RIZKI DEWANTARA
NIM. 18206050002

EVALUASI METODE OSSIM TERHADAP PENINGKATAN KEAMANAN INFORMASI (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)

PROGRAM STUDI INFORMATIKA
PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI
UIN SUNAN KALIJAGA YOGYAKARTA

2020

RIZKI DEWANTARA
NIM.18206050002

EVALUASI METODE OSSIM
TERHADAP PENINGKATAN KEAMANAN INFORMASI
(STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)

2020

EVALUASI METODE OSSIM TERHADAP PENINGKATAN KEAMANAN INFORMASI (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)

Oleh :

Nama : Rizki Dewantara

NIM : 18206050002

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI

UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA

YOGYAKARTA

2020

PROGRAM STUDI INFORMATIKA

PROGRAM MAGISTER FAKULTAS SAINS DAN TEKNOLOGI

UIN SUNAN KALIJAGA YOGYAKARTA

Rizki Dewantara

NIM. 18206050002

EVALUASI METODE OSSIM TERHADAP PENINGKATAN KEAMANAN INFORMASI (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)

2020

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Rizki Dewantara

NIM : 18206050015

Jenjang : Magister

Program Studi : Informatika

Menyatakan bahwa naskah tesis dengan judul " Evaluasi Metode OSSIM Terhadap Peningkatan Keamanan Informasi (Studi Kasus : UIN Sunan Kalijaga Yogyakarta)" tidak terdapat pada karya yang pernah diajukan untuk memperoleh gelar Magister di suatu Perguruan Tinggi, dan sepengatahuan saya tidak terdapat karya atau pendapat yang pernah ditulis oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 28 Desember 2019

Saya yang menyatakan,

Rizki Dewantara

NIM: 18206050002

PERNYATAAN BEBAS PLAGIASI

Yang bertanda tangan di bawah ini:

Nama : Rizki Dewantara

NIM : 18206050002

Jenjang : Magister

Program Studi : Informatika

menyatakan bahwa naskah tesis ini secara keseluruhan benar-benar bebas dari plagiasi. Jika di kemudian hari terbukti melakukan plagiasi, maka saya siap ditindak sesuai ketentuan hukum yang berlaku.

Yogyakarta, 28 Desember 2019

Saya yang menyatakan,

Rizki Dewantara

NIM: 18206050002

KEMENTERIAN AGAMA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
FAKULTAS SAINS DAN TEKNOLOGI
Jl. Marsda Adisucipto Telp. (0274) 540971 Fax. (0274) 519739 Yogyakarta 55281

PENGESAHAN TUGAS AKHIR

Nomor : B-1168/Un.02/DST/PP.00.9/06/2020

Tugas Akhir dengan judul : Evaluasi Metode OSSIM terhadap Peningkatan Keamanan Informasi (Studi Kasus: UIN Sunan Kalijaga Yogyakarta)

yang dipersiapkan dan disusun oleh:

Nama : RIZKI DEWANTARA, S.Kom
Nomor Induk Mahasiswa : 18206050002
Telah diujikan pada : Jumat, 24 April 2020
Nilai ujian Tugas Akhir : A/B

dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta

TIM UJIAN TUGAS AKHIR

Ketua Sidang

Dr. Bambang Sugiantoro, S.Si., M.T.
SIGNED

Valid ID: 5ed8b96167157

Penguji I

Dr. Shofwatul 'Uyun, S.T., M.Kom.
SIGNED

Valid ID: 5ed8bf02e51d4

Penguji II

Maria Ulfah Siregar, S.Kom. MIT., Ph.D.
SIGNED

Valid ID: 5ed8b21b580f7

Yogyakarta, 24 April 2020
UIN Sunan Kalijaga
Dekan Fakultas Sains dan Teknologi

Dr. Murtono, M.Si.
SIGNED

Valid ID: 5ed9bf42d3854

PERSETUJUAN TIM PENGUJI UJIAN

Tesis berjudul : Evaluasi Metode OSSIM Terhadap Peningkatan Keamanan Informasi (Studi Kasus : UIN Sunan Kalijaga Yogyakarta)

Nama : Rizki Dewantara

NIM : 18206050002

Prodi : Magister Informatika

telah disetujui tim penguji ujian munaqosah

Ketua Penguji/Pembimbing : Dr. Bambang Sugiantoro, S.Si., M.T.

Valid ID: 5ed8b96167157

Penguji 1 : Dr. Shofwatul 'Uyun, S.T., M.Kom.

Valid ID: 5ed8bf02e51d4

Penguji 2 : Maria Ulfah Siregar, S.Kom. MIT., Ph.D.

Diuji di Yogyakarta pada tanggal Jum'at 24 April 2020

Waktu : 15.00 – 16.00 WIB

Hasil/Nilai : _____

Predikat : ~~Memuaskan~~/Sangat Memuaskan/~~Cumlaude~~*

* Coret yang tidak perlu

NOTA DINAS PEMBIMBING

Kepada Yth.,
Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta

Assalamu 'alaikum wr. wb.

Setelah melakukan bimbingan, arahan, dan koreksi terhadap penulisan tesis yang berjudul:

Evaluasi Metode OSSIM Terhadap Peningkatan Keamanan Informasi
(Studi Kasus : UIN Sunan Kalijaga Yogyakarta)

Yang ditulis oleh:

Nama : Rizki Dewantara
NIM : 18206050002
Jenjang : Magister
Program Studi : Informatika

Saya berpendapat bahwa tesis tersebut sudah dapat diajukan kepada Magister Informatika UIN Sunan Kalijaga untuk diujikan dalam rangka memperoleh gelar Magister Informatika.

Wassalamu'alaikum wr. wb.

Yogyakarta, 28 Desember 2019

Pembimbing,

(Dr. Bambang Sugiantoro, S.Si., M.T.)

ABSTRAK

Serangan pada jaringan saat ini sangat sering terjadi, dengan semakin banyaknya cara untuk melakukan pengaksesan terhadap data dan semakin berkembangnya teknologi yang digunakan tentunya akan menyebabkan meningkatnya ancaman keamanan suatu jaringan. Evaluasi manajemen keamanan informasi menggunakan indeks keamanan informasi (KAMI) yang dilakukan pada jaringan di UIN Sunan Kalijaga Yogyakarta didapatkan hasil indeks 407 sehingga belum optimal. Hal ini yang mendasari perlunya implementasi Open Source SIEM (OSSIM) kedalam indeks KAMI. Penelitian ini dilakukan sebagai optimasi untuk mendukung proses keamanan informasi agar dapat bekerja sesuai dengan standar indeks KAMI. Metode penelitian yang digunakan meliputi studi literatur, melakukan Pre-Assesment Indeks KAMI, mengimplementasi infrastruktur OSSIM, monitoring indeks keamanan informasi menggunakan teknologi OSSIM, dan melakukan Post-Assesment Indeks KAMI, tahapan akhir ini menganalisis hasil monitoring untuk dibuat perbandingan bagaimana kondisi jaringan sebelum dan sesudah diimplementasikan OSSIM pada jaringan. Skor nilai perbandingan dari hasil penelitian terkait Indeks KAMI menunjukkan peningkatan skor penilaian sebesar 25, setelah diterapkan penggunaan OSSIM dari sebelumnya tanpa penerapan OSSIM sebesar nilai 407 menjadi 432. Peningkatan indeks KAMI membantu menaikan nilai pada aspek tata kelola, pengelolaan asset dan teknologi, namun tingkat kelayakan keamanan informasi masih di level I+ sampai dengan II+ sehingga keamanan informasi pada jaringan tidak layak dan butuh perbaikan.

Dengan hasil evaluasi akhir ini juga menunjukan bahwa jaringan UIN Sunan Kalijaga Yogyakarta membutuhkan perbaikan. dimana yang hasilnya sesuai data sesungguhnya sehingga dapat digunakan untuk membantu perbaikan pada jaringan UIN Sunan Kalijaga Yogyakarta berdasarkan Indeks Keamanan Informasi. Dalam hubungannya dengan indeks keamanan informasi (KAMI) pengunaan teknologi OSSIM terbukti menaikan nilai indeks Keamanan Informasi (KAMI) Jaringan UIN Sunan Kalijaga Yogyakarta di pada berbagai aspek, adapun kenaikan ini karena kemampuan OSSIM dalam menganalisa kelemahan dan perubahan konfigurasi asset informasi di Jaringan UIN Sunan Kalijaga Yogyakarta.

Kata kunci: ***Indeks*** **KAMI, Keamanan Informasi. OSSIM**

ABSTRACT

Attacks on networks today are very common, with more and more ways to access data and the development of technology used, they will certainly cause an increase in network security threats. Evaluation of information security management using the information security index (KAMI) conducted on the network at UIN Sunan Kalijaga Yogyakarta obtained an index result of 407, so it is not optimal. This is what underlies the need to implement Open Source SIEM (OSSIM) into the KAMI index. This research was conducted as an optimization to support the information security process so that it can work according to the KAMI index standards. The research methods used include literature study, conducting KAMI Index Pre-Assessment, implementing OSSIM infrastructure, monitoring information security index using OSSIM technology and conducting KAMI Index Post-Assessment, this final stage analyzes the results of monitoring to make comparisons of network conditions before and after implementation of OSSIM on the network. Comparative scores from the results of research related to the KAMI Index show an increase in the score of 25, after applying OSSIM from before without applying OSSIM, the value of 407 becomes 432. The increase in the KAMI index helps raise the value of governance aspects, asset management and technology, but the level of information security eligibility is still at the level of I+ to II+ so the information security on the network is not feasible and needs improvement.

where the results match the actual data so that it can be used to help improve the UIN Sunan Kalijaga network based on the Information Security Index. In connection with the information security index (US) the use of OSSIM technology has been proven to increase the value of the Information Security index (US) of Sunan Kalijaga Yogyakarta UIN Network in various aspects, while this increase is due to OSSIM's ability to analyze weaknesses and changes in the configuration of information assets in the UIN Sunan Kalijaga Network Yogyakarta.

Keywords: Indeks KAMI, Information Security.OSSIM

KATA PENGANTAR

Puji Syukur kehadirat Allah SWT yang telah memberikan rahmat dan hidayah-Nya, sehingga penyusun masih dapat merasakan segala nikmat anugerah dan kesempatan yang diberikan dalam penyelesaian Tesis yang berjudul "**EVALUASI METODE OSSIM TERHADAP PENINGKATAN KEAMANAN INFORMASI (STUDI KASUS : UIN SUNAN KALIJAGA YOGYAKARTA)".**

Sholawat serta salam semoga senantiasa tercurahkan kepada baginda Nabi Muhammad SAW, semoga kita sebagai umatnya mendapat *syafa'at* darinya kelak di hari akhir. Tesis ini disusun untuk memenuhi sebagian persyaratan guna mendapatkan gelar Magister Informatika Pada Program Studi Informatika (S2) Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dalam kesempatan ini penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Bapak Prof. Drs. KH Yudian Wahyudi, Ph.D., Selaku Rektor UIN Sunan Kalijaga Yogyakarta
2. Bapak Dr. Murtono, M.Si., selaku Dekan Fakultas Sains dan Teknologi
3. Bapak Dr. Bambang Sugiantoro, S.Si., M.T., dan Ibu Maria Ulfah Siregar, S.Kom. MIT., Ph.D., sebagai Kepala dan Sekretaris Program Studi Informatika Program Magister Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta,
4. Bapak Dr. Bambang Sugiantoro, S.Si., M.T., selaku Dosen Pembimbing Akademik Magister Informatika 2018.

5. Bapak Dr. Bambang Sugiantoro, M.T., selaku Dosen Pembimbing Tesis yang dengan sabar telah meluangkan waktunya untuk membimbing serta memberikan koreksi dan saran kepada penulis dalam menyelesaikan penelitian Tesis ini.
6. Bapak dan Ibu dosen Program Studi Magister Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta yang telah memberikan ilmu dan pengalaman kepada penulis selama masa kuliah.
7. Seluruh Staff Bagian Kemahasiswaan Sains dan Teknologi, PTIPD UIN Sunan Kalijaga yang telah membantu dalam menyelesaikan Penelitian ini.
8. Teman-teman sepenjuangan Program Studi Magister Informatika 2018 yang telah memberi dukungan dan bantuan dalam penelitian ini.
9. Semua pihak yang tidak dapat penulis sebutkan satu persatu yang telah membantu dalam proses penyelesaian tesis ini.

Penulis menyadari masih banyak kekurangan dan kelemahan dalam pelaksanaan dan penyusunan tesis ini. Oleh karena itu kritik dan saran penulis harapkan untuk dapat menyempurnakannya.Semoga tesis ini dapat bermanfaat bagi pembaca dan penulis khususnya.

Yogyakarta, 28 Desember 2019

Penyusun,

Rizki Dewantara
NIM:18206050007

HALAMAN PERSEMBAHAN

Alhamdulillahirobbil alamiin, atas keridhoan Allah SWT sebagai dzat yang maha kuasa, atas berkah rahmat, hidayah serta karunia-Nya sehingga salah satu kewajibanku ini dapat diselesaikan. Tak lupa sholawat serta salam kepada junjungan Nabi Besar Muhammad SAW semoga *syafa'at* diberikan di akhir zaman. Halaman ini saya tujukan terhadap semua pihak yang telah membantu dan Mensupport Penyelesain Tesis ini, sebagai berikut :

1. Kedua Orang Tua Tercinta, Ibunda Wiwik Rukmiyati, SE dan Ayahanda Iskandarsyah, SE., SH., MM serta Kakakku drg. Denie Candra Asmara serta seluruh anggota keluarga tercinta, yang selalu memberikan nasehat, dukungan, motivasi dan do'anya. Allahummaghfirlii waliwaalidayya warhamhumma kama rabbayaanii shagiraa.
2. Terima kasih banyak untuk bapak Pembimbing saya Bapak Dr. Bambang Sugiantoro, M.T., yang telah membimbing saya dalam pembuatan tesis ini.
3. Segenap Dosen Teknik Informatika dan Magister Informatika UIN Sunan Kalijaga Yogyakarta, Pak Bambang, Pak Agung , Pak Sumarsono, Pak Didik, Pak Nurochman, Pak Agus, Pak Mustaqim, Pak Aulia, Pak Imam, Pak Awik, Pak Taufik, Bu Uyun, Bu Maria, Bu Ade, terima kasih atas ilmu yang telah diberikan selama menempuh perkuliahan, semoga bermanfaat dikemudian hari.

4. Selvira Monita, S.Si yang telah memberikan saran, bantuan dan semangat selama proses pengerjaan Tesis. Terima kasih atas kesabaran menghadapi penulis dalam menyelesaikan tiap bait-bait tesis ini.
5. Teman-teman Seperjuangan, keluarga besar Magister Informatika sebagai **Founding Fathers** Angkatan pertama yang tidak bisa saya sebutkan satu persatu, terima kasih untuk kebersamaanya dan dukungan kalian setiap perjuangan kita sebagai mahasiswa Magister Informatika di UIN Sunan Kalijaga Yogyakarta.
6. Sahabat PMII KORP FREKUENSI beserta segenap Keluarga besar AUFKLARUNG dalam berproses berorganisasi selama ini.
7. Seluruh Teman-teman Senat Mahasiswa Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta.
8. Keluarga Besar Teknik Informatika Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta
9. Keluarga Besar Magister Informatika Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta
10. Ibu Dr. Shofwatul 'Uyun, S.T., M.Kom selaku Kepala UPT PTIPD UIN Sunan Kalijaga yang telah memberikan izin penelitian tesis.
11. Pak Hendra Hidayat, S. Kom dan Pak Rahmadhan Gatra, S.T. selaku bagian Divisi Teknologi Informasi UIN Sunan Kalijaga yang telah memberikan izin dan yang telah membantu dalam hal penelitian tesis ini.

12. Konco-konco Seperjuangan OTW jadi Bos (Jhony, Maulana, Setyo, Yuha, Yudi, Asep, Anggoro, Zahid, Roni, Aji Wahyu, Taufik, Tulus, Alviyan, Ryan) yang telah menemani setiap jejak langkah perjuangan saya selama menuntut ilmu di Yogyakarta, terima kasih untuk canda tawa, menyemangati saya dalam mengerjakan tesis ini serta tidak lupa lengkap dengan misuh-misuhnya.
13. PT Indomie, yang selalu menemani ketika lapar dan pusing disaat mengerjakan tugas kuliah.
14. Warung Kopi Legend, Nemo, Almond , NetCity, Blandongan, Kopas, Basa Basi yang menjadi tempat mencari inspirasi pembuatan kata demi kata pengerjaan Tesis ini hingga selesai.
15. Kupersembahkan tesis ini untuk orang yang bertanya " kapan tesismu selesai..?? ^_^ "
16. Saya berterima kasih banyak kepada semua pihak yang telah membantu saya dalam menyesaikan tesis ini. Terima kasih telah membuatku tersadar bahwa saya mempunyai tanggung jawab menyelesaikan tesis ini walaupun ada hal-hal yang tidak kalah penting selain menyelesaikan tesis ini, terima kasih kepada konco-koncoku yang bersedia meluangkan waktunya untuk menemaniku padahal memiliki kesibukannya masing-masing dan meyakinkan serta menyadarkanku bahwa cepat atau lambat semua bakal selesai pada waktunya dan berakhir bahagia, bahwa Tuhan adalah sebaik-sebaiknya Sutradara yang membuatku mengerti bahwa hidup tak seharusnya dijadikan kambing

hitam meskipun rasa ngantuk dan males melanda diriku ketika mengerjakannya

Sekian halaman persembahan ini saya buat sebagai apresiasi terhadap semua pihak yang telah memberi bantuan secara doa, moral, dan material dalam penunjang tesis saya ini. telah Terima kasih banyak dan mohon maaf apabila saya ada kesalahan dalam penulisan, mohon dimaafkan.

MOTTO

اَمَّنْ يُّجِيْبُ الْمُضْطَرَّ اِذَا دَعَاهُ وَيَكْشِفُ السُّوْۤءَ وَيَجْعَلُكُمْ خُلَفَاۤءَ الْاَرْضِ ۗ ءَاِلٰهٌ مَّعَ اللّٰهِ ۗ قَلِيْلًا مَّا تَذَكَّرُوْنَ ۗ

"Bukankah Dia (Allah) yang memperkenankan (doa) orang yang dalam kesulitan apabila dia berdoa kepada-Nya, dan menghilangkan kesusahan dan menjadikan kamu (manusia) sebagai khalifah (pemimpin) di Bumi? Apakah di samping Allah ada Tuhan (yang lain)? Sedikit sekali (nikmat Allah) yang kamu ingat."

(QS. An-Naml 27: Ayat 62)

Hidup ini seperti pensil yang pasti akan habis, tetapi meninggalkan tulisan-tulisan yang indah dalam kehidupan

(One Piece)

Jika Anda tidak bisa berlari maka berjalanlah, jika Anda tidak bisa berjalan maka merangkak, ingat apapun yang terjadi dan apapun yang Anda lakukan, Anda harus terus bergerak maju, jangan pernah berhenti walau sedetik, apalagi jangan pernah mundur walau hanya 1 mili, karena cita-cita anda disana sedang menunggu anda

Terlambat lulus atau lulus tidak tepat waktu bukan sebuah kejahatan, bukan juga sebuah aib, alangkah kecilnya jika seseorang mengukur kepintaran seseorang hanya dari siapa yang paling cepat lulus. Bukanlah sebaik-baiknya kerjaan adalah kerjaan yang selesai ? baik itu selesai tepat waktu maupun tidak tepat waktu

(Rizki Dewantara)

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR SINGKATAN

OSSIM	: *Open Source System Information Management*
KAMI	: Keamanan Informasi
IDS	: *Intrusion Detection System*
TCP	: *Transmision control protocol*
UDP	: *Use Datagram Protocol*
ICMP	: *Internet Control Message Protocol*
TFTP	: *Trivial File Transfer Protokol*

BAB I
PENDAHULUAN

A. Latar Belakang

Dengan Semakin banyaknya jumlah pengguna layanan intenet maka semakin banyak infomasi yang dapat diperoleh dari internet. Di seluruh Dunia Terdapat sekitar 640 *Terabytes* data dan 204 juta *email* dikirim melalui jaringan internet setiap menitnya(Rick B, 2013). Perencanaan, perancangan dan implementasi suatu topologi jaringan, dalam hal ini adalah jaringan komputer nirkabel, tidak dapat dihandalkan begitu saja. Perluasan jaringan komputer akan membawa dampak yang signifikan pada kualitas layanan koneksi internet maupun kondisi pertukaran data yang ada. Jika pada awal perbuatan jaringan komputer, koneksi internet yang ada hanya bisa digunakan oleh 1 (satu) fakultas saja namun sekarang digunakan menjadi 9 (Sembilan) fakultas yang terdiri dari : Fakultas Adab dan Ilmu Budaya, Fakultas Dakwah dan Komunikasi, Fakultas Ilmu Tarbiyah dan Keguruan, Fakultas Syariah dan Hukum, Fakultas Ushuluddin dan Pemikiran Islam, Fakultas Sains dan Teknologi, Fakultas Ilmu Sosial dan Humaniora, Fakultas Ekonomi dan Bisnis Islam dan Fakultas Pascasarjana. Kualitas layanan internet maupun koneksi pertukaran data setelah adanya perluasan jaringan tersebut tentunya akan sangat mengubah performa jaringan komputer menurun.

Berdasarkan peraturan Menteri Komunikasi dan Informatika No.4 Tahun 2016 tentang Standar Sistem Managemen Keamanan Informasi, setiap lembaga pemerintah wajib mematuhi SMKI dengan memegang nilai CIA (Confidentiality, Availability dan Integrity) terhadap aset informasi yang ada di instansinya.

Berdasarkan penelitian yang dilakukan oleh tim *Iccsindia* yang dijelaskan bahwa kerusakan *cybercrime* diperkirakan mencapai 6 triliun, terdapat 60 juta catatan dilanggar karena *cloud* yang tidak terkonfigurasi sesuai keamanan jaringan. Pelanggaran keamanan terjadi pada usaha kecil dengan total serangan mencapai 43%. Pelanggaran data mencapai 56% membutuhkan waktu lebih dari sebulan untuk ditemukan penangannya. Kemudian diperkuat dengan data dari serangan *Ransomware* paling umum ditemui pada tahun 2019, tetapi *WannaCry* terus membuat korban di seluruh dunia, dengan laporan baru mengungkapkan bahwa itu tetap menjadi infeksi *ransomware* nomor satu tahun lalu.

Lebih dari 23,5% perangkat yang akhirnya dikunci oleh *ransomware* menangkap *WannaCry*, *Precise Security* mengatakan, dengan *email spam* dan *phishing* tetap menjadi sumber infeksi paling umum tahun lalu. Tidak kurang dari 67% dari infeksi *ransomware* dikirim melalui email, sementara kurangnya pelatihan keamanan dunia maya dan kata sandi yang lemah serta manajemen akses adalah penyebab berikutnya dari komputer yang akhirnya dienkripsi setelah serangan. Hanya 16% dari serangan ransomware yang diberdayakan oleh situs web

berbahaya dan iklan *web*. "Jumlah serangan *ransomware* terhadap lembaga pemerintah, organisasi di bidang kesehatan, sektor energi, dan pendidikan terus meningkat. Sementara beberapa *ransomware* sederhana dapat mengunci sistem dengan cara yang tidak sulit bagi orang yang berpengetahuan untuk membalikkan, *malware* yang lebih maju mengeksploitasi teknik yang disebut pemerasan *kripto*-virus,

Dengan semakin banyaknya cara untuk melakukan pengaksesan terhadap data dan semakin berkembangnya teknologi yang digunanakan tentunya akan menyebabkan meningkatnya ancaman keamanan terhadap suatu jaringan. Hal ini tentu sangat berbahaya terutama pada bidang-bidang yang memiliki keamanan data yang sensitif terhadap data-data fakultas. Untuk itulah diperlukan sebuah perhatian khusus dalam bidang keamanan jaringan yang bertujuan untuk mencegah terjadinya percurian data-data perusahaan.

Di sisi lain, kejahatan komputer adalah salah satu masalah yang menjadi perhatian kami di dunia cyber saat ini. Ini jelas melibatkan moralitas buruk yang dilarang oleh Allah dan Rasul-Nya seperti ketidakpercayaan, penipuan dan mencuri. Kejahatan komputer tumbuh sangat cepat dibandingkan dengan kejahatan lain dan menyebabkan kerusakan serius pada sektor politik, ekonomi dan sosial (Lu, Liang and Taylor, 2010). Allah SWT telah melarang manusia untuk melanggar hak orang lain seperti ketidakpercayaan, penipuan dan mencuri. Hal ini jelas dibuktikan

dalam ayat-ayat al-Quran yang melarang manusia untuk berperilaku dengan moralitas buruk. Ini juga bertentangan dengan tujuan utama nabi Rasulullah S.A.W. sebagai Utusan Allah, yang memberikan contoh hidup dari moralitas yang baik untuk diikuti manusia. Rasulullah S.A.W. berkata "Saya telah dikirim untuk memuji moralitas yang baik" (Al-Baihaqi, 1994).

Universitas Islam Negeri Sunan Kalijaga Yogyakarta adalah kampus Islam negeri di Yogyakarta. UIN Sunan Kalijaga Yogyakarta memiliki Pusat Teknologi Informasi dan Pangkalan Data (PTIPD) UIN Sunan Kalijaga Yogyakarta memiliki Sistem Informasi Akademik (SIA) yang dibangun dengan tujuan untuk memberikan layanan kepada mahasiswa dan pihak *administrator* di tiap fakultas dalam menyelenggarakan sistem administrasi akademik. Di dalamnya terdapat layanan pengisian KRS online, KHS online, penjadwalan, presensi, nilai mahasiswa dan lain-lain. Layanan ini berbasis *web* agar lebih leluasa untuk dapat diakses melalui jaringan internet, yang di *input* secara *real time* setiap harinya. Oleh karena itu, jaringan dan internet sangatlah dibutuhkan untuk menunjang pekerjaan yang dilakukan oleh setiap sinitas akademik UIN Sunan Kalijaga Yogyakarta setiap harinya. Kampus ini sudah memiliki jaringan komputer yang terhubung dengan internet dari *vendor* sebuah *provider*. Berdasarkan *observasi* yang penulis lakukan keamanan Jaringan dan internet di kampus ini hanya dibangun melalui *default* dari vendor. Jaringan pada kampus ini sering terputus pada waktu – waktu tertentu, tetapi

belum diketahui masalah yang menyebabkan jaringan ini sering terputus. Oleh karena itu, penulis berpikir jika kampus ini memerlukan sistem monitoring jaringan untuk mengawasi keadaan jaringan serta memberi peringatan apabila ada yang mengancam kemananan jaringan.

Dengan adanya kebutuhan instansi pemerintahan untuk dapat menerapkan Standar Managemen Keamanan Informasi sesuai dengan SMKI dan Kebutuhan monitoring terhadap network menjadi pilihan yang mutlak agar *security officer* dapat dengan jelas melihat apa yang terjadi dengan jaringannya. Yang menjadi pertanyaan adalah apakah penggunaan OSSIM bisa mendeteksi semua serangan yang ada pada jaringan dan efektif mengamankan jaringan dari serangan yang ada.

Khusus dalam hal memonitor server dan jaringan tentunya seorang administrator tidak dapat bekerja 24 jam didepan komputernya sehingga selalu mengetahui apabila terjadi gangguan pada *server* dan jaringan.(Angga Juansyah, Bagus Pratama, 2018), oleh karena itu diperlukan sebuah fasilitas pendukung yaitu sistem monitoring agar administrator dapat memonitor *server* dan jaringan meskipun tidak berada didepan komputer secara langsung, sehingga dibutuhkan suatu sistem monitoring yang dapat memantau *server* dan jaringan mereka selama 24 jam dan mendapat notifikasi langsung kepada adminnya.

Sebelum standar keamanan informasi diterapkan, perlu dilakukan evaluasi *system* keamanan informasi di jaringan UIN

Sunan Kalijaga Yogyakarta untuk mendapatkan gambaran kondisi kesiapan dan kematangan manajemen keamanan informasi tersebut. Berdasarkan hal tersebut penelitian ini akan mengukur tingkat kematangan manajemen keamanan informasi pada jaringan UIN Sunan Kalijaga Yogyakarta mengunakan model yang di siapkan oleh Kominfo RI tahun 2019, yaitu *indeks* KAMI. *Indeks* KAMI dibuat dengan acuan ISO 27001:2018 yang berisi tentang keamanan informasi ISO 27001 adalah suatu bentuk kerangka kerja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi, lingkup penggunaan teknologi dan pengelolaan aset yang membantu organisasi memastikan bahwa keamanan informasi sudah berjalan dengan efektif

Berdasarkan latar belakang tersebut, Penulis membuat penelitian dengan judul ”Evaluasi Metode OSSIM Terhadap Peningkatan Keamanan Informasi (Studi Kasus : UIN Sunan Kalijaga Yogyakarta) “.

B. Rumusan Masalah

Dari latar belakang dan permasalahan yang telah disampaikan di atas, permasalahan yang menjadi fokus penelitian ini adalah :

1. Bagaimana menganalisis Sistem Informasi Akademik UIN Sunan Kalijaga sehingga dapat mencukupi kebutuhan informasi dari pengguna dalam melakukan pertukaran data dengan melakukan penelitian dengan

metode *Open Source System Information Management* (OSSIM) dan implikasinya pada *indeks* Keamanan Informasi (KAMI)?

2. Bagaimana memonitoring *server* untuk Sistem Informasi Akademik UIN Sunan Kalijaga dalam melakukan proses pertukaran data didalam sebuah jaringan komputer yang memiliki jumlah *client* yang banyak dan aktifitas jaringan komputer dalam skala besar ?

C. Batasan Masalah

Agar permasalahan tidak meluas, maka masalah yang diteliti dibatasi sebagai berikut:

1. Daerah dibatasi hanya pada Sistem Informasi Akademik kampus UIN Sunan Kalijaga.
2. Menggunakan *software Open source* yaitu *OSSIM AlienVault* pada *server* yang dirancang.
3. Pengujian sistem dilakukan dengan simulasi di UIN Sunan Kalijaga Yogyakarta.
4. Penerapan *Security Information And Event Management* (SIEM) dengan menggunakan OSSIM (Open Source Security Information Management) pada jaringan komputer yang berjalan pada simulasi GNS 3.
5. Pada Indeks Keamanan Informasi (KAMI) menggunakan kuosioner untuk mengetahui celah sistem yang berjalan.

D. Tujuan Penelitian

Dengan memonitor kondisi jaringan UIN Sunan Kalijaga Yogyakarta dapat diperoleh tujuan dari penelitian ini, yakni :

1. Memantau dan mengetahui lebih Detail permasalahan yang ada pada Jaringan UIN Sunan Kalijaga Yogyakarta sehingga dapat diketahui pola solusi untuk mengatasinya sehingga dapat memaksimalkan infrastruktur jaringan komputer yang ada dengan lebih efektif dan efisien sesuai fungsinya sebagai institusi pendidikan.
2. menganalisa dan menggambarkan untuk mendapatkan hasil pengukuran yang akurat dalam hal keamanan informasi pada sistem informasi akademik dan meningkatkan kualitas keamanan informasi. Selain itu untuk mengetahui tingkat kematangan sistem keamanan yang digunakan pada sistem informasi akademik. Diharapkan hasilnya dapat digunakan sebagai bahan pertimbangan dalam rangka menyusun langkah-langkah perbaikan manajemen keamanan sistem informasi pada Sistem Informasi UIN Sunan Kalijaga Yogyakarta.
3. Untuk mengetahui hasil penerapan *Security Information And Event Management (SIEM) Dan Implikasinya Pada Indeks Keamanan Informasi (KAMI)* pada jaringan UIN Sunan Kalijaga Yogyakarta

dengan Menciptakan sistem pendeteksi atau sensor terhadap area jaringan menggunakan aplikasi berbasis *open source*, yaitu *alientvault* OSSIM sehingga Memberikan laporan kepada *administrator* sistem mengenai upaya penyerangan terhadap sistem, melalui catatan atau *log* yang dihasilkan oleh aplikasi sebagai bukti digital yang mencatat segala upaya penyerangan atau penetrasi ke dalam suatu *area server*.

E. Manfaat Penelitian

Penelitian ini diharapkan dapat memberi beberapa manfaat, antara lain:

1. Bagi pemakai, akan mendapatkan pengetahuan yang terbaik didalam penggunaan jaringan pada suatu intansi untuk memperoleh informasi yang dibutuhkan.
2. Bagi penulis, sebagai acuan untuk mendokumentasikan serta memberikan laporan secara rinci kepada administrator sistem mengenai kondisi keamanan dari lalu lintas jaringan dan server, sehingga dapat dilakukan tindakan-tindakan pencegahan upaya penyerangan demi menjaga stabilitas dari layanan. yang sesuai dengan kondisi jaringan komputer pada Universitas Sunan Kalijaga Yogyakarta.
3. Sebagai Salah satu solusi pada *Network Administrator* yang lebih sesuai dengan kebutuhan sesuai dengan

fungsinya sehingga menjadikan jaringan menjadi lebih optimal dengan perannya sebagai Institusi Pendidikam.

4. Manfaat yang ingin diperoleh dari penelitian ini adalah sistem yang dihasilkan dapat memperkecil kemungkinan terjadinya kegagalan sistem pada server sehingga akses data setiap ada permintaan yang ada dapat dilayani dengan baik dan lancar dengan biaya seminimal mungkin dan hasil yang semaksimal mungkin.

F. Keaslian Penelitian

Penelitian yang berhubungan dengan implementasi *Open Source Security Information Managament* (OSSIM) ini sudah pernah dilakukan sebelumnya. Akan tetapi penelitian tentang Evaluasi Metode Ossim Terhadap Peningkatan Keamanan Informasi (Studi Kasus : UIN Sunan Kalijaga Yogyakarta) belum pernah dilakukan sebelumnya.

G. Sistematika Penulisan

Adapun sistematika penulisan pada penelitian ini terdiri atas enam bab, dengan sistematika sebagai berikut:

- Bab 1 Pendahuluan

  Membahas latar belakang mengenai penggunaan *Open Source System Information Management* (OSSIM) dalam suatu organisasi. Pada bab ini juga membahas mengenai Rumusan Masalah, Batasan Masalah, Tujuan Penelitian,

Manfaat Penelitian, Metodologi Penelitian dan Sistematika Penulisan Laporan pada penelitian yang dilakukan.

- Bab 2 Tinjauan Pustaka

  Membahas teori dasar yang digunakan dalam penelitian, terkait *Open Source System Information Management* (OSSIM), *indeks* KAMI. Pada bab ini juga dibahas mengenai tinjauan pustaka terkait penelitian yang pernah dilakukan sebelumnya.

- Bab 3 Metode Penelitian,

  Membahas langkah-langkah penelitian, analisis kebutuhan dan perancangan sistem, membahas analisis terhadap kebutuhan sistem yang dibangun, proses kerja dan perancangan sistem (Topologi. Insfratruktur, pilihan *Software* dll).

- Bab 4 Analisis dan Pembahasan,

  Membahas hasil penelitian berupa eksekusi model yang diusulkan dan pengujian parameter.

- Bab 5 Penutup

  Membahas kesimpulan berupa rangkuman dari hasil dan pembahasan pada bab sebelumnya serta saran yang perlu diperhatikan berdasarkan keterbatasan yang ditemukan dan asumsi-asumsi yang ada selama penelitian untuk perbaikan dan pengembangan berikutnya.

BAB V
PENUTUP

A. Kesimpulan

1. Tingkat kematangan dan kelengkapan keamanan informasi jaringan UIN Sunan Kalijaga Yogyakarta masih rendah. penyebab rendahnya tingkat kelengkapan dan kematangan keamanan informasi ini adalah jaringan UIN Sunan Kalijaga Yogyakarta belum menerapkan semua syarat keamanan informasi atau masih dalam perencanaan. Rendahnya tingkat kelengkapan ini ditunjukan oleh bar chart yang menunjukan warna merah dengan total nilai 272, warna kuning dengan total nilai 455 dan warna hijau muda dengan total nilai 583 yang artinya keamanan informasi pada jaringan UIN Sunan Kalijaga Yogyakarta tidak layak dan butuh perbaikan. Sedangkan tingkat kematangan setiap area keamanan informasi masih di I+ s/d II+,. Sedangkan sebagai kebijakan standar ISO/IEC 27001:2018, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah tingkat III+.
2. Dalam hubungannya dengan indeks keamanan informasi (KAMI) pengunaan teknologi OSSIM terbukti meningkatkan nilai *indeks* Keamanan Informasi (KAMI) Jaringan UIN Sunan Kalijaga Yogyakarta pada berbagai aspek. Adapun kenaikan ini karena kemampuan OSSIM dalam menganalisa kelemahan dan perubahan konfigurasi asset informasi di Jaringan UIN Sunan Kalijaga Yogyakarta. OSSIM juga dapat memonitor dan melakukan proses analisa dan audit terhadap asset yang dimiliki

Jaringan UIN Sunan Kalijaga Yogyakarta secara rutin dan sistematis.

B. Saran

Saran untuk penelitian yang akan datang adalah dibangunnya kesadaran dari para staff PTIPD UIN Sunan Kalijaga terkait keamanan informasi. Para *staff* harus terlebih dahulu menyadari pentingnya suatu keamanan informasi untuk melindungi seluruh aspek yang berkaitan dengan keamanan informasi dalam mendukung jalannya kinerja proses jaringan. Indeks KAMI sebaiknya digunakan 2 kali dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu. Untuk Evaluasi selanjutnya menggunakan standarisasi lainnya selain Indeks KAMI, seperti COBIT 5, TOGAF 9, ISO 15500 dan tools yang lainnya.

DAFTAR PUSTAKA

Achmad, B., Nur, I. W. and Siti, K. (2019) 'Development of Linux Ubuntu Open Source Distribution Based Open Source Distribution System to Minimize Students 'Software Study', 287(Icesre 2018), pp. 286–290. doi:10.2991/icesre-18.2019.63.

Akhirina, T. Y., Arif, S. M. and . R. (2016) 'Evaluasi Keamanan Teknologi Informasi pada PT Indotama Partner Logistics Menggunakan Indeks Keamanan Informasi (KAMI)', *Jurnal Nasional Teknologi dan Sistem Informasi*, 2(2), pp. 53–62. doi: 10.25077/teknosi.v2i2.2016.53-62.

Al-Baihaqi, A. bin al-H. bin A. (1994) *Sunan al-Baihaqi al-Kubro*. Makkah:Maktabah Dar Al-Baz.

Al-Quran al-Karim.

Angga Juansyah, Bagus Pratama, I. D. (2018) 'Analisis dan implementasi open source security information managament (ossim) pada keamanan jaringan komputer pt. satria antaran prima palembang'.

Arfanudin, C. (2017) 'Real Time Analisis Keamanan Router Di Jaringan Dengan Security Information and Event Management (Siem) Dan Implikasinya Pada Indeks Keamanan Informasi (Kami) Real Time Analisis Keamanan Router Jaringan Dengan Security Information and Event Management'.

Basyarahil, F. A., Astuti, H. M. and Hidayanto, B. C. (2017) 'Evaluasi Manajemen Keamanan Informasi Menggunakan Indeks Keamanan Informasi (KAMI) Berdasarkan ISO/IEC 27001:2013 Pada Direktorat Pengembangan Teknologi Dan Sistem Informasi (DPTSI) ITS Surabaya', *Jurnal Teknik ITS*, 6(1), p. 227. doi: 10.1016/j.juro.2016.01.039.

Chazar, C. and Ramdani, A. (2016) 'Model perencanaan keamanan sistem informasi menggunakan pendekatan metode octave dan iso 27001:2005', *Seminar Nasional Telekomunikasi dan Informatika (SELISIK 2016)*, (Selisik), pp. 80–85.

Farvin, S. and Baharom, F. (2016) 'Computer Crimes From Islamic Perspective and the Role of Secure', (May).

Fleming, T. and Wilander, H. (2018) 'Network Intrusion and Detection : An evaluation of SNORT', *Linköping Univ., Linköping, Sweden, Tech. Rep.* Available at: http://www.diva-portal.org/smash/record.jsf?pid=diva2%3A1175693&dswid=-7800.

Hadiansyah chandra and Iskandar, I. (2017) 'Pembangunan Server Security Information Management Untuk Monitoring Keamanan Di Server Diskominfo Provinsi Jawa Barat', pp. 1–8.

Hidayat, R., Suyanto, M. and Sunyoto, A. (2018) 'Indeks Penilaian Keamanan Informasi Untuk Mengukur Kematangan Manajemen Keamanan Layanan TI', *Pengembangan Aplikasi Untuk Mendeteksi Pergerakan Sendi Pada Pasien Pasca Stroke Menggunakan Sensor Accelerometer Di Smartphone Android*, 3(1).

HM, J. (2011) *Sistem Tatakelola Teknologi Informasi*. Edited by Andi Offset. Yogyakarta.

ISO/IEC (2018) 'International Standard ISO / IEC Information technology — Security techniques — Information security management systems — Overview and', 2018, p. 38. doi: 10.1177/0011128708322943.

Lenawati, M., Winarno, W. W. and Amborowati, A. (2017) 'Tata Kelola Keamanan Informasi pada PDAM Menggunakan ISO/IEC 27001:2013 Dan COBIT 5', *Sentra Penelitian Engineering dan Edukasi*, 9(1), pp. 44–49. doi: 10.1007/978-981-10-2618-8_18.

Lizarti, N. and Agustin, W. (2015) 'Aplikasi Network Traffic Monitoring Menggunakan Simple Network Management Protocol (SNMP) pada Jaringan Virtual Private Network (VPN)', *SATIN - Sains dan Teknologi Informasi*, 1(1), p. 27. doi: 10.33372/stn.v1i1.17.

Loshin, P. (2003) 'User Datagram Protocol', *TCP/IP Clearly Explained*, pp. 341–349. doi: 10.1016/b978-155860782-8/50020-8.

Lu, H., Liang, B. and Taylor, M. (2010) 'A Comparative Analysis of Cybercrimes

and Governmental Law Enforcement in China and the United States', *Asian Journal of Criminology*, 5, pp. 123–135. doi: 10.1007/s11417-010-9092-5.

Menkominfo (2015) 'Peraturan Menteri Komunikasi Dan Informatika Nomor Tahun 2015', *Peraturan Menteri Komunikasi Dan Informatika Nomor Tahun 2015 Tentang Sistem Manajemen Pengamanan Informasi*, 53(9), pp. 1689–1699. doi: 10.1017/CBO9781107415324.004.

MikroTik (no date). Available at: https://id.wikipedia.org/wiki/MikroTik (Accessed: 4 December 2018).

Muhamad Husni Lafif (2007) 'TCP/IP'.

Muzakka, A. *et al.* (2019) 'Pemanfaatan Hasil Report Next-Generation Firewall Sebagai Using Next-Generation Firewall Report Result As A Security', 2(2), pp. 25–32.

Nabil Bawafie and Muslihudin (2013) 'Perancangan Sistem Monitoring Bandwidth', *Sarjana Teknik Informatika*, 1(1), pp. 241–247.

Nandhini, U., Nivetha, B. and Shobana, D. (2016) 'An Analysis of Linux Operating System', 3(1), pp. 32–35.

Network-Monitoring . Available at: https://www.helpsystems.com/resources/artices/top-benefits-network-mmonitoring.

Pramono, P. P., Fahrianto, F. and Sc, M. (2019) 'Pendeteksian Dini Tingkat Kemanan Informasi Berbasis Iso 27001 : 2013 Menggunakan Metode Ahp (Analytical Hierarchy Process)', 2(2), pp. 57–64.

Pratama, E. R., Suprapto and Perdanakusuma, A. R. (2018) 'Evaluasi Tata Kelola Sistem Keamanan Teknologi Informasi Menggunakan Indeks KAMI dan ISO 27001: Studi Kasus KOMINFO Provinsi Jawa Timur', *Jurnal Pengembangan Teknologi Informasi dan Ilmu Komputer*, 2(11), pp. 5911–5920.

Putra, M. Y. and Tjahjadi, D. (2018) 'Evaluasi Keamanan Informasi Pada Perguruan Tinggi Bina Insani Berdasarkan Indeks Keamanan Informasi SNI ISO/IEC 27001', *PIKSEL : Penelitian Ilmu Komputer Sistem Embedded and Logic*, 6(1), pp. 95–104. doi: 10.33558/piksel.v6i1.1404.

Riani, R. *et al.* (2018) 'Implementasi Monitoring Lalu Lintas Jaringan Dengan Ntop pada Jaringan Dual Stack Implementation of Network Traffic Monitoring With Ntop on DualStack Networks', *Techno.COM*, 17(4), pp. 424–432.

Rick B (2013) *One minute on the Internet: 640TB data transferred, 100k tweets, 204 million e-mails sent*. Available at: https://www.techspot.com/community/topics/one-minute-on-the-internet-640tb-data-transferred-100k-tweets-204-million-e-mails-sent.190833/ (Accessed: 6 November 2018).

Rosen, R. and Rosen, R. (2014) 'Internet Control Message Protocol (ICMP)', *Linux Kernel Networking*, pp. 37–61. doi: 10.1007/978-1-4302-6197-1_3.

Sakti P., E., Kusyanti, A. and Setyawan, R. A. (2014) 'Audit Dan Investigasi Sistem Keamanan Jaringan Komputer Di Lingkungan Kampus', *Jurnal Teknologi Informasi dan Ilmu Komputer*, 1(1), p. 14. doi: 10.25126/jtiik.20141199.

Siga, M., Susanto, T. D. and Hidayanto, B. C. (2014) 'Evaluasi Keamanan Informasi Menggunakan Indeks Keamanan Informasi Pada Kantor Wilayah Ditjen Perbendaharaan Negara Jawa Timur', *Seminar Nasional Sistem Informasi Indonesia*, (479), pp. 1–6.

Sugiantoro, B. (2017) 'Pengembangan Deteksi Penyusupan Menggunakan Multiagent', *Telematika*, 14(2), pp. 83–88. doi: 10.31315/telematika.v14i2.2095.

Sutara, B. (2018) 'Pengukuran Keamanan Informasi PDAM Titra Medal Menggunakan Indeks KAMI Untuk Analisis Tingkat Kematangan Keamanan Informasi', 17(2), pp. 34–41.

Tarigan, A. (2009) *Bikin Gateway Murah pakai MikroTik*. Jakarta: Gramedia.

Vianello, V. *et al.* (2013) 'A scalable SIEM correlation engine and its application to the olympic games it infrastructure', in *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 625–629. doi: 10.1109/ARES.2013.82.

Y. Sattarova FeruzaT.-H. Kim (2007) 'IT Security Review: Privacy, Protection,

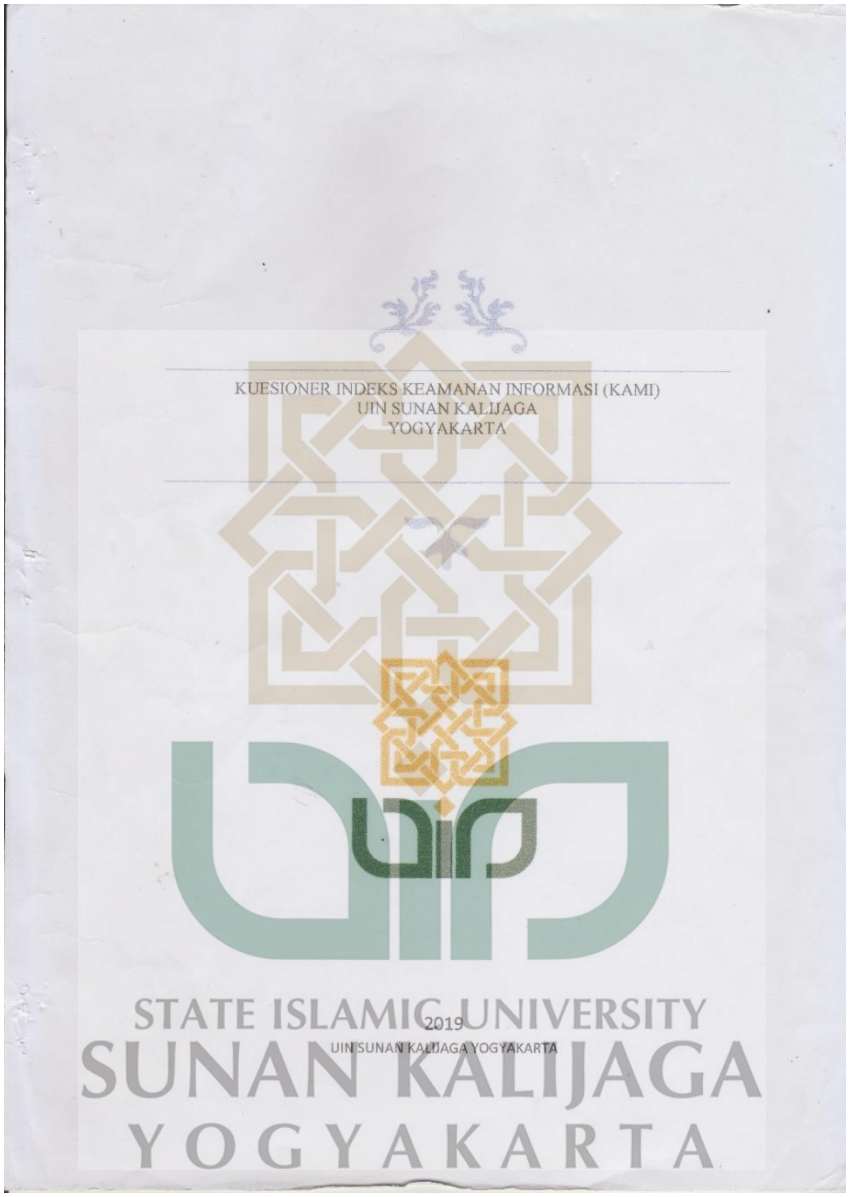
Access Control, Assurance and System Security'.

LAMPIRAN

1. Kuisioner *Pre-Assessment Indeks* KAMI UIN Sunan Kalijaga


KUESIONER INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

2019
UIN SUNAN KALIJAGA YOGYAKARTA


KUESIONER INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA
STATE ISLAMIC UNIVERSITY
2019
UIN SUNAN KALIJAGA YOGYAKARTA
SUNAN KALIJAGA
YOGYAKARTA

DATA PENGISI KUESIONER

Instansi : UIN Sunan Kalijaga

Nama : Hendra Hidayat, S.Kom

NIP : 19790506 200604 1 003

Jabatan : Analis Sistem Informasi

Nomor Kontak 081727474142

Email : -

Tanda Tangan dan Cap Instansi

Form Checklist

I. Aspek Sistem Elektronik ☑
II. Aspek Tata Kelola Keamanan Informasi ☑
III. Aspek Pengelolaan Risiko Keamanan Informasi ☑
IV. Aspek Kerangka Kerja Keamanan Informasi ☑
V. Aspek Pengelolaan Aset Informasi ☑
VI. Aspek Teknologi dan Keamanan Informasi ☑
VII. Aspek Suplemen ☑

KUISIONER ASPEK SISTEM ELEKTRONIK
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan dalam Instansi anda. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 5 = A
- 2 = B
- 1 = C

No	Karakteristik Instansi/Perusahaan	Status		
		A	B	C
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar		√	
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar			√
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus		√	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi		√	
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	√		
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data		√	

	pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi			
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa		✓	
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	✓		
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih		✓	
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)			✓
	Skor penetapan Aspek Sistem Elektronik		24	

KUISIONER ASPEK TATA KELOLA KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
2.1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?				√
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?			√	
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?			√	
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?			√	
2.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?		√		
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?			√	
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan			√	

	keahlian yang memadai sesuai persyaratan/standar yang berlaku?				
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?			✓	
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?			✓	
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?			✓	✓
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?			✓	
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?			✓	
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?			✓	
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*busmess continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?				✓
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?			✓	
2.16	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?				✓
2.17	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi			✓	

	tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?				
2.18	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?			✓	
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?			✓	
2.20	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?				✓
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?			✓	
2.22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?		✓	✓	
	Total Nilai Evaluasi Tata Kelola		46		

KUISIONER ASPEK PENGELOLAAN RISIKO KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Kajian Risiko Keamanan Informasi					
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			√	
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			√	
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?		√		
3.4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?		√		
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?			√	
3.6	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama penting dan proses kerja utama yang menggunakan aset tersebut?			√	
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			√	

3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?		✓			
3.9	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?		✓			
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓		
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?			✓		
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓		
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?		✓			
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?		✓			
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?		✓			
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?		✓			
	Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi		24			

KUISIONER ASPEK KERANGKA KERJA KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi					
4.1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?			√	
4.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?			√	
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?			√	
4.4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?		√		
4.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?			√	
4.6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?		√		

4.7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?		✓		
4.8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		✓		
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?		✓		
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?			✓	
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?			✓	
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?			✓	
4.13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?			✓	
4.14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?			✓	
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?			✓	
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?				✓
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?				✓

4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan)* dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?			✓	
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?			✓	
Pengelolaan Strategi dan Program Keamanan Informasi					
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?		✓		
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?			✓	
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?			✓	
4.23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?			✓	
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?				✓
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?				✓
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?				✓
4.27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?			✓	
4.28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah			✓	

	pembenahan yang diperlukan, telah diterapkan secara efektif?				
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?			✓	
	Total Nilai Evaluasi Kerangka Kerja		56		

KUISIONER ASPEK ENGELOLAAN ASET INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Pengelolaan Aset Informasi					
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)				√
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?				√
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?			√	√
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?			√	
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?			√	
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?				√
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?				√
5.8	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			√	
5.9	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda			√	

5.10	Tata tertib penggunaan komputer, email, internet dan intranet				✓
5.11	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI			✓	
5.12	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan			✓	
5.13	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi			✓	
5.14	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya				✓
5.15	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi				✓
5.16	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data			✓	
5.17	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya				✓
5.18	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi			✓	
5.19	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala				✓
5.20	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya			✓	
5.21	Proses pengecekan latar belakang SDM			✓	
5.22	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.		✓		
5.23	Prosedur penghancuran data/aset yang sudah tidak diperlukan		✓		
5.24	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya (*user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku			✓	
5.25	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.			✓	
5.26	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?				✓
5.27	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?			✓	
Pengamanan Fisik					
5.28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis				✓

	dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?				
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?				✓
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?				✓
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?				✓
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?			✓	
5.33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?			✓	
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?				✓
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?			✓	
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?			✓	
5.37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)				✓
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?				✓
	Total Nilai Evaluasi Pengelolaan Aset		91		

KUISIONER ASPEK TEKNOLOGI DAN KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Pengamanan Teknologi					
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?				√
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?				√
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?				√
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?			√	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?				√
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?				√
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?				√
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?				√
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?				√

6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?			✓	
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?			✓	
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?			✓	
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?			✓	
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?		✓		
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?			✓	
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?				✓
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?				✓
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?				✓
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?			✓	✓
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?				✓
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?				✓
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?				✓
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?				✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?			✓	
6.25	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi			✓	

	yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?				
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?			✓	
	Total Nilai Evaluasi Teknologi dan Keamanan Informasi	66			

KUISIONER ASPEK SUPLEMEN
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

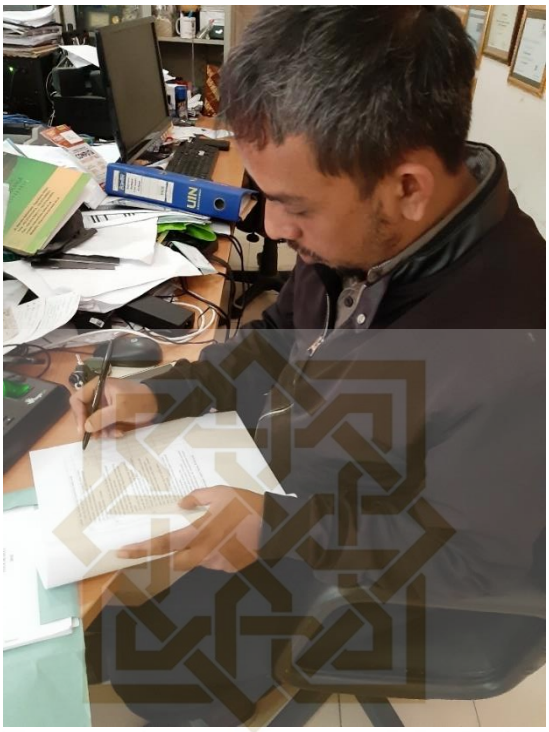
No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
7.1	**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**				
7.1.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**				
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?			√	
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?				√
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?				√
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?			√	
7.1.1.5	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?		√		
7.1.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?		√		
7.1.1.7	Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga?			√	

	Termasuk di dalamnya akses terhadap laporan audit internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?				
7.1.2	**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**				
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?			✓	
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?				✓
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?			✓	
7.1.3	**Pengelolaan Layanan dan Keamanan Pihak Ketiga**				
7.1.3.1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?			✓	
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?			✓	
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?			✓	
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?			✓	
7.1.3.5	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?			✓	
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?			✓	
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?			✓	
7.1.3.8	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?				✓

7.1.4	**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**					
7.1.4.1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?					✓
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?					✓
7.1.5	**Penanganan Aset**					
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset?				✓	
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?					✓
7.1.6	**Pengelolaan Insiden oleh Pihak Ketiga**					
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?					✓
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?					✓
7.1.7	**Rencana Kelangsungan Layanan Pihak Ketiga**					
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?					✓
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?					✓
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?					✓
7.2	**Pengamanan Layanan Infrastruktur Awan (Cloud Service)**					
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?		✓			
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?		✓			
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?		✓			

7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?		✓		
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?		✓		
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud*, termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?		✓		
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?		✓		
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?		✓		
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?		✓		
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud*, termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?		✓		
7.3	**Perlindungan Data Pribadi**				
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?			✓	
7.3.2	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?			✓	
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?			✓	
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?		✓		
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?		✓		
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?		✓		

7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?		✓		
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?		✓		
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?		✓		
7.3.10	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?		✓		
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?		✓		
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?		✓		
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?			✓	
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?			✓	
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?			✓	
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?		✓		



2. Langkah *installation* OSSIM

1. Edit /etc/apt/soutces.list dan tambahkan baris berikut pada debian-ossim:

[-- /etc/apt/sources.list –]
deb http://www.ossim.net/download/ debian/
deb http://ftp.debian.org/debian/ testing main
debhttp://secure-testing.debian.net/debian-secure-testing testing/security-updates\ main

2. Edit file /etc/apt/apt.conf dan tambahkan baris berikut pada konfigurasi *proxy server*:
[-- /etc/apt/apt.conf –]
Acquire::http::User::Pass "proxy:port"

3. *Update list* info paket pada debian:

apt-get update

4. *Install* OSSIM-mysql:
apt-get install ossim-mysql

5. *set password root* untuk *database* mysql:
mysqladmin –u root password your_secret_password

6. buat *database- database* berikut ini untuk kebutuhan OSSIM dan *dependency* nya :
mysql –u root –p
mysql> create database ossim;
mysql> create database ossim_acl;
mysql> create database snort;
mysql> create database phpgacl;
mysql> create database snort_log;
mysql> create database snort_archive;
mysql>exit;

7. *Load* tabel-tabel berikut kedalam *database OSSIM* dan *snort:*
zcat /usr/share.doc/ossim-mysql/contrib/create_mysql.gz \
/usr/share/doc/ossim-mysql/contrib/ossim_config.sql.gz \
mysql -u root ossim –p

8. #zcat /usr/share/doc/ossim-mysql/contrib/create_mysql.sql.gz \
/usr/share/doc/ossim-mysql/contrib/create_acid_tbls_mysql.sql.gz
\
| mysql –u root snort –p

9. Install ossim-server:
apt-get install ossim-server
Jalankan ‘dpkg-reconfigure ossim-server’ jika ingin menganti konfigurasi kembali ossim-server (nb : jangan mengedit manual file /etc/ossim/server/config.xml jika mengalami kesulitan)

10. install ossim-agent:
apt-get install ossim-agent
Jalankan ‘dpkg-reconfigure ossim-agent’ jika ingin mengkonfigurasi kembali ossim-agent (nb : jangan mengedit manual file /etc/ossim/server/config.xml jika mengalami kesulitan)

11. install phpgacl:
apt-get install phpgacl

12. install ossim-framework dan dependencynya. Disini saya akan menggunakan apache2 sebagai webserver:
apt-get install apache2
apt-get install ossim-framework
13. install ossim-utilities:
apt-get install ossim-utils
Jalankan 'dpkg-reconfigure ossim-framework' jika ingin mengkonfigurasi kembali ossim-framework (jangan mengedit manual file /etc/ossim/framework/ossim.conf jika mengalami kesulitan)

14. Install nessus server dan nessus client:
apt-get install nessusd nessus

15. Install snort-mysql:
apt-get install snort-mysql
Edit manual file konfigurasi /etc/snort/snort.conf
[-- /etc/snort/snort.conf --]
Var HOME_NET [192.168.0.13/16] //ganti dengan network anda
Var EXTERNAL_NET!$HOME_NET
Tambahkan baris berikut di akhir baris, sesuaikan dengan database snort: output database: alert, mysql, user=root password=rizki dbname=snort host=yourdbhost sensor_name=your_sensor_ip logfile=alert

16. update rule snort langsung ke website dengan menggunakan wget, konfigure dulu proxy untuk wget(/etc/wgetrc), edit option http_proxy and ftp_proxy:
[-- /etc/wgetrc --]

17. install ntop dan dependencynya:
#apt-get install librrd0 ntop
Jika tidak ada library librrd0, gantikan dengan librrd versi yang lain.

18. set password untuk user admin yang menjalankan Ntop:
ntop –u ntop
>> please enter the password for the admin user:

Jalankan service Ntop:
/etc/init.d/ntop start
Cek apakah port 3000 untuk ntop sudah listen, kalo sudah berarti Ntop sudah jalan:
netstat –na | grep 3000

19. cek dengan browser dengan alamat http://yourhost:3000/ untuk mengecek Ntop

20. install plugin-plugin yang lain dari OSSIM:
#apt-get install nagios-mysql p0f arpwatch pads tcptrack

21. matikan proses start otomatis dari service arpwatch, biatkan ossim-agent yang menjalankannya:
update-rc.d –f arpwatch remove

22. review kembali konfigurasi di /etc/ossim/framework/ossim.conf, /etc/ossim/agent/config.xml, dan /etc/ossim/server/config.xml

23. gunakan browser dan alamatkan ke http://yourhost/ossim. Seharusnya menu phpgacl muncul. Klik pada menu yang ada linknya untuk setup phpgacl.

24. klik dibaris paling bawah yang ada link untuk melanjtukan setup. Maka konfigurasi ossim akan disesuaikan dengan phpgacl. Phpgacl di sini berfungsi sebagai Acess Control List (ACL) dari aplikasi OSSIM.

25. klik menu back di baris paling bawah, jika instalasi benar maka akan langsung muncul halaman autentikasi dari OSSIM. User dan password secara default adalah admin:admin, dan ini harus diganti begitu masuk ke sistem OSSIM.

26. Last, reboot mesin dan cek bahwa semua service di /etc/init.d/* (terutama ossim-server, ossim-framework, ossim-agent, apache2, ntop, snort,nessusd, pads, p0f, dan tcptrack, sudah berjalan dengan baik. Jika ada yang belum jalan, gunakan script "/etc/init.d/nama_aplikasi start" untuk menjalankan servicenya.

3. Kuisioner *Post-Assessment Indeks* KAMI UIN Sunan Kalijaga

KUESIONER INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

2019
UIN SUNAN KALIJAGA YOGYAKARTA

DATA PENGISI KUESIONER

Instansi	: UIN Sunan Kalijaga
Nama	: Hendra Hidayat, S.Kom.
NIP	: 1979 0506 200604 1 003
Jabatan	: Analisis Sistem Informasi
Nomor Kontak	: 08 17 27 4142
Email	: -

Tanda tangan dan Cap Instansi

Form Checklist

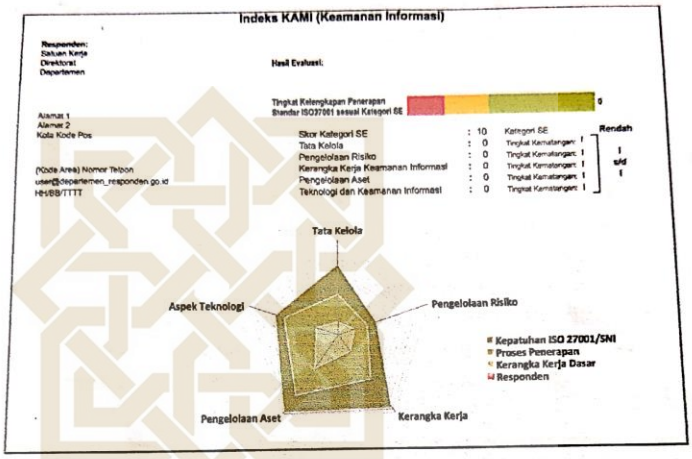
I. **Aspek Sistem Elektronik** ☑
II. **Aspek Tata Kelola Keamanan Informasi** ☑
III. **Aspek Pengelolaan Risiko Keamanan Informasi** ☑
IV. **Aspek Kerangka Kerja Keamanan Informasi** ☑
V. **Aspek Pengelolaan Aset Informasi** ☑
VI. **Aspek Teknologi dan Keamanan Informasi** ☑
VII. **Aspek Suplemen** ☑

Indeks Keamanan Informasi (Indeks KAMI)

Versi 4.0, Maret 2019

INDEKS KEAMANAN INFORMASI

Mengenai Indeks KAMI



Indeks KAMI adalah alat evaluasi untuk menganalisa tingkat kesiapan pengamanan informasi di suatu organisasi. Alat evaluasi ini tidak ditujukan untuk menganalisa kelayakan atau efektifitas bentuk pengamanan yang ada, melainkan sebagai perangkat untuk memberikan gambaran kondisi kesiapan (kelengkapan dan kematangan) kerangka kerja keamanan informasi kepada pimpinan Instansi/Perusahaan. Evaluasi dilakukan terhadap berbagai area yang menjadi target penerapan keamanan informasi dengan ruang lingkup pembahasan yang juga memenuhi semua aspek keamanan yang didefinisikan oleh standar ISO/IEC 27001:2013.

Bentuk evaluasi yang diterapkan dalam indeks KAMI dirancang untuk dapat digunakan oleh suatu organisasi dari berbagai tingkatan, ukuran, maupun tingkat kepentingan penggunaan TIK dalam mendukung terlaksananya proses yang ada. Data yang digunakan dalam evaluasi ini nantinya akan memberikan *snapshot* indeks kesiapan - dari aspek kelengkapan maupun kematangan - kerangka kerja keamanan informasi yang diterapkan dan dapat digunakan sebagai pembanding dalam rangka menyusun langkah perbaikan dan penetapan prioritasnya.

Alat evaluasi ini kemudian bisa digunakan secara berkala untuk mendapatkan gambaran perubahan kondisi keamanan informasi sebagai hasil dari program kerja yang dijalankan, sekaligus sebagai sarana untuk menyampaikan peningkatan kesiapan kepada pihak yang terkait (*stakeholders*).

Khusus untuk Instansi Pemerintah, penggunaan dan publikasi hasil evaluasi Indeks KAMI merupakan bentuk tanggungjawab penggunaan dana publik sekaligus menjadi sarana untuk meningkatkan kesadaran mengenai kebutuhan keamanan informasi. Pertukaran informasi dan diskusi dengan Instansi pemerintah lainnya sebagai bagian dari penggunaan alat evaluasi Indeks KAMI ini juga menciptakan alur komunikasi antar pengelola keamanan informasi di sektor pemerintah sehingga semua pihak dapat mengambil manfaat dari lesson learned yang sudah dilalui.

Petunjuk Penggunaan Alat Evaluasi Indeks Keamanan Informasi (Indeks KAMI)

Alat evaluasi Indeks KAMI ini dapat digunakan oleh organisasi dengan skala nasional, maupun yang berukuran kecil. Penggunaan di Instansi pemerintah dapat dilakukan di tingkat pusat maupun satuan kerja yang ada di tingkatan Direktorat Jenderal, Badan, Pusat atau Direktorat untuk mendapatkan gambaran mengenai kematangan program kerja keamanan informasi yang dijalankannya. Evaluasi ini dianjurkan untuk dilakukan oleh pejabat yang secara langsung bertanggungjawab dan berwenang untuk mengelola keamanan informasi di seluruh cakupan instansinya.

Proses evaluasi dilakukan melalui sejumlah pertanyaan di masing-masing area di bawah ini:

- Sistem Elektronik yang digunakan Instansi
-Tata Kelola Keamanan Informasi
- Pengelolaan Risiko Keamanan Informasi
- Kerangka Kerja Keamanan Informasi
- Pengelolaan Aset Informasi, dan
- Teknologi dan Keamanan Informasi
- Suplemen: Area evaluasi untuk aspek Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan, Pengamanan Layanan Infrastruktur Awan (*Cloud Service*) dan Perlindungan Data Pribadi.

Pertanyaan yang ada belum tentu dapat dijawab semuanya, akan tetapi yang harus diperhatikan adalah jawaban yang diberikan harus merefleksikan kondisi penerapan keamanan informasi SESUNGGUHNYA. Alat evaluasi ini hanya akan memberikan nilai tambah bagi semua pihak apabila pengisiannya menggunakan azas keterbukaan dan kejujuran.Sebelum mulai menjawab pertanyaan terkait kesiapan pengamanan informasi, responden diminta untuk mendefinisikan Kategori Sistem Elektronik di Instansinya. Definisi ini bisa dijabarkan untuk tingkat Satuan Kerja baik di tingkat Kementerian/Lembaga, ataupun untuk satuan kerja yang lebih kecil, sampai ke Unit Eselon III. Responden juga diminta untuk mendeskripsikan infrastruktur TIK yang ada dalam satuan kerjanya secara singkat. Tujuan dari proses ini adalah untuk mengelompokkan Sistem Elektronik yang digunakan instansi ke "tingkat" tertentu: Rendah, Tinggi dan Strategis. Dengan pengelompokan ini nantinya bisa dilakukan pemetaan terhadap instansi yang mempunyai karakteristik Sistem Elektronik yang sama.Pertanyaan dikelompokkan untuk 2 keperluan. Pertama, pertanyaan dikategorikan berdasarkan tingkat kesiapan penerapan pengamanan sesuai dengan **kelengkapan** kontrol yang diminta oleh standar ISO/IEC 27001:2013. Dalam pengelompokan ini responden diminta untuk memberi tanggapan mulai dari area yang terkait dengan bentuk kerangka kerja dasar keamanan informasi (pertanyaan diberi label "1"), efektifitas dan konsistensi penerapannya (label "2"), sampai dengan kemampuan untuk selalu meningkatkan kinerja keamanan informasi (label "3"). Tingkat terakhir ini sesuai dengan kesiapan minimum yang diprasyaratkan oleh proses sertifikasi standar ISO/IEC 27001:2013. Setiap jawaban diberikan skor yang nantinya dikonsolidasi untuk menghasilkan angka indeks sekaligus digunakan untuk menampilkan hasil evaluasi dalam *dashboard* di akhir proses ini.Skor yang diberikan untuk jawaban pertanyaan sesuai tingkat kematangannya mengacu kepada:

	Kategori Pengamanan		
Status Pengamanan	1	2	3
Tidak Dilakukan	0	0	0
Dalam Perencanaan	1	2	3
Dalam Penerapan atau Diterapkan Sebagian	2	4	6
Diterapkan secara Menyeluruh	3	6	9

(Catatan: untuk keseluruhan area pengamanan, pengisian pertanyaan dengan label "3" hanya dapat memberikan hasil apabila semua pertanyaan terkait dengan label "1" dan "2" sudah diisi dengan status minimal "Diterapkan Sebagian")

Hasil dari penjumlahan skor untuk masing-masing area ditampilkan dalam diagram radar dengan latar belakang area untuk tingkat maksimal kematangan 1 s/d 3. Dalam diagram ini bisa dilihat perbandingan antara kondisi kesiapan sebagai hasil dari proses evaluasi dengan acuan tingkat kematangan yang ada.

Dengan membaca diagram ini, pimpinan instansi dapat melihat kebutuhan pembenahan yang diperlukan dan korelasi antara berbagai area penerapan keamanan informasi. Adapun korelasi antara Kategori Sistem Elektronik dengan Status Kesiapan didefinisikan melalui tabel berikut:

KATEGORI SISTEM ELEKTRONIK				
Rendah		Skor Akhir		Status Kesiapan
10	15	0	174	Tidak Layak
		175	312	Pemenuhan Kerangka Kerja Dasar
		313	535	Cukup Baik
		536	645	Baik
Tinggi		Skor Akhir		Status Kesiapan
16	34	0	272	Tidak Layak
		273	455	Pemenuhan Kerangka Kerja Dasar
		456	583	Cukup Baik
		584	645	Baik
Strategis		Skor Akhir		Status Kesiapan
35	50	0	333	Tidak Layak
		334	535	Pemenuhan Kerangka Kerja Dasar
		536	609	Cukup Baik
		610	645	Baik

Pengelompokan kedua dilakukan berdasarkan tingkat **kematangan** penerapan pengamanan dengan kategorisasi yang mengacu kepada tingkatan kematangan yang digunakan oleh kerangka kerja COBIT atau CMMI. Tingkat kematangan ini nantinya akan digunakan sebagai alat untuk melaporkan pemetaan dan pemeringkatan kesiapan keamanan informasi di Kementerian/Lembaga

.

Untuk keperluan Indeks KAMI, tingkat kematangan tersebut didefinisikan sebagai:

-Tingkat I - Kondisi Awal
-Tingkat II - Penerapan Kerangka Kerja Dasar
-Tingkat III - Terdefinisi dan Konsisten
-Tingkat IV - Terkelola dan Terukur
-Tingkat V - Optimal

Untuk membantu memberikan uraian yang lebih detil, tingkatan ini ditambah dengan tingkatan antara - I+, II+, III+, dan IV+, sehingga total terdapat 9 tingkatan kematangan. Sebagai awal, semua responden akan diberikan kategori kematangan

Tingkat I. Sebagai padanan terhadap standar ISO/IEC 27001:2013, tingkat kematangan yang diharapkan untuk ambang batas minimum kesiapan sertifikasi adalah Tingkat III+.

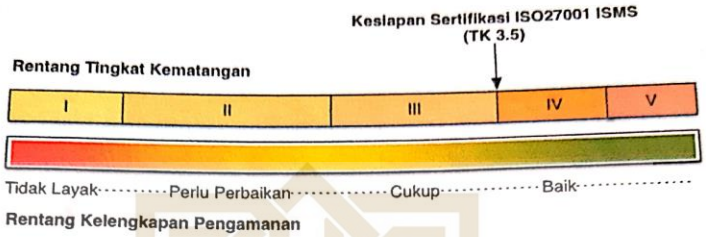
Ilustrasi di bawah menunjukkan label pengelompokan kematangan (kolom di sebelah kanan nomor urut) dan kelengkapan (kolom di sebelah kiri pertanyaan).

Bagian II: Tata Kelola Keamanan Informasi

Bagian ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/fungsi, tugas dan tanggung jawab pengelola keamanan informasi.

[Penilaian] Tidak Dilakukan; Dalam Perencanaan; Dalam Penerapan atau Diterapkan Sebagian; Diterapkan Secara Menyeluruh					Status
#			Fungsi/Instansi Keamanan Informasi		
2.1	II	1	Apakah pimpinan instansi anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?		Tidak Dilakukan
2.2	II	1	Apakah Instansi anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?		✓ Tidak Dilakukan Dalam Perencanaan Dalam Penerapan / Diterapkan Sebagian Diterapkan Secara Menyeluruh
2.3	II	1	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?		
2.4	II	1	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?		Tidak Dilakukan
2.5	II	1	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?		Tidak Dilakukan
2.6	II	1	Apakah Instansi anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?		Tidak Dilakukan
2.7	II	1	Apakah semua pelaksana pengamanan informasi di instansi anda memiliki kompetensi dan keahlian yang memadai sesuai persyaratan/standar yang berlaku?		Tidak Dilakukan
2.8	II	1	Apakah instansi anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?		Tidak Dilakukan
2.9	II	2	Apakah Instansi anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?		Tidak Dilakukan
2.10	II	2	Apakah instansi anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?		Tidak Dilakukan

Kedua pengelompokan ini dapat dipetakan (lihat gambar di bawah) untuk memberikan dua sudut pandang yang berbeda: tingkat kelengkapan pengamanan dan tingkat kematangan pengamanan. Instansi responden dapat menggunakan metrik ini sebagai target program keamanan informasi.



Indeks KAMI sebaiknya digunakan 2X dalam setahun sebagai alat untuk melakukan tinjauan ulang kesiapan keamanan informasi sekaligus untuk mengukur keberhasilan inisiatif perbaikan yang diterapkan, dengan pencapaian tingkat kelengkapan atau kematangan tertentu.

Suplemen

Perkembangan teknologi yang pesat dan pola bisnis yang dinamis menyebabkan munculnya risiko keamanan informasi baru. Keterlibatan pihak ketiga dalam rantai pasok (supply chain) layanan suatu instansi/perusahaan menimbulkan risiko terkait keberadaan/keterlibatan pihak eksternal tersebut. Layanan berbasis infrastruktur awan (Cloud) memberikan peluang efisiensi dan peningkatan kinerja yang sangat signifikan bagi instansi/perusahaan, akan tetapi risiko terkait data yang berada pada pengendalian pihak ketiga (penyelenggara layanan) perlu dimitgasi. Sedangkan disahkannya peraturan terkait perlindungan data pribadi oleh banyak negara memerlukan kerangka kerja yang secara spesifik membahas bagaimana data pribadi yang ada/digunakan dalam instansi/perusahaan diamankan sesuai dengan persyaratan hukum.

Untuk menilai kesiapan instansi/perusahaan dalam mengelola risiko di 3 (tiga) area baru ini, pada revisi 4.0 disediakan modul suplemen yang membahas aspek kesiapan pengamanan untuk ketiga aspek tersebut.

Penggunaan modul suplemen untuk evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi digunakan sesuai konteks atau cakupan yang ada. Responden hanya perlu menjawab area evaluasi yang berlaku.

Butir-butir evaluasi kesiapan pengamanan yang disusun untuk setiap area merupakan persyaratan dasar yang bagi instansi/perusahaan yang terpapar risiko terkait ketiga area tersebut.

Hasil penilaian evaluasi kesiapan Pengamanan Keterlibatan Pihak Ketiga, Pengamanan Layanan Infrastrukutur Awan dan Perlindungan Data Pribadi disampaikan dalam bentuk persentase (%) dengan obyektif/sasaran pencapaian maksimal.

KUISIONER ASPEK SISTEM ELEKTRONIK
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi tingkat atau kategori sistem elektronik yang digunakan dalam Instansi anda. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 5 = A
- 2 = B
- 1 = C

No	Karakteristik Instansi/Perusahaan	Status		
		A	B	C
1.1	Nilai investasi sistem elektronik yang terpasang [A] Lebih dari Rp.30 Miliar [B] Lebih dari Rp.3 Miliar s/d Rp.30 Miliar [C] Kurang dari Rp.3 Miliar		√	
1.2	Total anggaran operasional tahunan yang dialokasikan untuk pengelolaan Sistem Elektronik [A] Lebih dari Rp.10 Miliar [B] Lebih dari Rp.1 Miliar s/d Rp.10 Miliar [C] Kurang dari Rp.1 Miliar			√
1.3	Memiliki kewajiban kepatuhan terhadap Peraturan atau Standar tertentu [A] Peraturan atau Standar nasional dan internasional [B] Peraturan atau Standar nasional [C] Tidak ada Peraturan khusus		√	
1.4	Menggunakan teknik kriptografi khusus untuk keamanan informasi dalam Sistem Elektronik [A] Teknik kriptografi khusus yang disertifikasi oleh Negara [B] Teknik kriptografi sesuai standar industri, tersedia secara publik atau dikembangkan sendiri [C] Tidak ada penggunaan teknik kriptografi		√	
1.5	Jumlah pengguna Sistem Elektronik [A] Lebih dari 5.000 pengguna [B] 1.000 sampai dengan 5.000 pengguna [C] Kurang dari 1.000 pengguna	√		
1.6	Data pribadi yang dikelola Sistem Elektronik [A] Data pribadi yang memiliki hubungan dengan Data Pribadi lainnya [B] Data pribadi yang bersifat individu dan/atau data		√	

	pribadi yang terkait dengan kepemilikan badan usaha [C] Tidak ada data pribadi			
1.7	Tingkat klasifikasi/kekritisan Data yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Sangat Rahasia [B] Rahasia dan/atau Terbatas [C] Biasa		✓	
1.8	Tingkat kekritisan proses yang ada dalam Sistem Elektronik, relatif terhadap ancaman upaya penyerangan atau penerobosan keamanan informasi [A] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak langsung pada layanan publik [B] Proses yang berisiko mengganggu hajat hidup orang banyak dan memberi dampak tidak langsung [C] Proses yang hanya berdampak pada bisnis perusahaan	✓		
1.9	Dampak dari kegagalan Sistem Elektronik [A] Tidak tersedianya layanan publik berskala nasional atau membahayakan pertahanan keamanan negara [B] Tidak tersedianya layanan publik dalam 1 propinsi atau lebih [C] Tidak tersedianya layanan publik dalam 1 kabupaten/kota atau lebih		✓	
1.10	Potensi kerugian atau dampak negatif dari insiden ditembusnya keamanan informasi Sistem Elektronik (sabotase, terorisme) [A] Menimbulkan korban jiwa [B] Terbatas pada kerugian finansial [C] Mengakibatkan gangguan operasional sementara (tidak membahayakan dan mengakibatkan kerugian finansial)			✓
	Skor penetapan Aspek Sistem Elektronik		24	

KUISIONER ASPEK TATA KELOLA KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kesiapan bentuk tata kelola keamanan informasi beserta instansi/perusahaan/fungsi, tugas dan tanggung jawab pengelola keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
2.1	Apakah pimpinan instansi/perusahaan anda secara prinsip dan resmi bertanggungjawab terhadap pelaksanaan program keamanan informasi (misal yang tercantum dalam ITSP), termasuk penetapan kebijakan terkait?				√
2.2	Apakah instansi/perusahaan anda memiliki fungsi atau bagian yang secara spesifik mempunyai tugas dan tanggungjawab mengelola keamanan informasi dan menjaga kepatuhannya?			√	
2.3	Apakah pejabat/petugas pelaksana pengamanan informasi mempunyai wewenang yang sesuai untuk menerapkan dan menjamin kepatuhan program keamanan informasi?				√
2.4	Apakah penanggungjawab pelaksanaan pengamanan informasi diberikan alokasi sumber daya yang sesuai untuk mengelola dan menjamin kepatuhan program keamanan informasi?				√
2.5	Apakah peran pelaksana pengamanan informasi yang mencakup semua keperluan dipetakan dengan lengkap, termasuk kebutuhan audit internal dan persyaratan segregasi kewenangan?			√	
2.6	Apakah instansi/perusahaan anda sudah mendefinisikan persyaratan/standar kompetensi dan keahlian pelaksana pengelolaan keamanan informasi?				√
2.7	Apakah semua pelaksana pengamanan informasi di instansi/perusahaan anda memiliki kompetensi dan				√

	keahlian yang memadai sesuai persyaratan/standar yang berlaku?				
2.8	Apakah instansi/perusahaan anda sudah menerapkan program sosialisasi dan peningkatan pemahaman untuk keamanan informasi, termasuk kepentingan kepatuhannya bagi semua pihak yang terkait?				✓
2.9	Apakah instansi/perusahaan anda menerapkan program peningkatan kompetensi dan keahlian untuk pejabat dan petugas pelaksana pengelolaan keamanan informasi?				✓
2.10	Apakah instansi/perusahaan anda sudah mengintegrasikan keperluan/persyaratan keamanan informasi dalam proses kerja yang ada?				✓
2.11	Apakah instansi/perusahaan anda sudah mengidentifikasikan data pribadi yang digunakan dalam proses kerja dan menerapkan pengamanan sesuai dengan peraturan perundangan yang berlaku?			✓	
2.12	Apakah tanggungjawab pengelolaan keamanan informasi mencakup koordinasi dengan pihak pengelola/pengguna aset informasi internal dan eksternal maupun pihak lain yang berkepentingan, untuk mengidentifikasikan persyaratan/kebutuhan pengamanan (misal: pertukaran informasi atau kerjasama yang melibatkan informasi penting) dan menyelesaikan permasalahan yang ada?			✓	
2.13	Apakah pengelola keamanan informasi secara proaktif berkoordinasi dengan satker terkait (SDM, Legal/Hukum, Umum, Keuangan dll) dan pihak eksternal yang berkepentingan (misal: regulator, aparat keamanan) untuk menerapkan dan menjamin kepatuhan pengamanan informasi terkait proses kerja yang melibatkan berbagai pihak?			✓	
2.14	Apakah tanggungjawab untuk memutuskan, merancang, melaksanakan dan mengelola langkah kelangsungan layanan TIK (*business continuity* dan *disaster recovery plans*) sudah didefinisikan dan dialokasikan?				✓
2.15	Apakah penanggungjawab pengelolaan keamanan informasi melaporkan kondisi, kinerja/efektifitas dan kepatuhan program keamanan informasi kepada pimpinan instansi/perusahaan secara rutin dan resmi?			✓	
2.16	Apakah kondisi dan permasalahan keamanan informasi di instansi/perusahaan anda menjadi konsiderans atau bagian dari proses pengambilan keputusan strategis di instansi/perusahaan anda?				✓
2.17	Apakah pimpinan satuan kerja di instansi/perusahaan anda menerapkan program khusus untuk mematuhi			✓	

	tujuan dan sasaran kepatuhan pengamanan informasi, khususnya yang mencakup aset informasi yang menjadi tanggungjawabnya?				
2.18	Apakah instansi/perusahaan anda sudah mendefinisikan metrik, paramater dan proses pengukuran kinerja pengelolaan keamanan informasi yang mencakup mekanisme, waktu pengukuran, pelaksananya, pemantauannya dan eskalasi pelaporannya?				✓
2.19	Apakah instansi/perusahaan anda sudah menerapkan program penilaian kinerja pengelolaan keamanan informasi bagi individu (pejabat & petugas) pelaksananya?				✓
2.20	Apakah instansi/perusahaan anda sudah menerapkan target dan sasaran pengelolaan keamanan informasi untuk berbagai area yang relevan, mengevaluasi pencapaiannya secara rutin, menerapkan langkah perbaikan untuk mencapai sasaran yang ada, termasuk pelaporan statusnya kepada pimpinan instansi/perusahaan?				✓
2.21	Apakah instansi/perusahaan anda sudah mengidentifikasi legislasi, perangkat hukum dan standar lainnya terkait keamanan informasi yang harus dipatuhi dan menganalisa tingkat kepatuhannya?			✓	
2.22	Apakah instansi/perusahaan anda sudah mendefinisikan kebijakan dan langkah penanggulangan insiden keamanan informasi yang menyangkut pelanggaran hukum (pidana dan perdata)?		✓		
	Total Nilai Evaluasi Tata Kelola		51		

KUISIONER ASPEK PENGELOLAAN RISIKO KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kesiapan penerapan pengelolaan risiko keamanan informasi sebagai dasar penerapan strategi keamanan informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Kajian Risiko Keamanan Informasi					
3.1	Apakah instansi/perusahaan anda mempunyai program kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?			√	
3.2	Apakah instansi/perusahaan anda sudah menetapkan penanggung jawab manajemen risiko dan eskalasi pelaporan status pengelolaan risiko keamanan informasi sampai ke tingkat pimpinan?			√	
3.3	Apakah instansi/perusahaan anda mempunyai kerangka kerja pengelolaan risiko keamanan informasi yang terdokumentasi dan secara resmi digunakan?		√		
3.4	Apakah kerangka kerja pengelolaan risiko ini mencakup definisi dan hubungan tingkat klasifikasi aset informasi, tingkat ancaman, kemungkinan terjadinya ancaman tersebut dan dampak kerugian terhadap instansi/perusahaan anda?		√		
3.5	Apakah instansi/perusahaan anda sudah menetapkan ambang batas tingkat risiko yang dapat diterima?			√	
3.6	Apakah instansi/perusahaan anda sudah mendefinisikan kepemilikan dan pihak pengelola *(custodian)* aset informasi yang ada, termasuk aset utama/penting dan proses kerja utama yang menggunakan aset tersebut?			√	
3.7	Apakah ancaman dan kelemahan yang terkait dengan aset informasi, terutama untuk setiap aset utama sudah teridentifikasi?			√	

3.8	Apakah dampak kerugian yang terkait dengan hilangnya/terganggunya fungsi aset utama sudah ditetapkan sesuai dengan definisi yang ada?		✓		
3.9	Apakah instansi/perusahaan anda sudah menjalankan inisiatif analisa/kajian risiko keamanan informasi secara terstruktur terhadap aset informasi yang ada (untuk nantinya digunakan dalam mengidentifikasi langkah mitigasi atau penanggulangan yang menjadi bagian dari program pengelolaan keamanan informasi)?		✓		
3.10	Apakah instansi/perusahaan anda sudah menyusun langkah mitigasi dan penanggulangan risiko yang ada?			✓	
3.11	Apakah langkah mitigasi risiko disusun sesuai tingkat prioritas dengan target penyelesaiannya dan penanggungjawabnya, dengan memastikan efektifitas penggunaan sumber daya yang dapat menurunkan tingkat risiko ke ambang batas yang bisa diterima dengan meminimalisir dampak terhadap operasional layanan TIK?			✓	
3.12	Apakah status penyelesaian langkah mitigasi risiko dipantau secara berkala, untuk memastikan penyelesaian atau kemajuan kerjanya?			✓	
3.13	Apakah penyelesaian langkah mitigasi yang sudah diterapkan dievaluasi, melalui proses yang obyektif/terukur untuk memastikan konsistensi dan efektifitasnya?		✓		
3.14	Apakah profil risiko berikut bentuk mitigasinya secara berkala dikaji ulang untuk memastikan akurasi dan validitasnya, termasuk merevisi profil terebut apabila ada perubahan kondisi yang signifikan atau keperluan penerapan bentuk pengamanan baru?		✓		
3.15	Apakah kerangka kerja pengelolaan risiko secara berkala dikaji untuk memastikan/meningkatkan efektifitasnya?		✓		
3.16	Apakah pengelolaan risiko menjadi bagian dari kriteria proses penilaian obyektif kinerja efektifitas pengamanan?		✓		
	Total Nilai Evaluasi Pengelolaan Risiko Keamanan Informasi	24			

KUISIONER ASPEK KERANGKA KERJA KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kelengkapan dan kesiapan kerangka kerja (kebijakan & prosedur) pengelolaan keamanan informasi dan strategi penerapannya. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Penyusunan dan Pengelolaan Kebijakan & Prosedur Keamanan Informasi					
4.1	Apakah kebijakan dan prosedur maupun dokumen lainnya yang diperlukan terkait keamanan informasi sudah disusun dan dituliskan dengan jelas, dengan mencantumkan peran dan tanggung jawab pihak-pihak yang diberikan wewenang untuk menerapkannya?			✓	
4.2	Apakah kebijakan keamanan informasi sudah ditetapkan secara formal, dipublikasikan kepada semua staf/karyawan termasuk pihak terkait dan dengan mudah diakses oleh pihak yang membutuhkannya?			✓	
4.3	Apakah tersedia mekanisme untuk mengelola dokumen kebijakan dan prosedur keamanan informasi, termasuk penggunaan daftar induk, distribusi, penarikan dari peredaran dan penyimpanannya?			✓	
4.4	Apakah tersedia proses (mencakup pelaksana, mekanisme, jadwal, materi, dan sasarannya) untuk mengkomunikasikan kebijakan keamanan informasi (dan perubahannya) kepada semua pihak terkait, termasuk pihak ketiga?		✓		
4.5	Apakah keseluruhan kebijakan dan prosedur keamanan informasi yang ada merefleksikan kebutuhan mitigasi dari hasil kajian risiko keamanan informasi, maupun sasaran/obyektif tertentu yang ditetapkan oleh pimpinan instansi/perusahaan?			✓	
4.6	Apakah tersedia proses untuk mengidentifikasi kondisi yang membahayakan keamanan infomasi dan menetapkannya sebagai insiden keamanan informasi untuk ditindak lanjuti sesuai prosedur yang diberlakukan?		✓		

4.7	Apakah aspek keamanan informasi yang mencakup pelaporan insiden, menjaga kerahasiaan, HAKI, tata tertib penggunaan dan pengamanan aset maupun layanan TIK tercantum dalam kontrak dengan pihak ketiga?		✓			
4.8	Apakah konsekwensi dari pelanggaran kebijakan keamanan informasi sudah didefinisikan, dikomunikasikan dan ditegakkan?		✓			
4.9	Apakah tersedia prosedur resmi untuk mengelola suatu pengecualian terhadap penerapan keamanan informasi, termasuk proses untuk menindak lanjuti konsekwensi dari kondisi ini?		✓			
4.10	Apakah organisasi anda sudah menerapkan kebijakan dan prosedur operasional untuk mengelola implementasi *security patch*, alokasi tanggung jawab untuk memonitor adanya rilis *security patch* baru, memastikan pemasangannya dan melaporkannya?			✓		
4.11	Apakah organisasi anda sudah membahas aspek keamanan informasi dalam manajemen proyek yang terkait dengan ruang lingkup?			✓		
4.12	Apakah organisasi anda sudah menerapkan proses untuk mengevaluasi risiko terkait rencana pembelian (atau implementasi) sistem baru dan menanggulangi permasalahan yang muncul?			✓		
4.13	Apakah organisasi anda sudah menerapkan proses pengembangan sistem yang aman *(Secure SDLC)* dengan menggunakan prinsip atau metode sesuai standar platform teknologi yang digunakan?			✓		
4.14	Apabila penerapan suatu sistem mengakibatkan timbulnya risiko baru atau terjadinya ketidakpatuhan terhadap kebijakan yang ada, apakah ada proses untuk menanggulangi hal ini, termasuk penerapan pengamanan baru (*compensating control*) dan jadwal penyelesaiannya?			✓		
4.15	Apakah tersedia kerangka kerja pengelolaan perencanaan kelangsungan layanan TIK (*business continuity planning*) yang mendefinisikan persyaratan/konsiderans keamanan informasi, termasuk penjadwalan uji cobanya?			✓		
4.16	Apakah perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah mendefinisikan komposisi, peran, wewenang dan tanggungjawab tim yang ditunjuk?			✓		
4.17	Apakah uji coba perencanaan pemulihan bencana terhadap layanan TIK (*disaster recovery plan*) sudah dilakukan sesuai jadwal?				✓	

4.18	Apakah hasil dari perencanaan pemulihan bencana terhadap layanan TIK *(disaster recovery plan)* dievaluasi untuk menerapkan langkah perbaikan atau pembenahan yang diperlukan - misal, apabila hasil uji coba menunjukkan bahwa proses pemulihan tidak bisa (gagal) memenuhi persyaratan yang ada?			✓	
4.19	Apakah seluruh kebijakan dan prosedur keamanan informasi dievaluasi kelayakannya secara berkala?			✓	
Pengelolaan Strategi dan Program Keamanan Informasi					
4.20	Apakah organisasi anda mempunyai strategi penerapan keamanan informasi sesuai hasil analisa risiko yang penerapannya dilakukan sebagai bagian dari rencana kerja organisasi?		✓		
4.21	Apakah organisasi anda mempunyai strategi penggunaan teknologi keamanan informasi yang penerapan dan pemutakhirannya disesuaikan dengan kebutuhan dan perubahan profil risiko?			✓	
4.22	Apakah strategi penerapan keamanan informasi direalisasikan sebagai bagian dari pelaksanaan program kerja organisasi anda?			✓	
4.23	Apakah organisasi anda memiliki dan melaksanakan program audit internal yang dilakukan oleh pihak independen dengan cakupan keseluruhan aset informasi, kebijakan dan prosedur keamanan yang ada (atau sesuai dengan standar yang berlaku)?			✓	
4.24	Apakah audit internal tersebut mengevaluasi tingkat kepatuhan, konsistensi dan efektivitas penerapan keamanan informasi?				✓
4.25	Apakah hasil audit internal tersebut dikaji/dievaluasi untuk mengidentifikasi langkah pembenahan dan pencegahan, ataupun inisiatif peningkatan kinerja keamanan informasi?				✓
4.26	Apakah hasil audit internal dilaporkan kepada pimpinan organisasi untuk menetapkan langkah perbaikan atau program peningkatan kinerja keamanan informasi?				✓
4.27	Apabila ada keperluan untuk merevisi kebijakan dan prosedur yang berlaku, apakah ada analisa untuk menilai aspek finansial (dampak biaya dan keperluan anggaran) ataupun perubahan terhadap infrastruktur dan pengelolaan perubahannya, sebagai prasyarat untuk menerapkannya?			✓	
4.28	Apakah organisasi anda secara periodik menguji dan mengevaluasi tingkat/status kepatuhan program keamanan informasi yang ada (mencakup pengecualian atau kondisi ketidakpatuhan lainnya) untuk memastikan bahwa keseluruhan inisiatif tersebut, termasuk langkah			✓	

	pembenahan yang diperlukan, telah diterapkan secara efektif?				
4.29	Apakah organisasi anda mempunyai rencana dan program peningkatan keamanan informasi untuk jangka menengah/panjang (1-3-5 tahun) yang direalisasikan secara konsisten?			✓	
	Total Nilai Evaluasi Kerangka Kerja	56			

KUISIONER ASPEK ENGELOLAAN ASET INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner ini mengevaluasi kelengkapan pengamanan aset informasi, termasuk keseluruhan siklus penggunaan aset tersebut. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Pengelolaan Aset Informasi					
5.1	Apakah tersedia daftar inventaris aset informasi dan aset yang berhubungan dengan proses teknologi informasi secara lengkap, akurat dan terpelihara ? (termasuk kepemilikan aset)				√
5.2	Apakah tersedia definisi klasifikasi aset informasi yang sesuai dengan peraturan perundangan yang berlaku?				√
5.3	Apakah tersedia proses yang mengevaluasi dan mengklasifikasi aset informasi sesuai tingkat kepentingan aset bagi instansi/perusahaan dan keperluan pengamanannya?			√	
5.4	Apakah tersedia definisi tingkatan akses yang berbeda dari setiap klasifikasi aset informasi dan matriks yang merekam alokasi akses tersebut?			√	
5.5	Apakah tersedia proses pengelolaan perubahan terhadap sistem, proses bisnis dan proses teknologi informasi (termasuk perubahan konfigurasi) yang diterapkan secara konsisten?			√	
5.6	Apakah tersedia proses pengelolaan konfigurasi yang diterapkan secara konsisten?				√
5.7	Apakah tersedia proses untuk merilis suatu aset baru ke dalam lingkungan operasional dan memutakhirkan inventaris aset informasi?				√
5.8	Apakah instansi/perusahaan anda memiliki dan menerapkan kontrol keamanan di bawah ini, sebagai kelanjutan dari proses penerapan mitigasi risiko?			√	
5.9	Definisi tanggungjawab pengamanan informasi secara individual untuk semua personil di instansi/perusahaan anda				√

5.10	Tata tertib penggunaan komputer, email, internet dan intranet				✓	
5.11	Tata tertib pengamanan dan penggunaan aset instansi/perusahaan terkait HAKI			✓		
5.12	Peraturan terkait instalasi piranti lunak di aset TI milik instansi/perusahaan			✓		
5.13	Peraturan penggunaan data pribadi yang mensyaratkan pemberian ijin tertulis oleh pemilik data pribadi			✓		
5.14	Pengelolaan identitas elektronik dan proses otentikasi (*username* & *password*) termasuk kebijakan terhadap pelanggarannya				✓	
5.15	Persyaratan dan prosedur pengelolaan/pemberian akses, otentikasi dan otorisasi untuk menggunakan aset informasi				✓	
5.16	Ketetapan terkait waktu penyimpanan untuk klasifikasi data yang ada dan syarat penghancuran data			✓		
5.17	Ketetapan terkait pertukaran data dengan pihak eksternal dan pengamanannya				✓	
5.18	Proses penyidikan/investigasi untuk menyelesaikan insiden terkait kegagalan keamanan informasi			✓		
5.19	Prosedur *back-up* dan uji coba pengembalian data (*restore*) secara berkala				✓	
5.20	Ketentuan pengamanan fisik yang disesuaikan dengan definisi zona dan klasifikasi aset yang ada di dalamnya			✓		
5.21	Proses pengecekan latar belakang SDM			✓		
5.22	Proses pelaporan insiden keamanan informasi kepada pihak eksternal ataupun pihak yang berwajib.			✓		
5.23	Prosedur penghancuran data/aset yang sudah tidak diperlukan				✓	
5.24	Prosedur kajian penggunaan akses (*user access review*) dan hak aksesnya *(user access rights*) berikut langkah pembenahan apabila terjadi ketidaksesuaian (*non-conformity*) terhadap kebijakan yang berlaku				✓	
5.25	Prosedur untuk *user* yang mutasi/keluar atau tenaga kontrak/*outsource* yang habis masa kerjanya.				✓	
5.26	Apakah tersedia daftar data/informasi yang harus di-*backup* dan laporan analisa kepatuhan terhadap prosedur *backup*-nya?					✓
5.27	Apakah tersedia daftar rekaman pelaksanaan keamanan informasi dan bentuk pengamanan yang sesuai dengan klasifikasinya?					✓
Pengamanan Fisik						
5.28	Apakah sudah diterapkan pengamanan fasilitas fisik (lokasi kerja) yang sesuai dengan kepentingan/klasifikasi aset informasi, secara berlapis					✓

	dan dapat mencegah upaya akses oleh pihak yang tidak berwenang?				
5.29	Apakah tersedia proses untuk mengelola alokasi kunci masuk (fisik dan elektronik) ke fasilitas fisik?				✓
5.30	Apakah infrastruktur komputasi terlindungi dari dampak lingkungan atau api dan berada dalam kondisi dengan suhu dan kelembaban yang sesuai dengan prasyarat pabrikannya?				✓
5.31	Apakah infrastruktur komputasi yang terpasang terlindungi dari gangguan pasokan listrik atau dampak dari petir?				✓
5.32	Apakah tersedia peraturan pengamanan perangkat komputasi milik instansi/perusahaan anda apabila digunakan di luar lokasi kerja resmi (kantor)?			✓	
5.33	Apakah tersedia proses untuk memindahkan aset TIK (piranti lunak, perangkat keras, data/informasi dll) dari lokasi yang sudah ditetapkan (termasuk pemutakhiran lokasinya dalam daftar inventaris)?			✓	
5.34	Apakah konstruksi ruang penyimpanan perangkat pengolah informasi penting menggunakan rancangan dan material yang dapat menanggulangi risiko kebakaran dan dilengkapi dengan fasilitas pendukung (deteksi kebakaran/asap, pemadam api, pengatur suhu dan kelembaban) yang sesuai?				✓
5.35	Apakah tersedia proses untuk memeriksa (inspeksi) dan merawat: perangkat komputer, fasilitas pendukungnya dan kelayakan keamanan lokasi kerja untuk menempatkan aset informasi penting?				✓
5.36	Apakah tersedia mekanisme pengamanan dalam pengiriman aset informasi (perangkat dan dokumen) yang melibatkan pihak ketiga?				✓
5.37	Apakah tersedia peraturan untuk mengamankan lokasi kerja penting (ruang server, ruang arsip) dari risiko perangkat atau bahan yang dapat membahayakan aset informasi (termasuk fasilitas pengolah informasi) yang ada di dalamnya? (misal larangan penggunaan telpon genggam di dalam ruang server, menggunakan kamera dll)				✓
5.38	Apakah tersedia proses untuk mengamankan lokasi kerja dari keberadaan/kehadiran pihak ketiga yang bekerja untuk kepentingan instansi/perusahaan anda?				✓
	Total Nilai Evaluasi Pengelolaan Aset	99			

KUISIONER ASPEK TEKNOLOGI DAN KEAMANAN INFORMASI
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner Bagian ini mengevaluasi kelengkapan, konsistensi dan efektifitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
Pengamanan Teknologi					
6.1	Apakah layanan TIK (sistem komputer) yang menggunakan internet sudah dilindungi dengan lebih dari 1 lapis pengamanan?				√
6.2	Apakah jaringan komunikasi disegmentasi sesuai dengan kepentingannya (pembagian instansi/perusahaan, kebutuhan aplikasi, jalur akses khusus, dll)?				√
6.3	Apakah tersedia konfigurasi standar untuk keamanan sistem bagi keseluruhan aset jaringan, sistem dan aplikasi, yang dimutakhirkan sesuai perkembangan (standar industri yang berlaku) dan kebutuhan?				√
6.4	Apakah instansi/perusahaan anda secara rutin menganalisa kepatuhan penerapan konfigurasi standar yang ada?			√	
6.5	Apakah jaringan, sistem dan aplikasi yang digunakan secara rutin dipindai untuk mengidentifikasi kemungkinan adanya celah kelemahan atau perubahan/keutuhan konfigurasi?				√
6.6	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dirancang untuk memastikan ketersediaan (rancangan redundan) sesuai kebutuhan/persyaratan yang ada?				√
6.7	Apakah keseluruhan infrastruktur jaringan, sistem dan aplikasi dimonitor untuk memastikan ketersediaan kapasitas yang cukup untuk kebutuhan yang ada?				√
6.8	Apakah setiap perubahan dalam sistem informasi secara otomatis terekam di dalam log?				√
6.9	Apakah upaya akses oleh yang tidak berhak secara otomatis terekam di dalam log?				√

6.10	Apakah semua log dianalisa secara berkala untuk memastikan akurasi, validitas dan kelengkapan isinya (untuk kepentingan jejak audit dan forensik)?			✓	
6.11	Apakah instansi/perusahaan anda menerapkan enkripsi untuk melindungi aset informasi penting sesuai kebijakan pengelolaan yang ada?			✓	
6.12	Apakah instansi/perusahaan anda mempunyai standar dalam menggunakan enkripsi?			✓	
6.13	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mengelola kunci enkripsi (termasuk sertifikat elektronik) yang digunakan, termasuk siklus penggunaannya?			✓	
6.14	Apakah semua sistem dan aplikasi secara otomatis mendukung dan menerapkan penggantian *password* secara otomatis, termasuk menon-aktifkan *password*, mengatur kompleksitas/panjangnya dan penggunaan kembali *password* lama?		✓		
6.15	Apakah akses yang digunakan untuk mengelola sistem (administrasi sistem) menggunakan bentuk pengamanan khusus yang berlapis?			✓	
6.16	Apakah sistem dan aplikasi yang digunakan sudah menerapkan pembatasan waktu akses termasuk otomatisasi proses *timeouts*, *lockout* setelah kegagalan *login*,dan penarikan akses?				✓
6.17	Apakah instansi/perusahaan anda menerapkan pengamanan untuk mendeteksi dan mencegah penggunaan akses jaringan (termasuk jaringan nirkabel) yang tidak resmi?				✓
6.18	Apakah instansi/perusahaan anda menerapkan bentuk pengamanan khusus untuk melindungi akses dari luar instansi/perusahaan?				✓
6.19	Apakah sistem operasi untuk setiap perangkat *desktop* dan *server* dimutakhirkan dengan versi terkini?				✓
6.20	Apakah setiap *desktop* dan *server* dilindungi dari penyerangan virus (*malware*)?				✓
6.21	Apakah ada rekaman dan hasil analisa (jejak audit - *audit trail*) yang mengkonfirmasi bahwa antivirus/antimalware telah dimutakhirkan secara rutin dan sistematis?				✓
6.22	Apakah adanya laporan penyerangan virus/malware yang gagal/sukses ditindaklanjuti dan diselesaikan?				✓
6.23	Apakah keseluruhan jaringan, sistem dan aplikasi sudah menggunakan mekanisme sinkronisasi waktu yang akurat, sesuai dengan standar yang ada?				✓
6.24	Apakah setiap aplikasi yang ada memiliki spesifikasi dan fungsi keamanan yang diverifikasi/validasi pada saat proses pengembangan dan uji coba?			✓	
6.25	Apakah instansi/perusahaan ada menerapkan lingkungan pengembangan dan uji coba yang sudah diamankan sesuai dengan standar platform teknologi				✓

	yang ada dan digunakan untuk seluruh siklus hidup sistem yng dibangun?				
6.26	Apakah instansi/perusahaan anda melibatkan pihak independen untuk mengkaji kehandalan keamanan informasi secara rutin?				✓
	Total Nilai Evaluasi Teknologi dan Keamanan Informasi	69			

KUISIONER ASPEK SUPLEMEN
INDEKS KEAMANAN INFORMASI (KAMI)
UIN SUNAN KALIJAGA
YOGYAKARTA

Kuisoner Bagian ini mengevaluasi kelengkapan, konsistensi dan efektivitas penggunaan teknologi dalam pengamanan aset informasi. Berilah tanda (√) untuk jawaban yang sesuai dengan kondisi yang ada di instansi anda dan isi sesuai dengan tingkat kepentingan yaitu

- 0 = Tidak Dilakukan
- 1 = Dalam Perencanaan
- 2 = Dalam Penerapan / Diterapkan Sebagian
- 3 = Diterapkan Secara Menyeluruh

No	Fungsi/Organisasi Keamanan Informasi	Status			
		0	1	2	3
7.1	**Pengamanan Keterlibatan Pihak Ketiga Penyedia Layanan**				
7.1.1	**Manajemen Risiko dan Pengelolaan Keamanan pihak ketiga**				
7.1.1.1	Apakah instansi/perusahaan mengidentifikasi risiko keamanan informasi yang ada terkait dengan kerjasama dengan pihak ketiga atau karyawan kontrak?			√	
7.1.1.2	Apakah instansi/perusahaan mengkomunikasikan dan mengklarifikasi risiko keamanan informasi yang ada pada pihak ketiga kepada mereka?				√
7.1.1.3	Apakah instansi/perusahaan mengklarifikasi persyaratan mitigasi risiko instansi/perusahaan dan ekspektasi mitigasi risiko yang harus dipatuhi oleh pihak ketiga?				√
7.1.1.4	Apakah rencana mitigasi terhadap risiko yang diidentifikasi tersebut disetujui oleh manajemen pihak ketiga atau karyawan kontrak?			√	
7.1.1.5	Apakah instansi/perusahaan telah menerapkan kebijakan keamanan informasi bagi pihak ketiga secara memadai, mencakup persyaratan pengendalian akses, penghancuran informasi, manajemen risiko penyediaan layanan pihak ketiga, dan NDA bagi karyawan pihak ketiga?		√		
7.1.1.6	Apakah kebijakan tersebut (7.1.1.5) telah dikomunikasikan kepada pihak ketiga dan mereka menyatakan persetujuannya dalam dokumen kontrak, SLA atau dokumen sejenis lainnya?		√		
7.1.1.7	Apakah hak audit TI secara berkala ke pihak ketiga telah ditetapkan sebagai bagian dan persyaratan kontrak, dikomunikasikan dan disetujui pihak ketiga?			√	

	Termasuk di dalamnya akses terhadap laporan audit internal/eksternal tentang kondisi kontrol keamanan informasi pihak ketiga?				
7.1.2	**Pengelolaan Sub-Kontraktor/Alih Daya pada Pihak Ketiga**				
7.1.2.1	Apakah pihak ketiga sudah mengidentifikasi risiko terkait alih daya, subkontraktor atau penyedia teknologi/infrastruktur yang digunakan dalam layanannya?			✓	
7.1.2.2	Apakah pihak ketiga sudah menerapkan pengendalian risikonya dalam perjanjian dengan mereka atau dokumen sejenis?				✓
7.1.2.3	Apakah pihak ketiga melakukan pemantauan dan evaluasi terhadap kepatuhan alih daya, subkontraktor atau penyedia teknologi/infrastruktur terhadap persyaratan keamanan yang ditetapkan?			✓	
7.1.3	**Pengelolaan Layanan dan Keamanan Pihak Ketiga**				
7.1.3.1	Apakah instansi/perusahaan telah menetapkan proses, prosedur atau rencana terdokumentasi untuk mengelola dan memantau layanan dan aspek keamanan informasi (termasuk pengamanan aset informasi dan infrastruktur milik instanasi/perusahaan yang diakses) dalam hubungan kerjasama dengan pihak ketiga?			✓	
7.1.3.2	Apakah peran dan tanggung jawab pemantauan, evaluasi dan/atau audit aspek keamanan informasi pihak ketiga telah ditetapkan dan/atau ditugaskan dalam unit organisasi tertentu?			✓	
7.1.3.3	Apakah tersedia laporan berkala tentang pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan yang disyaratkan dalam perjanjian komersil (kontrak)?			✓	
7.1.3.4	Apakah ada rapat secara berkala untuk memantau dan mengevaluasi pencapaian sasaran tingkat layanan (SLA) dan aspek keamanan?			✓	
7.1.3.5	Apakah hasil pemantauan dan evaluasi terhadap laporan atau pembahasan dalam rapat berkala tersebut didokumentasikan, dikomunikasikan dan ditindaklanjuti oleh pihak ketiga serta dilaporkan kemajuannya kepada instansi/perusahaan?			✓	
7.1.3.6	Apakah instansi/perusahaan telah menetapkan rencana dan melakukan audit terhadap pemenuhan persyaratan keamanan informasi oleh pihak ketiga?			✓	
7.1.3.7	Apakah hasil audit tersebut ditindaklanjuti oleh pihak ketiga dengan melaporkan rencana perbaikan yang terukur dan bukti-bukti penerapan rencana tersebut?			✓	
7.1.3.8	Apakah kondisi terkait denda/penalti karena ketidakpatuhan pihak ketiga terhadap persyaratan dan/atau tingkat layanan telah didokumentasikan, dikomunikasikan, dipahami dan diterapkan?				✓

7.1.4	**Pengelolaan Perubahan Layanan dan Kebijakan Pihak Ketiga**				
7.1.4.1	Apakah instansi/perusahaan mengelola perubahan yang terjadi dalam hubungan dengan pihak ketiga yang menyangkut antara lain? - Perubahan layanan pihak ketiga; - Perubahan kebijakan, prosedur, dan/atau - Kontrol risiko pihak ketiga?				✓
7.1.4.2	Apakah risiko yang menyertai perubahan tersebut dikaji, didokumentasikan dan ditetapkan rencana mitigasi barunya?				✓
7.1.5	**Penanganan Aset**				
7.1.5.1	Apakah pihak ketiga memiliki prosedur formal untuk menangani data selama dalam siklus hidupnya mulai dari pembuatan, pendaftaran, perubahan, dan penghapusan/penghancuran aset?			✓	
7.1.5.2	Apakah per untuk penghancuran (disposal) data secara aman telah disepakati bersama pihak ketiga (pihak ketiga)?				✓
7.1.6	**Pengelolaan Insiden oleh Pihak Ketiga**				
7.1.6.1	Apakah pihak ketiga memiliki prosedur untuk pelaporan, pemantauan, penanganan, dan analisis insiden keamanan informasi?				✓
7.1.6.2	Apakah pihak ketiga memiliki bukti-bukti penerapan yang memadai dalam menangani insiden keamanan informasi?				✓
7.1.7	**Rencana Kelangsungan Layanan Pihak Ketiga**				
7.1.7.1	Apakah pihak ketiga memiliki kebijakan, prosedur atau rencana terdokumentasi untuk mengatasi kelangsungan layanan pihak ketiga dalam keadaan darurat/bencana?				✓
7.1.7.2	Apakah kebijakan, prosedur atau rencana kelangsungan layanan tersebut telah diujicoba, didokumentasikan hasilnya dan dievaluasi efektivitasnya?				✓
7.1.7.3	Apakah pihak ketiga memiliki organisasi atau tim khusus yang ditugaskan untuk mengelola proses kelangsungan layanannya?				✓
7.2	**Pengamanan Layanan Infrastruktur Awan (Cloud Service)**				
7.2.1	Apakah instansi/perusahaan sudah melakukan kajian risiko terkait penggunaan layanan berbasis *cloud* dan menyesuaikan kebijakan keamanan informasi terkait layanan ini?		✓		
7.2.2	Apakah instansi/perusahaan sudah menetapkan data apa saja yang akan disimpan/diolah/dipertukarkan melalui layanan berbasis *cloud*?		✓		
7.2.3	Apakah instansi/perusahaan sudah menerapkan langkah pengamanan data pribadi yang disimpan/diolah/dipertukarkan melalui layanan *cloud*?		✓		

7.2.4	Apakah instansi/perusahaan sudah mengkaji, menetapkan kriteria dan memastikan aspek hukum (jurisdiksi, hak dan kewenangan) terkait penggunaan layanan berbasis *cloud*?		✓		
7.2.5	Apakah instansi/perusahaan sudah mengevaluasi penyelenggara layanan *cloud* terkait reputasi penyelenggaranya?		✓		
7.2.6	Apakah instansi/perusahaan sudah menetapkan standar keamanan teknis penggunaan layanan *cloud,* termasuk aspek penggunaannya oleh pengguna di internal instansi/perusahaan?		✓		
7.2.7	Apakah instansi/perusahaan sudah mengevaluasi kelaikan keamanan layanan *cloud* termasuk aspek ketersediaannya dan pemenuhan sertifikasi layanan berbasis ISO 27001?		✓		
7.2.8	Apakah instansi/perusahaan sudah memiliki kebijakan, strategi dan proses untuk mengganti layanan *cloud* atau menyediakan fasilitas pengganti apabila terjadi gangguan sementara pada layanan tersebut?		✓		
7.2.9	Apakah instansi/perusahaan sudah memiliki proses pelaporan insiden terkait layanan *cloud*?		✓		
7.2.10	Apakah instansi/perusahaan sudah memiliki proses untuk menghentikan layanan *cloud,* termasuk proses pengamanan data yang ada (memindahkan dan menghapus data)?		✓		
7.3	**Perlindungan Data Pribadi**				
7.3.1	Apakah instansi/perusahaan sudah mendokumentasikan jenis dan bentuk (dokumen kertas/elektronik) data pribadi yang disimpan, diolah dan dipertukarkan dengan pihak eksternal?			✓	
7.3.2	Apakah instansi/perusahaan sudah memetakan alur pemrosesan data di internal dan pertukaran data dengan pihak eksternal, termasuk kapan dan dimana data pribadi tersebut diperoleh?			✓	
7.3.3	Apakah proses terkait penyimpanan, pengolahan dan pertukaran data pribadi di instansi/perusahaan sudah didokumentasikan?			✓	
7.3.4	Apakah instansi/perusahaan sudah memiliki kebijakan terkait Perlindungan Data Pribadi sesuai dengan Peraturan dan Perundangan yang berlaku?		✓		
7.3.5	Apakah instansi/perusahaan sudah menunjuk pejabat-pejabat (*Data Protection Officer, Data Controller, Data Processor*) yang bertanggung-jawab dan berwenang dalam penerapan kebijakan dan proses Perlindungan Data Pribadi?		✓		
7.3.6	Apakah instansi/perusahaan sudah menganalisa dampak terkait terungkapnya data pribadi yang disimpan, diolah dan dipertukarkan secara ilegal atau karena insiden lain?		✓		

7.3.7	Apakah kajian risiko keamanan pada instansi/perusahaan sudah memasukkan aspek Perlindungan Data Pribadi?		✓		
7.3.8	Apakah mekanisme perlindungan data pribadi sudah diterapkan sesuai keperluan mitigasi risiko dan peraturan perundangan yang berlaku?		✓		
7.3.9	Apakah instansi/perusahaan sudah menjalankan program peningkatan pemahaman/kepedulian kepada seluruh pegawai terkait Perlindungan Data Pribadi, termasuk hal-hal terkait Peraturan Perundangan yang berlaku?		✓		
7.3.10	Apakah instansi/perusahaan sudah mendapatkan persetujuan dari pemilik data pribadi saat mengambil data tersebut, termasuk penjelasan hak pemilik data, apa saja yang akan diberlakukan pada data pribadi tersebut dan menyimpan catatan persetujuan tersebut ?		✓		
7.3.11	Apakah instansi/perusahaan sudah memiliki proses untuk melaporkan insiden terkait terungkapnya data pribadi?		✓		
7.3.12	Apakah instansi/perusahaan sudah menerapkan proses yang menjamin hak pemilik data pribadi untuk mengakses data tersebut?		✓		
7.3.13	Apakah instansi/perusahaan sudah menerapkan proses yang terkait dapat memastikan data pribadi tersebut akurat dan termutakhirkan?			✓	
7.3.14	Apakah instansi/perusahaan sudah menerapkan proses terkait periode penyimpanan data pribadi dan penghapusan/pemusnahannya sesuai dengan peraturan atau perjanjian dengan pemilik data?			✓	
7.3.15	Apakah instansi/perusahaan sudah menerapkan proses terkait penghapusan/pemusnahan data apabila sudah tidak ada keperluan yang sah untuk menyimpan/mengolahnya lebih lanjut atau atas permintaan pemilik data dan menyimpan catatan proses tersebut?			✓	
7.3.16	Apakah instansi/perusahaan sudah menerapkan proses terkait pengungkapan data pribadi atas permintaan resmi aparat penegak hukum?		✓		

Universitas Islam Negeri Sunan Kalijaga FM-STUINSK-BM-05-B/R0

PENUNJUKAN PEMBIMBING TESIS

Kepada Yth. Bapak/Ibu:
Bambang Sugiantoro

Assalaamu'alaikum wr.wb.
Dengan hormat,
Berdasarkan rapat koordinasi Program Studi Magister Informatika tentang Tesis, kami meminta Bapak/Ibu untuk menjadi pembimbing Tesis mahasiswa:

Nama	:	Rizki Dewantara
NIM	:	18206050002
Prodi	:	Magister Informatika
Fakultas	:	Sains dan Teknologi
Tema	:	Perancangan Optimalisasi Jaringan Komputer di UIN Sunan Kalijaga Menggunakan Metode Traffic Load Balancing dengan Security and Event Management (SIEM) dan Implikasinya pada Indeks Keamanan Informasi (KAMI)

Kami berharap Bapak/Ibu dapat segera mengarahkan dan membimbing mahasiswa tersebut untuk menyusun Tesis. Atas perhatiannya, kami mengucapkan terima kasih.

Wassalaamu'alaikum wr.wb.

Yogyakarta, 10 Januari 2019
Ketua Program Studi

Bambang Sugiantoro

Mohon difoto copy 1 lembar untuk Dosen Pembimbing

KEMENTERIAN AGAMA REPUBLIK INDONESIA
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA YOGYAKARTA
FAKULTAS SAINS DAN TEKNOLOGI
Jalan Marsda Adisucipto Yogyakarta 55281, Telepon (0274) 519739; Faksimili (0274) 540971;
Website: http://saintek.uin-suka.ac.id

Nomor : B-1545/Un.02/DST.1/PT.01.04/04/2019 Yogyakarta, 30 April 2019
Lamp : 1 bendel proposal
Hal : Permohonan Ijin Penelitian

Kepada:
Yth. Kepala Pusat Teknologi Informasi dan Pangkalan Data (PTIPD)
UIN Sunan Kalijaga Yogyakarta
di Tempat.

Assalamu'alaikum Wr.Wb.

Kami beritahukan bahwa untuk kelengkapan penyusunan Tugas Akhir/Tesis dengan judul: **"Optimalisasi Jaringan Komputer di Universitas UIN Sunan Kalijaga Menggunakan Metode Traffic Load Balancing dengan Security Information and Event Management (SIEM) dan Implementasinya Pada Indeks Keamanan Informasi (KAMI)"** diperlukan Penelitian.

Oleh karena itu, kami mengajukan permohonan kepada Kepala PTIPD UIN Sunan Kalijaga Yogyakarta untuk memberikan izin penelitian kepada mahasiswa kami,

Nama	:	Rizki Dewantara, S.Kom, CCNA
NIM	:	18206050002
Program Studi	:	Magister Informatika
Alamat	:	Nusupan RT 01 RW 28, Trihanggo, Gampin, Sleman, D.I. Yogyakarta

untuk melakukan penelitian di PTIPD UIN Sunan Kalijaga Yogyakarta, dengan metode penelitian *SIEM* yang dijadwalkan pada tanggal 02 Mei 2019 s.d 31 Desember 2019.

Sebagai bahan pertimbangan bersama ini kami lampirkan:
1. Proposal Tesis
2. Fotocopy Kartu Tanda Mahasiswa (KTM)
3. Fotocopy Kartu Rencana Studi (KRS)

Demikian surat permohonan ini disampaikan, atas diperkenankannya diucapkan terimakasih.

Wassalamu'alaikum Wr.Wb.

a.n. Dekan,
Wakil Dekan Bidang Akademik,

Agung Fatwanto

Tembusan:
- Dekan (Sebagai laporan)

Lampiran KODE DOKUMEN : FST-01 / 17

SURAT KETERANGAN BEBAS LABORATORIUM

Laboratorium Terpadu Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta dengan ini menerangkan bahwa mahasiswa yang tersebut di bawah ini :

Nama : RIZKI DEWANTARA
NIM : 18206050002
Prodi : INFORMATIKA

telah menyelesaikan segala bentuk administrasi yang terkait aktivitas yang bersangkutan di Laboratorium Terpadu Fakultas Sains dan Teknologi. Oleh karena itu, mahasiswa tersebut dinyatakan telah BEBAS TANGGUNGAN LABORATORIUM.

Telah diverifikasi oleh Pranata Laboratorium Pendidikan (PLP) :

Nama PLP	Tanda Tangan
1. Yusuf Murdani, S.Kom.	.....
2. Awan Pramudya W, S.Kom.	.....
3. Muhammad Munawir, S.T.	.....

Surat Keterangan Bebas Laboratorium ini dibuat untuk digunakan sebagaimana mestinya.

Yogyakarta, 04 Juni 2020
Koordinator Laboratorium Bidang Teknik Informatika

M. Taufiq Nuruzzaman, S.T., M.Eng, Ph.D
NIP.19791118 200501 1 003

MINISTRY OF RELIGIOUS AFFAIRS
STATE ISLAMIC UNIVERSITY SUNAN KALIJAGA YOGYAKARTA
CENTER FOR LANGUAGE DEVELOPMENT

TEST OF ENGLISH COMPETENCE CERTIFICATE

No: UIN.02/L4/PM.03.2/2.20611.35.177/2020

This is to certify that:

Name : **Rizki Dewantara, S.Kom**
Date of Birth : **December 28, 1995**
Sex : **Male**

achieved the following scores on the Test of English Competence (TOEC) held on **January 16, 2020** by Center for Language Development of State Islamic University Sunan Kalijaga:

CONVERTED SCORE	
Listening Comprehension	**43**
Structure & Written Expression	**44**
Reading Comprehension	**48**
Total Score	**450**

Validity: 2 years since the certificate's issued

Yogyakarta, January 16, 2020
Director,

Dr. Sembodo Ardi Widodo, S.Ag., M.Ag.
NIP. 19680915 199803 1 005

وزارة الشؤون الدينية
جامعة سونان كاليجاكا الإسلامية الحكومية بجوكجاكرتا
مركز التنمية اللغوية

شهادة
اختبار كفاءة اللغة العربية

الرقم: UIN.02/L4/PM.03.2/6.20611.35.1/2020

تشهد إدارة مركز التنمية اللغوية بأنّ

الاسم : Rizki Dewantara, S.Kom
تاريخ الميلاد : ٢٨ ديسمبر ١٩٩٥

قد شارك في اختبار كفاءة اللغة العربية في ١٥ يناير ٢٠٢٠, وحصل على درجة :

فهم المسموع	٤٨
التراكيب النحوية و التعبيرات الكتابية	٣١
فهم المقروء	٢٧
مجموع الدرجات	٣٥٣

هذه الشهادة صالحة لمدة سنتين من تاريخ الإصدار

جوكجاكرتا, ١٥ يناير ٢٠٢٠
المدير

Dr. Sembodo Ardi Widodo, S.Ag., M.Ag.
رقم التوظيف : ١٩٦٨٠٩١٥١٩٩٨٠٣١٠٠٥

Thesis Dewantara

ORIGINALITY REPORT

14%	9%	0%	16%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Universitas Brawijaya Student Paper	7%
2	ejournal.ikmi.ac.id Internet Source	2%
3	imanagustrian.blogspot.co.id Internet Source	2%
4	library.binus.ac.id Internet Source	2%

Exclude quotes	On	Exclude matches	< 2%
Exclude bibliography	On		