

ANALISIS MANAJEMEN RISIKO KEAMANAN SISTEM BMKGSOFT MENGUNAKAN METODE OCTAVE-S

Megawati¹, Fitara Nisa², Muhammad Luthfi Hamzah³, Idria Maita⁴

^{1,2} Program Studi Sistem Informasi, Fakultas Sains dan Teknologi, UIN Sultan Syarif Kasim Riau
Jl. HR. Soebrantas No. 155 Simpang Baru, Panam, Pekanbaru, 28293

Email: megawati@uin-suska.ac.id, fitaranisa01@gmail.com, luthfi.hamzah@lecturer.pelitaindonesia.ac.id,
idria@uin-suska.ac.id

ABSTRAK

Stasiun Klimatologi Kelas IV Kampar telah menerapkan sebuah sistem informasi pengolahan database untuk mendukung operasional instansi yaitu sistem BMKGSoft, yang berfungsi menyediakan data yang valid, cepat, dan mudah untuk diakses. Namun selama diterapkannya sistem tersebut pernah terjadi ancaman yang memberikan dampak bagi instansi yaitu terjadinya server down, connection error, dan human error. Untuk mengatasi berulangnya permasalahan tersebut, perlu dilakukan analisis risiko ancaman. Adapun Metode yang digunakan dalam penelitian ini yaitu metode OCTAVE-S. Metode ini memberikan solusi bagi pihak manajemen untuk mengatasi ancaman keamanan sistem informasi. Hasil dari analisis risiko menghasilkan bahwa terdapat 8 praktek keamanan yang berada pada status stoplight Red yaitu Pengendalian Akses Fisik, Sistem dan Manajemen Jaringan, Pemantauan dan Audit Keamanan TI, Pengesahan dan Otorisasi, Manajemen Kerentanan, Enkripsi, Perancangan dan Arsitektur Keamanan, Manajemen Insiden. Dari hasil tersebut pihak instansi perlu meninjau ulang terkait praktek keamanan untuk mencegah terjadinya risiko baru yang berdampak pada keberlangsungan bisnis instansi.

Kata Kunci: *BMKGSoft, OCTAVE-S, Manajemen Risiko IT, Keamanan Sistem Informasi.*

A. PENDAHULUAN

Perkembangan teknologi informasi pada era globalisasi berkembang cukup pesat, dan telah mengambil peranan penting dalam berbagai sektor. Seperti dalam sektor pemerintahan, sebuah instansi dan teknologi informasi merupakan hal yang tidak terpisahkan, pasalnya teknologi informasi dapat meningkatkan efektivitas dan efisiensi kinerja pemerintah dalam memberikan pelayanan terhadap masyarakat. Namun, dalam penerapan teknologi informasi tidak terlepas dari adanya sebuah risiko yang berpotensi mengganggu proses bisnis suatu instansi, seperti hilangnya data yang diakibatkan oleh serangan virus, pencurian data, minimnya keamanan sistem informasi, kerusakan yang disebabkan oleh terjadinya bencana alam, dan kesalahan yang ditimbulkan oleh orang-orang yang terlibat dalam penggunaan sistem informasi di dalam perusahaan tersebut. Norken (2015) mengatakan risiko sebagai faktor yang berdampak buruk dan harus dihilangkan dalam rangka penyelesaian pekerjaan, terbatas waktu, biaya dan kualitas.

Kategori aset bersifat kontekstual untuk setiap organisasi dan harus ditentukan agar dapat dilakukan evaluasi dengan tepat. Alberts, dkk (2005) mengatakan kategori aset teknologi informasi yaitu sistem, informasi, aplikasi, dan orang. Pengelolaan risiko terhadap aset teknologi informasi perlu dilakukan untuk menjaga keamanan informasi dan meminimalkan kerugian. Sebuah instansi perlu memiliki atensi yang tinggi dalam menjaga aset

teknologi informasi yang dimiliki agar tidak rusak, hilang, dan tetap terkelola dengan benar. Karena mengingat perkembangan teknologi tidak terlepas dari sebuah risiko yang dapat disebabkan oleh beberapa faktor yang sebelumnya telah dipaparkan.

Badan Meteorologi, Klimatologi, dan Geofisika (BMKG) yang sebelumnya memiliki nama Badan Meteorologi dan Geofisika (BMG) merupakan Lembaga Pemerintah Non Departemen yang melaksanakan tugas pemerintahan di bidang Meteorologi, Klimatologi, Kualitas Udara dan Geofisika sesuai dengan ketentuan perundang-undangan yang berlaku. BMKG memiliki Unit Pelaksana Teknis (UPT) di setiap wilayah di Indonesia dan salah satu UPT tersebut berada di Provinsi Riau yaitu Stasiun Klimatologi Kelas IV Kampar, adapun tugasnya yaitu untuk mengamati, mengumpulkan data-data, mengolah data yang telah di dapat dan menyebarkan informasi kepada pihak-pihak terkait mengenai perubahan iklim dan cuaca yang terjadi di Provinsi Riau. Dalam menjalankan tugasnya Stasiun Klimatologi bekerjasama dengan pos-pos pengamatan yang tersebar di seluruh wilayah kabupaten atau kota Pekanbaru di Provinsi Riau.

Stasiun Klimatologi Kelas IV Kampar dibawah naungan BMKG telah menerapkan sebuah sistem informasi pengolahan database untuk mendukung operasional instansi yaitu sistem BMKGSoft yang merupakan sebuah aplikasi entry data berbasis web yang dipergunakan untuk

mengolah database secara online dan terpusat. Fungsi dari BMKGSoft yaitu menyediakan data yang valid, cepat, dan mudah untuk diakses. BMKGSoft dapat diakses di setiap UPT (Unit Pelaksana Teknis) dengan cara login terlebih dahulu menggunakan IP yang telah ditentukan. BMKGSoft telah digunakan oleh Stasiun Klimatologi Kelas IV Kampar sejak maret 2018, dengan user sebanyak 10 orang. Dalam penerapan BMKGSoft selama 3 tahun pernah terjadi ancaman terhadap sistem dan infrastruktur yang memberikan dampak bagi Stasiun Klimatologi Kelas IV Kampar.

Berdasarkan hasil studi pendahuluan, melalui observasi dan wawancara yang dilakukan di Stasiun Klimatologi Kelas IV Kampar, risiko yang pernah terjadi yaitu server down yang setiap bulan terjadi dan membuat sistem BMKGSoft tidak dapat diakses, yang berdampak pada kinerja pegawai karena tidak dapat melakukan penginputan dan pengiriman data, untuk hal tersebut terjadi terakhir kali pada februari 2021 yang mengakibatkan sistem tidak dapat diakses selama 15 jam. Kemudian risiko *connection error* terhadap id user pada sistem yang disebabkan oleh jaringan internet down yang pernah terjadi pada februari 2021 dan untuk hal tersebut pihak provider lambat dalam merespon, hal tersebut berdampak pada sistem BMKGSoft yang tidak dapat diakses dan menghambat produktivitas kinerja pegawai. Stasiun Klimatologi Kelas IV Kampar juga pernah

Metode OCTAVES dapat memberikan solusi untuk manajemen sistematis ancaman keamanan sistem informasi, dan juga dapat mencakup semua aktivitas. Metode OCTAVE-S memiliki 3 fase, 5 proses, 16 aktivitas dan 30 langkah yang dapat membantu dalam melakukan proses pengelolaan risiko keamanan sebuah sistem informasi untuk mendukung tercapainya visi dan misi dari sebuah instansi. (Albert, dkk, 2005). Dengan melakukan analisis risiko keamanan sistem BMKGSoft pada Stasiun Klimatologi Kelas IV Kampar diharapkan dapat diketahui seberapa besar tingkat keamanan sistem yang dapat meningkatkan efektivitas dan efisiensi kinerja instansi.

B. LANDASAN TEORI

B.1 Manajemen Risiko

Menurut (Fahmi dan Mulia, 2011) manajemen risiko ialah bidang ilmu yang mengkaji bagaimana suatu instansi atau perusahaan menggunakan pengukuran untuk memetakan problema yang ada melalui aplikasi kompleks dari pendekatan manajemen yang berbeda secara komperhensif dan sistematis. Adapun menurut (Suswinarno, 2012) dalam (Megawati, 2018) manajemen risiko merupakan strategi sistematis untuk mengelola ketidakpastian yang terkait dengan

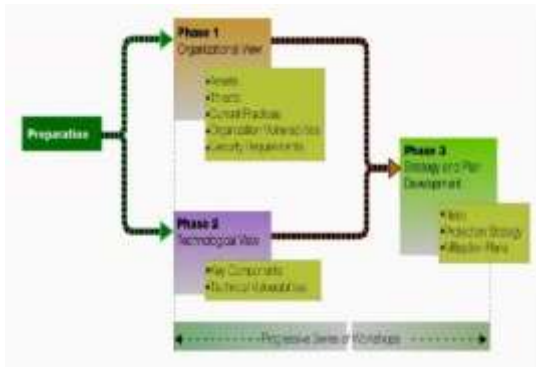
mengalami ancaman risiko *human error* pada proses penginputan data yang terjadi sebanyak 3 kali sejak tahun 2021, hal tersebut berdampak pada hasil perhitungan rata-rata pada saat analisis data yang dilakukan oleh pegawai Stasiun Klimatologi Kelas IV Kampar yang membuat data tidak akurat. Ancaman lain yang dapat mengganggu keamanan informasi instansi selain dari apa yang telah dipaparkan diatas, yang dapat mengakibatkan kerugian lebih besar dan mengganggu proses bisnis dan operasioanl yang terdapat di instansi. Untuk menghindari hal-hal tersebut maka dilakukanlah sebuah analisis risiko pada sistem informasi BMKGSoft dan infrastruktur sistem yang dimiliki oleh Stasiun Klimatologi Kelas IV Kampar

Tujuan penelitian ini adalah mengidentifikasi adanya risiko dalam penggunaan sistem tersebut, serta membuat perencanaan tindakan risiko strategi perlindungan terhadap risiko keamanan sistem BMKGSoft dan kelemahan infrastruktur sistem yang tepat sesuai dengan hasil identifikasi dari risiko. Untuk merealisasikannya diperlukan sebuah kerangka kerja yang sesuai untuk mengetahui risiko keamanan informasi yang digunakan seperti metode FMEA, COBIT, dan OCTAVE-S. Metode yang digunakan dalam penelitian ini yaitu metode OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation-Small*).

ancaman atau urutan aktivitas manusia, yang meliputi evaluasi risiko, merancang strategi pengelolaan risiko, dan meminimalkan risiko melalui pengelolaan sumber daya. Menurut (SBC Warburg, 2004) dikutip dalam (Hanafi, 2016) manajemen risiko merupakan seperangkat kebijakan dan prosedur lengkap milik sebuah organisasi. Guna mengelola, memonitor, serta mengendalikan eksposur instansi atau perusahaan terhadap sebuah risiko.

B.2 Metode OCTAVE-S

(Alberts dkk., 2005) mengatakan OCTAVE-S (*Operationally Critical Threat, Asset, and Vulnerability Evaluation-Small*) adalah variasi dari pendekatan OCTAVE yang dikembangkan untuk memenuhi kebutuhan organisasi kecil dan kurang hierarkis. Hal ini membutuhkan analisis dari sebuah tim untuk melihat risiko keamanan mengenai aset organisasi terhadap tujuan bisnis. Dengan menerapkan hasil OCTAVE-S, maka sebuah organisasi berusaha untuk melindungi seluruh informasi lebih baik lagi dan meningkatkan sektor keamanan informasi secara keseluruhan. Adapun fase metode OCTAVE-S dapat dilihat pada Gambar 1.



Gambar 1. Fase Metode OCTAVE-S

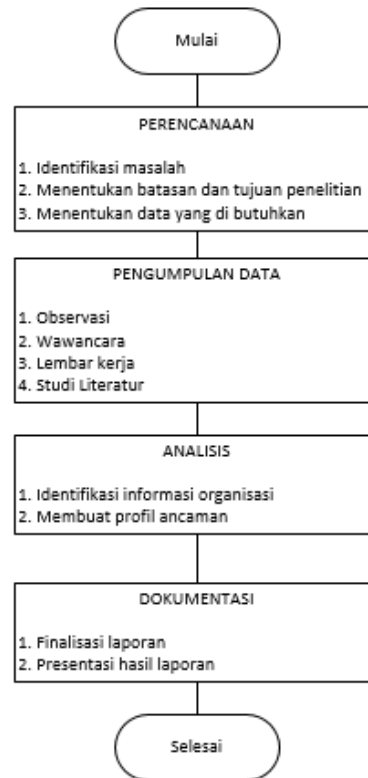
Menurut (Alberts dkk., 2005) selama pengevaluasian OCTAVE-S, tim analis akan melihat keamanan dari beberapa perspektif dan memastikan bahwa rekomendasi diselesaikan sesuai dengan persyaratan instansi atau perusahaan yang seimbang. Setiap fase OCTAVE-S menghasilkan hasil yang dapat digunakan, yang berarti bahwa bahkan beberapa evaluasi akan memberikan informasi untuk meningkatkan keamanan organisasi. Hasil OCTAVE-S yang paling penting terdiri dari tiga tingkat yaitu:

1. Rencana mitigasi risiko, yang dirancang untuk mengurangi risiko terhadap aset penting dengan meningkatkan praktek keamanan yang ditentukan.
2. Strategi perlindungan diseluruh organisasi, strategi perlindungan menguraikan arah organisasi sehubungan dengan praktek keamanan informasinya.
3. Daftar tindakan, ini termasuk item tindakan jangka pendek yang diperlukan untuk mengatasi kelemahan yang spesifik.

Hasil berguna lainnya dari OCTAVE-S yaitu:

1. Daftar aset terkait informasi penting yang mendukung tujuan dan sasaran bisnis dari instansi atau perusahaan.
2. Hasil survei yang menunjukkan sejauh mana sebuah organisasi mengikuti praktek keamanan dengan baik.
3. Profil ancaman untuk setiap aset penting yang kisaran risiko terhadap aset tersebut.

C. METODE PENELITIAN



Gambar 2. Metodologi Penelitian

Gambar 2. merupakan alur dari penelitian yang akan dilakukan yang dimulai dari perencanaan, pengumpulan data, analisis, dan yang terakhir yaitu dokumentasi.

D. HASIL DAN PEMBAHASAN

D.1 Identifikasi Informasi Instansi

Penilaian terhadap risiko dimulai dengan mengidentifikasi informasi dari Stasiun Klimatologi Kelas IV Kampar untuk dapat mengetahui level risiko yang bisa berdampak pada keberlangsungan proses bisnis instansi. Pada tahap ini terdapat tiga aktivitas dan untuk pengumpulan data dilakukan berdasarkan lembar kerja yang terdapat pada OCTAVE-S.

D.1.1 Membangun Dampak Dari Kriteria Evaluasi

Pada tahap ini dilakukan pengumpulan data untuk aktivitas membangun dampak risiko dari kriteria evaluasi yang terdapat pada lembar kerja OCTAVE-S yang digunakan sebagai penilaian kriteria dampak risiko pada Stasiun Klimatologi Kelas IV Kampar. Adapun data yang diperoleh yaitu sebagai berikut :

Tabel 1. Data Pengisian Lembar Kerja Identifikasi Risiko dari Kriteria Dampak Evaluasi Instansi.

| No. | Kriteria Dampak | Tipe/ Dampak | Level |
|-----|------------------------------|-----------------------------------|--------|
| 1. | Reputasi dan Kehilangan Data | Reputasi | Sedang |
| 2. | Keuangan | Biaya Operasional | Rendah |
| | | Kehilangan Pendapatan | Rendah |
| 3. | Produktivitas | Jam Kerja | Sedang |
| 4. | Kesehatan/ Keselamatan | Kesehatan/ Keselamatan Pegawai | Rendah |

Berdasarkan tabel 1. diketahui bahwa Indikator reputasi dan kehilangan data berada pada level sedang (*medium*), hal tersebut dikarenakan Stasiun Klimatologi Kelas IV Kampar telah memiliki sistem informasi BMKGSoft. Sistem BMKGSoft telah memiliki reputasi yang baik, karena sistem serta layanan yang ada sangat membantu para pegawai sebagai user dalam melakukan pekerjaan mereka. Namun dalam sistem BMKGSoft ada beberapa data yang tidak tersedia, hal tersebut mempengaruhi reputasi instansi terhadap individu maupun organisasi yang memiliki kepentingan terhadap data yang dimaksud. Pada penilaian indikator keuangan untuk tipe dampak biaya operasional Stasiun Klimatologi Kelas IV Kampar berada pada level (*low*) karena Stasiun Klimatologi Kelas IV Kampar tidak mengalami penurunan pendapatan. Pada indikator produktivitas berada pada level sedang (*medium*), hal tersebut dikarenakan jika terjadi suatu ancaman pada instansi maka jam kerja pegawai akan mengalami peningkatan. Pada indikator kesehatan/keselamatan Stasiun Klimatologi Kelas IV Kampar berada pada level rendah (*low*), hal tersebut terjadi karena sejauh ini para pegawai tidak pernah mengalami ancaman atau masalah pada kesehatan secara serius dan hanya sebuah permasalahan kesehatan yang dapat diselesaikan dengan diberi waktu istirahat sekitar 2-3 hari kerja, karena hal tersebut juga berkaitan dengan kemungkinan akan kurang tercapainya proses bisnis di instansi.

D.1.2 Identifikasi Aset Instansi

Pada tahap ini dilakukan pengumpulan data untuk aktivitas identifikasi aset instansi pada lembar kerja OCTAVE-S yang digunakan sebagai penilaian terhadap aset yang terdapat pada Stasiun Klimatologi Kelas IV Kampar. Adapun data yang diperoleh terdapat pada tabel 2. dan 3. yaitu sebagai berikut :

Tabel 2. Data Aset Instansi

| Sistem | Informasi | Aplikasi/ Layanan | Aset lainnya |
|--------|-----------|----------------------|-----------------|
|--------|-----------|----------------------|-----------------|

| | | | |
|-----------------|---|--------------------------------|-------------------|
| BMKGSoft | Informasi Curah hujan, Suhu udara, Kelembaban, Tekanan, Keadaan cuaca, Keadaan atmosfer, Penyinaran matahari, Arah dan Kecepatan angin. | Server, Jaringan internet, PC. | CMSS, AWS Center. |
|-----------------|---|--------------------------------|-------------------|

Tabel 3. Data Aset Instansi Sumber Daya Manusia Berdasarkan data yang diperoleh dari Stasiun Klimatologi Kelas IV Kampar.

| Sumber Daya Manusia | |
|---------------------|--|
| Jabatan | Keahlian |
| Teknisi | Bagian teknisi dipilih karena memiliki tanggung jawab dalam pengelolaan IT yang digunakan di lingkungan Stasiun Klimatologi Kelas IV Kampar. |

Dari tabel diatas dapat diketahui bahwa instansi memiliki aset informasi kritis yaitu sistem BMKGSoft dan untuk aset manusia yaitu bagian teknisi.

D.1.3 Evaluasi Praktek Keamanan Instansi

Pada tahap ini dilakukan pengumpulan data untuk aktivitas evaluasi praktek keamanan instansi pada lembar kerja OCTAVE-S yang digunakan sebagai penilaian terhadap praktek keamanan yang ada pada Stasiun Klimatologi Kelas IV Kampar. Adapun data yang diperoleh yaitu :

Tabel 4. Evaluasi Praktek Keamanan Instansi

| NO. | PRAKTEK KEAMANAN | STOPLIGHT | | |
|-----|-------------------------------------|-----------|--------|-------|
| | | RED | YELLOW | GREEN |
| 1. | Kesadaran Keamanan dan Pelatihan | | √ | |
| 2. | Strategi Keamanan | | √ | |
| 3. | Manajemen Keamanan | | √ | |
| 4. | Peraturan dan Kebijakan Keamanan | | √ | |
| 5. | Manajemen Keamanan dan Kolaborasi | | | √ |
| 6. | Perencanaan Contingency | | | √ |
| 7. | Pengendalian Akses Fisik | √ | | |
| 8. | Pemantauan dan Audit Keamanan Fisik | | | √ |
| 9. | Sistem dan Manajemen Jaringan | √ | | |
| 10. | Pemantauan dan Audit Keamanan TI | √ | | |
| 11. | Pengesahan dan Otorisasi | √ | | |
| 12. | Manajemen Kerentanan | √ | | |
| 13. | Enkripsi | √ | | |
| 14. | Perancangan dan Arsitektur Keamanan | √ | | |
| 15. | Manajemen Insiden | √ | | |

Terlihat pada tabel 4. terdapat delapan praktek keamanan Stasiun Klimatologi Kelas IV Kampar yang berada pada status stoplight Red yang

berarti Stasiun Klimatologi Kelas IV Kampar belum menerapkan praktek keamanan dalam area tersebut, dan empat praktek keamanan berada pada status Yellow hal ini berarti Stasiun Klimatologi Kelas IV Kampar sudah menerapkan praktik keamanan namun belum cukup baik, serta tiga praktek keamanan berada yang berada pada status Green yang berarti Stasiun Klimatologi Kelas IV Kampar sudah menerapkan praktek keamanan tersebut dengan baik.

D.2 Rekomendasi

Setelah dilakukan penilaian maka akan dilakukan tindakan risiko terhadap setiap bidang teknologi informasi berdasarkan hasil yang didapat, yaitu sebagai berikut :

Tabel 5. Daftar Tindakan Risiko

| No. | Praktek Keamanan | Tindakan Risiko |
|-----|-------------------------------------|--|
| 1. | Pengendalian Akses Fisik | Melakukan pengendalian terhadap akses fisik dengan benar. Serta implementasi kebijakan dan prosedur terdokumentasi untuk setiap pengunjung. |
| 2. | Sistem dan Manajemen Jaringan | Melakukan perlindungan terhadap informasi sensitif instansi dilokasi yang aman. Dan melakukan pemeriksaan terhadap sistem dan jaringan secara berkala di instansi. |
| 3. | Pemantauan dan Audit Keamanan TI | Melakukan pemantauan dan audit berkala terhadap sistem serta jaringan didalam instansi. |
| 4. | Pengesahan dan Otorisasi | Melakukan kontrol yang baik sesuai dengan kebijakan yang ada. |
| 5. | Manajemen Kerentanan | Terapkan langkah-langkah untuk mengelola tingkat kerentanan pada instansi dan lakukan penelitian kerentanan TI secara teratur. |
| 6. | Enkripsi | Menerakan manajemen keamanan sesuai kebutuhan instansi dan lindungi sensitivitas informasi. |
| 7. | Perancangan dan Arsitektur Keamanan | Melakukan pengelolaan sistem desigen dan arsitektur keamanan yang baik terhadap sistem yang digunakan di instansi. |
| 8. | Manajemen Insiden | Melakukan prosedur yang didokumentasikan oleh instansi dengan tujuan untuk identifikasi, pelaporan, dan proses tindak lanjut dari insiden dan pelanggaran keamanan yang dicurigai terjadi. |

E. KESIMPULAN

Berdasarkan analisis yang dilakukan terhadap keamanan sistem BMKGSof pada Stasiun Klimatologi Kelas IV Kampar, maka didapatkan sebuah kesimpulan yaitu:

1. Dari proses analisis yang telah dilakukan yaitu identifikasi informasi instansi terdapat tiga indikator dampak yang berda pada level sedang (*medium*) yaitu reputasi, biaya operasional, dan jam kerja. Dan dari proses identifikasi aset instansi diketahui bahwa Stasiun

2. Klimatologi Kelas IV Kampar memiliki aset kritis yaitu sistem BMKGSof.
2. Hasil analisis identifikasi praktek keamanan terhadap teknologi informasi pada Stasiun Klimatologi Kelas IV Kampar ditemukan Terdapat 8 praktek keamanan yang berada pada status *Stoplight Red* yaitu Pengendalian Akses Fisik, Sistem dan Manajemen Jaringan, Pemantauan dan Audit Keamanan TI, Pengesahan dan Otorisasi, Manajemen Kerentanan, Enkripsi, Perancangan dan Arsitektur Keamanan, dan Manajemen Insiden. Kemudian terdapat 4 praktek keamanan berada pada status *Yellow* yaitu Kesadaran Keamanan dan Pelatihan, Strategi Keamanan, Manajemen Keamanan, serta Peraturan dan Kebijakan Keamanan. Kemudian 3 praktek keamanan berada pada status *Green* yaitu Manajemen Keamanan dan Kolaborasi, Perencanaan *Contingency*, dan Pengendalian Akses Fisik.

REFERENSI

- [1] Alberts, C., Dorofee, A., Stevens, J., & Woody, C. *Octave-s Implementation Guide, Version 1.0*. Pittsburgh: Carnege Mellon Software Engineering Institute. 2005.
- [2] Garcia, C., Sarita, H., & Jimmy, A. *Information Security Risk Management Model for Peruvian SMEs*. IEEE Sciences and Humanities International Research Conference (SHIRCON). 2018. 1-5.
- [3] Kurniawan, A. N., Buce, T. H., & Suprpto. Penerapan Manajemen Risiko Teknologi Informasi Menggunakan Metode OCTAVES-S Pada UPT Pusat Komputer Politeknik Negeri Malang. *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*. 4(6). 1802-1808. 2020.
- [4] Norken, I. Nyoman dkk. Pengantar Analisis dan Manajemen Risiko Pada Proyek Pembangunan Infrastruktur Bangunan Gedung Bertingkat. *Jurnal Desain Konstruksi*. Udayana University Press. 2015
- [5] Pratama, R., Dedy, S., & Yesi, N. K. Evaluasi Risiko Keamanan Informasi Menggunakan OCTAVE-S. *Seminar Nasional Teknologi Informasi dan Komunikasi (SEMNASTIK) X*. 147-152. 2018.

- [6] Rahardjo, Budi. Keamanan Sistem Informasi Berbasis Internet. PT. Insan Infonesia : Bandung. 1998.
- [7] Rohman, A. F., Awalludiyah, A., & Eman, S. Analisis Manajemen Risiko IT dan Keamanan Aset Menggunakan Metode OCTAVE-S. *Journal of Information Technology and Computer Science (INTECOMS)*. 3(2). 298-310. 2020.
- [8] Setyawan, A. A., Agustinus, F.W. Analisis Manajemen Risiko Teknologi Informasi Pada Diskominfo Kota Salatiga Menggunakan Metode OCTAVE-S. *Seminar Nasional Sistem Informasi Indonesia*. 59-64. 2018.