawab, hingga perawatan SIASAT. | Almost Certain | Catastrophic | Extreme Risk |
| R 2 | Infrastructure | Mengakibatkan kerugiaan khususnya secara materi yang dapat menganggu jalannya proses bisnis. | Unlikely | Catastrophic | Extreme Risk |
| R 3 | Infrastructure | Proses registrasi mata kuliah akan terganggu. | Likely | Moderate | High Risk |
| R 4 | Infrastructure | Performa layanan dapat terus ditingkatkan. | Almost Certain | Catastrophic | Extreme Risk |
| R 4 | Human Resource | Beberapa hal kecil yang seharusnya menjadi job descriptiondari masing – masing bagian akan bergantung pada Administrator. | Almost Certain | Major | Extreme Risk |
| R 5 | Human Resource | Kesulitan untuk mencari tau job description dan hak akses setiap orang secara jelas ketika diperlukan. | Almost Certain | Minor | High Risk |
| R 6 | Human Resource | Beberapa orang melakukan job description ganda sehingga mengganggu produktifitas pada job descriptionutamanya. | Almost Certain | Minor | High Risk |
| P 1 | Software | Tersendatnya proses registrasi mata kuliah yang akan merugikan mahasiswa itu sendiri. | Almost Certain | Minor | High Risk |
| R 7 | Hardware Security | Kemungkinan terjadinya penyalahgunaan kepentingan oleh pihak – puhak yang tidak bertanggung jawab. | Moderate | Minor | Moderate Risk |

1. Risk Evaluation

Tahapan evaluasi risiko dan peluang dilakukan dengan cara membandingkan hasil analisa risiko dengan kriteria risiko yang telah disusun sebelumnya, serta menjadikan analisa risiko menjadi fokus utama penanganan risiko untuk kedepannya. Proses evaluasi risiko pada penelitian ini membandingkan hasil analisa risiko yang meliputi likelihood assesment, consequences assesment, dan risk level assesment dengan kriteria risiko yang meliputi kategori risiko, jenis risiko, penyebab, dan konsekuensi. Hasil evaluasi risiko ini disajikan dalam bentuk diagram pada Fig 2:

Fig. 2 Comparison Chart of Risk Categories and Risk Levels.

Diagram pada Fig 2 menjelaskan perbandingan tingkat risiko dan kategori risiko serta peluang sesuai dari hasil yang sudah dijabarkan pada Tabel V. Dari diagram pada Fig 2, dapat diketahui jumlah dari tingkat risiko Extreme Risk yaitu 4, tingkat High Risk 4, dan Moderate Risk 1. Kategori yang masuk ke dalam Extreme Risk yaitu Infrastructure dan Human Resource, kategori yang masuk ke dalam High Risk meliputi Software, Infrastructure, dan Human Resource, dan satu yang termasuk ke dalam Moderate Risk adalah Hardware Security. Dengan begitu, dapat disimpulkan bahwa SIASAT memiliki risiko dan peluang TI yang tinggi terhadap dampak negatif yang kedepannya dapat menimbulkan hambatan pada layanan yang telah diimplementasikan serta juga dapat mengalami kerugiaan secara materi.

1. Recommendation

Dari proses penilaian keselurahan, maka hasil temuan beserta risiko dan peluang yang didapatkan akan diberikan rekomendasi untuk dilakukan perbaikan kedepannya guna mengurangi dampak dari risiko dan peluang yang ditimbulkan, disajikan pada Tabel VI:

Table VI  
Recommendation

|  |  |  |
| --- | --- | --- |
| **Categories** | **Findings** | **Recommendation** |
| Human Resource | Administrator harus memberikan ijin kepada user untuk melakukan akses pada kebutuhan – kebutuhan mendasar tertentu. | Memperjelas dan memberi hak akses untuk setiap user sesuai dengan bagian dan tanggung jawabnya agar ketika membutuhkan beberapa hal tidak selalu bergantung pada Administrator. |
| Human Resource | Belum terdapat sumber daya manusia yang ditunjuk secara khusus untuk melakukan dokumentasi secara rinci. | Mencari sumber daya manusia yang mumpuni dalam melakukan penyusunan dokumen control access. |
| Human Resource | Terbatasnya sumber daya manusia yang dapat dipercaya dan memiliki kemampuan untuk bertanggung jawab memegang kendali di SIASAT. | Melakukan pelatihan terhadap Sumber Daya Manusia, sehingga memiliki standar penggunaan fasilitas IT. |
| Infrastructure | Selama ini SOP SIASAT mengikuti SOP yang dimiliki oleh Biro Administrasi dan Registrasi (BARA). | Perlu dibuat SOP secara terdokumentasi yang terpisah antara SOP SIASAT dan SOP BARA, supaya lebih mudah membedakan ketika ada masalah yang muncul terutama pada SIASAT. |
| Infrastructure | Bencana alam yang tidak terduga dapat merusak beberapa infrastruktur TI yang ada. | Memastikan selalu melakukan backup data vital secara rutin di tempat yang terpisah dan memastikan pemasangan infrastruktur TI sudah diminimalisir dengan lokasi yang rentan akan bencana alam. |
| Infrastructure | Koneksi jaringan yang terganggu dari pihak ketiga pemberi layanan. | Memastikan untuk memilih vendor penyedia layanan jaringan yang terpercaya dan stabil, serta selalu melakukan pemantauan jaringan terutama pada saat – saat menjelang registrasi mata kuliah. |
| Infrastructure | Memiliki hubungan kerjasama yang baik dengan vendor – vendor pemberi layanan serta memiliki dana yang cukup untuk merealisasikan permintaan kebutuhan yang sesuai dengan hasil rapat kerja bersama dengan stakeholder. | Selalu memastikan bahwa penggunanan sumber daya IT sudah dimaksimalkan dan sesuai dengan kebutuhan. |
| Software | Kelalaian mahasiswa dalam melakukan proses log in dan log out, serta tidak merubah password template dari BTSI sesuai dengan anjuran yang tertera. | Selalu memberikan himbauan kepada mahasiswa untuk mengubah password dan tidak lagi menggunakan password template dari BTSI. Serta memastikan mahasiswa tidak sembarangan melakukan log in di berbagai device dan tidak melupakan proses log out setelah selesai menggunakan SIASAT. |
| Hardware Security | Akses keluar masuk ruang server masih belum dibatasi, khususnya untuk pihak – pihak yang memiliki kewenangan tertentu di luar BTSI masih diperbolehkan masuk. | Memberikan pengamanan ketat dan mempertegas siapa saja yang mempunyai ijin dan tanggung jawab untuk keluar masuk ruang server. |

1. Conclusions

Berdasarkan hasil analisis keseluruhan dari kondisi SIASAT UKSW terdapat 9 temuan dengan 8 risiko dan 1 peluang. Setelah dilakukan penilaian dari temuan – temuan tersebut, maka dapat ditarik kesimpulan bahwa perlu adanya prosedur penanganan risiko terutama terkait infrastruktur teknologi informasi yang digunakan. Respon terhadap manajemen sumber daya manusia juga sangat perlu diperhatikan terkait dengan jumlah serta kemampuan dari sumber daya manusia yang diperlukan oleh BTSI untuk mencapai efektivitas dan efisiensi pekerjaan. Risiko teknologi informasi yang menimbulkan dampak negatif juga perlu diberikan perhatian khusus dan dilakukan penanganan segera dengan mempertimbangkan rekomendasi – rekomendasi yang telah diberikan. Kepala BTSI selaku senior manajemen yang bertanggung jawab dalam berjalanannya proses bisnis ini perlu mengkomunikasikan permasalahan internal terkait kebutuhan yang diperlukan BTSI khususnya dalam menangani SIASAT beserta instrumen yang terkait di dalamnya bersama dengan pimpinan Universitas dan manajemen yang bertanggung jawab agar pelayanan berjalan lebih baik sesuai dengan harapan.

References

|  |  |
| --- | --- |
| [1] | G. Disterer, “ISO/EIC 27000, 27001, and 27002 for Information Security Management,” *Journal of Information Security,* pp. 92-100, 2013. |
| [2] | ISO/IEC 17799, Information Technology -- Security Techniques -- Code Practices for Information Security Management, International Standard, 2005. |
| [3] | G. Pavlov and J. Karakaneva, “Information Security Management System In Organization,” *Trakia Journal Sciences,* vol. 9, p. 25, 2011. |
| [4] | A. Gillies, “Improving The Quality of Information Security Management Systems With ISO 27000,” *The TQM Journal,* vol. 23, 2011. |
| [5] | S. Al-Dhahri, M. Al-Sarti and A. Abdul Aziz, “Information Security Management System,” *International Journal of Computer Applications (0975-8887),* vol. 158, 2017. |
| [6] | “BTSI UKSW,” 2021. [Online]. Available: https://btsi.uksw.edu/pages/sekilas-btsi. [Accessed 30 January 2021]. |
| [7] | A. A. Nasser, “Information security gap analysis based on ISO 27001: 2013 standard: A case study of the Yemeni Academy for Graduate Studies, Sana'a, Yemen,” *International Journal of Scientific Research in Multidisciplinary Studies,* vol. 3, no. 11, pp. 4-13, 2017. |
| [8] | D. Rutanaji, S. S. Kusumawardani and W. W. Winarno, “Penggunaan Kerangka Kerja SNI ISO/IEC 27001:2013 Untuk Implementasi Tata Kelola Keamanan Informasi Arsip Digital Pemerintah Berbasis Komputasi Awan (Arsip Nasional RI),” in *Prosiding Seminar Nasional GEOTIK*, Yogyakarta, 2018. |
| [9] | Y. Darmawan and A. F. Wijaya, “Analisis Sistem Manajemen Keamanan Informasi Pada Perguruan Tinggi Menggunakan ISO 27001:2013,” in *Seminar Nasional Sistem Informasi Indonesia*, 2017. |
| [10] | F. Mauladani and D. O. Siahaan, “Perancangan SMKI Berdasarkan SNI ISO/IEC27001:2013 dan SNI ISO/IEC27005:2013 (Studi Kasus DPTSI-ITS),” *CSRID Journal,* vol. 10, pp. 56-67, 2018. |
| [11] | P. G. Anarkhi, A. H. N. Ali and I. Kurnia, “Penyusunan Perangkat Audit Keamanan Informasi Aplikasi Berbasis Web Menggunakan ISO/IEC 27001 Klausul Kendali Akses,” *Jurnal Teknik POMITS,* vol. 1(1), pp. 1-5, 2013. |
| [12] | ISO (International Organization for Standarization), Information Technology - Security Techniques - Information Security Management Systems - Requirements, International Standard ISO/IEC 27001, 2013. |
| [13] | ISACA, Implementation Guideline ISO/IEC 27001:2013, Berlin: ISACA Germany Chapter e.V., 2016. |
| [14] | D. I. Sensuse, A. Syahrizal, F. Aditya and M. Nazri, “Information Security Risk Management Planning of Digital Certificate Management Case Study: Balai Sertifikasi Elektronik,” in *IEEE*, Gorontalo, 2020. |