E-ISSN : 2722-4759
P-ISSN : 2722-4732

PENILAIAN KEAMANAN APLIKASI BERBAGI BERKAS AUFRATIA MENGGUNAKAN STANDAR ISO 27001

Khurin In Noviarani[1], Walied Ghaly[2], Johan Ferliansyah[3]
[1,2,3]Program Studi Teknik Informatika, Fakultas Teknik, Universitas Muhammadiyah Gresik, Kabupaten Gresik, Jawa Timur, Indonesia
khurin.noviarani@gmail.com[1], waliedgly@gmail.com[2],
jojosulaiman49@gmail.com[3]

Abstract
Background *- The Covid-19 pandemic has an impact on the educational aspect of using online internet media. however, storage media for online activities is still lacking. Especially the lack of flexibility, space for modification and privacy controls provided free of charge by existing file sharing service providers provide various obstacles in accelerating and exchanging information and data using file sharing media services, this is what makes various universities and their academics to develop their file sharing services..*
Purpose *- to evaluate the results of the quality of information security from the Aufratia file sharing application developed independently by the UMG academic community.*
Design/methodology/approach *- This research is a descriptive qualitative research type, while the root cause analysis uses the Fishbone Diagram.*
Findings *- The Aufratia application still does not meet the ISO 27001 standard. Information protection is minimal and almost non-existent, making Aufratia unfit to be a release application and currently it is more suitable to be a beta version (tested) application.*
Research implications *- This research provides a contribution in terms of developing file sharing application software that utilizes the internet.*
Research limitation *- Research only examines one software, further research can be modified or compared with other software to assess the advantages and disadvantages that can be used to complement each other.*

Keywords*: Aufratia, file, sharing, application, online.*

Abstrak
Latar Belakang – Pandemi covid-19 berimbas pada aspek pendidikan yang menggunakan media online imternet, namum media penyimpanan untuk aktivitas daring tersebut masih kurang. Terutama kurangnya fleksibilitas, ruang modifikasi dan kontrol privasi yang disediakan secara gratis oleh *provider* layanan berbagi berkas yang ada memberikan berbagai hambatan dalam percepatan dan pertukaran informasi dan data menggunakan layanan media berbagi berkas, hal inilah yang membuat berbagai universitas dan civitas akademiknya untuk mengembangkan layanan berbagi berkasnya sendiri.
Tujuan - untuk mengevaluasi hasil kualitas keamanan informasi dari aplikasi berbagi berkas Aufratia yang dikembangkan secara mandiri oleh civitas akademik UMG.
Desain/metodologi/pendekatan - Penelitian ini merupakan jenis penelitian deskriptif kualitatif sedangkan analisa pencarian akar masalah dengan menggunakan *Fishbone* Diagram.
Temuan - Aplikasi Aufratia masih belum memenuhi Standar ISO 27001. Perlindungan informasi yang sangat minimal dan hampir tidak ada, menjadikan aufratia tidak layak menjadi aplikasi release dan saat ini lebih pantas untuk dijadikan applikasi beta version (*tested*).

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

Implikasi penelitian – Penelitian ini memberikan sumbangsi dalam hal pengembangan software aplikasi berbagi berkas yang memanfaatkan internet..
Batasan penelitian – Penelitian hanya menelaah satu *software*,penelitian selajutnya bisa dengan modifikasi atau perbandingan dengan *software* lain untuk menilai kelebihan dan kekurangan yang dapat digunakan untuk saling melengkapi.

Kata kunci : Aufratia, aplikasi berbagi berkas, *online*.

I. PENDAHULUAN

Tahun 2020 merupakan evolusi struktur sosial terbesar dalam peradaban manusia, pandemi Covid-19 secara masif telah mengubah pola komunikasi manusia akibat kebijakan lockdown yang diterapkan berbagai negara di dunia termasuk indonesia. Telkomsel sebagai penyedia jasa layanan komunikasi menyatakan dalam situs berita *the jakarta post*, bahwa terdapat kenaikan *broadband traffic* sebesar 16% yang mana 5% di antaranya didominasi oleh aplikasi *e-learning* (Eloksari, 2020). Pernyataan tersebut secara implisit menunjukan perubahan yang terjadi dalam pola pembelajaran di dunia pendidikan di indonesia.

Perubahan pola pembelajaran melalui digitalisasi metode pembelajaran, tidak hanya dipengaruhi oleh kebijakan *lockdown* akibat pandemi COVID-19, perkembangan teknologi dan pengguna internet juga mengambil peran dalam digitalisasi metode pembelajaran. Seperti data yang dirilis Tim *WeAreSocial* pada bulan Januari 2020, pengguna aktif internet di Indonesia mencapai 175,4 Juta atau 64% dari jumlah populasi penduduk di Indonesia sebagaimana gambar 1 (Kemp, 2020).

Gambar 1. Pengguna Internet di Indonesia

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

Salah satu digitalisasi yang mendasari pengembangan Aufratia adalah kebijakan perkuliahan secara daring yang diterapkan kampus, kebijakan perkuliahan secara daring yang diterapkan kampus memberikan peluang kepada pemanfaatan layanan media/ aplikasi berbagi berkas sebagai percepatan pertukaran informasi dan data seperti *google drive*, dropbox dan berbagai layanan lain.

Kurangnya fleksibilitas, ruang modifikasi dan kontrol privasi yang disediakan secara gratis oleh provider layanan berbagi berkas yang ada memberikan berbagai hambatan dalam percepatan dan pertukaran informasi dan data menggunakan layanan media berbagi berkas, hal inilah yang membuat berbagai universitas dan civitas akademiknya untuk mengembangkan layanan berbagi berkasnya sendiri.

Aufratia merupakan salah satu aplikasi berbagi berkas yang dikembangkan secara mandiri oleh civitas akademik UMG untuk menjawab tantangan di atas. Mengingat pentingnya informasi dari berkas yang diunggah dalam Aufratia, maka informasi harus diamankan. Terjadinya masalah keamanan dapat menimbulkan kegagalan dalam menjalankan perkuliahan secara daring. Pengembang Aufratia selama ini belum pernah mengetahui sampai dimana tingkat keamanan informasi yang dimilikinya.

Dibutuhkan evaluasi atau audit keamanan informasi untuk menjaga keamanan informasi yang berada di Aufratia. ISO 27001 yang digunakan secara fleksibel dapat dikembangkan tergantung kebutuhan organisasi, tujuan organisasi, dan persyaratan keamanan sebagai media penelitian asesmen untuk menilai dan memetakan permasalahan keamanan terhadap aset informasi pada Aufratia yang akan digunakan sebagai pendekatan dan pedoman dalam membuat rancangan model pengendalian keamanan informasi menggunakan ISO 27001. Pada penelitian ini akan digunakan ISO 27001 *Annex A Controls* untuk mengevaluasi hasil kualitas keamanan informasi dan *Fishbone* untuk menganalisis hasil untuk diberikan rekomendasi dari masalah terkait.

II. TINJUAN PUSTAKA

Aufratia

Aufratia merupakan aplikasi berbagi berkas yang dikembangkan secara mandiri oleh civitas akademik UMG sebagai salah satu respon terhadap kebijakan perkuliahan secara daring yang diterapkan kampus. Tampilan dari Aufratia sebagaimana gambar 2.

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

Gambar 2. Tampilan Aufratia pada halaman unggah berkas

ISO 27001

ISO 27001 adalah suatu bentuk kerangka kerja standar internasional yang berisi tentang standar-standar dalam area keamanan informasi. ISO 27001 menyediakan kerangka kerja dalam lingkup penggunaan teknologi dan pengelolaan aset yang membantu organisasi memastikan bahwa keamanan informasi sudah efektif. Hal ini termasuk kemampuan akses data secara berkelanjutan kerahasiaan, dan integritas atas informasi yang dimilikinya. (*International Organization for Standardization*, 2018) (Asriyanik, 2016).

Adapun 11 klausa dari ISO 27001 (Putra et al., 2016) (Bakri & Irmayana, 2017) yaitu:

A5. *Security policy*
A6. *Organization of information security*
A7. *Asset management*
A8. *Human resources security*
A9. *Physical and environmental security*
A10. *Communications and operations management*
A11. *Access control*
A12. *Information system acquisition, development and maintenance*
A13. *Information security incident management*
A14. *Business continuity management*
A15. *Compliance*

III. METODOLOGI PENELITIAN

Penelitian ini merupakan jenis penelitian analisis deskriptif kualitatif dimana peneliti akan melakukan analisis dengan mendiskusikan tingkat kematangan Aplikasi Aufratia yang dikembangkan oleh civitas akademik UMG berdasarkan skor atau nilai yang dihasilkan Skala Likert dan dilakukan analisa pencarian akar masalah dengan menggunakan *Fishbone* Diagram. Deskripsi yang dilakukan penulis berdasarkan pada panduan dalam 11 Klausa pada ISO 27001.

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

Gambar 4. Alur Penelitian

Pengumpulan data

1. Review dokumen

Menggali informasi yang tersaji dalam teori dan latar belakang yang telah dikumpulkan dari berbagai sumber, antara lain jurnal akademik, dokumen pemerintah, dan kertas kerja atau catatan *feedback* (Periyadi, 2015).

2. Observasi

Observasi dilakukan untuk mencari data bagaimana kinerja Aufratia dalam menjalankan peranya sebagai aplikasi berbagi berkas, metode observasi memungkinkan untuk mengamati fakta dari sudut pandang *subject* (Office & Merdeka, 2005).

3. *Interview*

Metode *Interview* merupakan metode pengumpulan data dengan jalan tanya jawab dengan pengguna maupun pengembang Aufratia yang dikerjakan dengan sistematik dan berlandaskan kepada tujuan penelitian.

Analisa

1. Skala Likert

Skala likert digunakan sebagai alat ukur untuk menilai data yang telah dikumpulkan terkait *security assessment* Aufratia menggunakan 11 *klausa annex A* ISO 27001. Interval penilaian skala likert yang digunakan dalam penelitian ini sebagaimana tabel 1.

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

Tabel 1
Interval skala likert

NO	KATEGORI	PRESENTASE CHECKLIST TELAH DITERAPKAN
1	SANGAT BAIK	80% - 100%
2	BAIK	60% - 80%
3	CUKUP	40% - 60%
4	TIDAK BAIK	20% - 40%
5	SANGAT TIDAK BAIK	0% - 20%

Dari penilaian skala likert nantinya akan dibuatkan Diagram *Maturity* Level untuk lebih memberikan gambaran visual tentang interval skala likert per masing-masing klausa (Maingak & Harsono, 2018).

2. *Fishbone* Diagram

Diagram *Fishbone* atau *ishikawa*, digunakan dalam analisa pencarian *root cause* atau akar permasalahan terkait dengan keamanan dan privasi aset informasi yang dimiliki oleh Aufratia (Azis, 2017).

IV. HASIL DAN PEMBAHASAN

Pada tahap pengumpulan data ditemukan beberapa hal menarik yang dapat digunakan dalam penilaian atau assessment sistem keamanan aufratia antara lain :

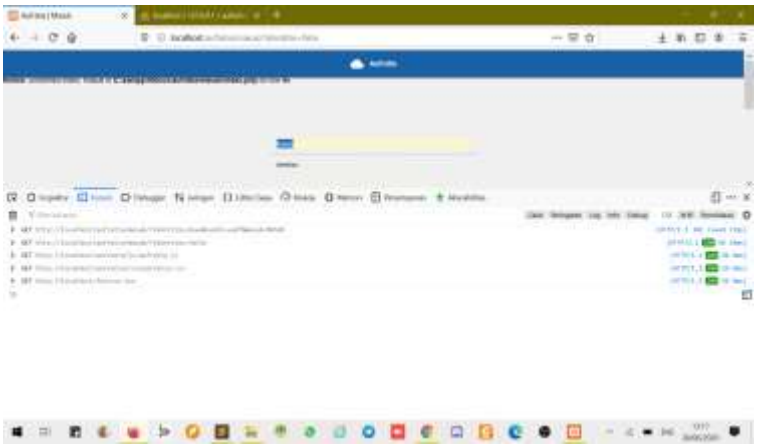
1. Dalam dokumen *Software Requirement Specification* (SRS) aufratia, tidak membahas keamanan aufratia secara detail, terutama terkait dengan keamanan informasi pengguna, seperti autentikasi login, metode enkripsi *credential, masking request* dan kebijakan akses langsung ke berkas yang disimpan pengguna. Keamanan aufratia dibahas dalam SRS merupakan keamanan general/ umum tekait *client* dan *server*.
2. Catatan kertas kerja analisa *source code*/ kode sumber dan database aufratia memiliki *vulnerability*/ kerentanan tinggi karena :
    1) Database tidak terenkripsi, sehingga sangat rentan pencurian data pribadi melalui *sql injection*.
    2) Folder penyimpanan berkas terdapat dalam *doc root*/ folder publik, sehingga berkas dapat diakses secara bebas oleh siapapun selain pengguna (tanpa *login*).

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

3) Berkas yang diunggah diperbolehkan dalam bentuk/ tipe berkas .php. Karena folder penyimpanan berkas terdapat dalam folder publik, sangat dimungkinkan ada yang dengan sengaja mengunggah berkas bertipe .php berisi *script* untuk melakukan *run console* atau untuk mengambil data pengguna dari database.

3. Hasil Observasi aplikasi menunjukan bahwa Aufratia tidak melakukan *masking* setiap HTTP *Request Method* yang menyebabkan informasi yang dikirim user tidak terlindungi sama sekali, hal ini memberikan peluang pencurian data melalui *scanning package html* sederhana hingga pembobolan menggunakan teknik *hacking* seperti *protocol layer attack*.



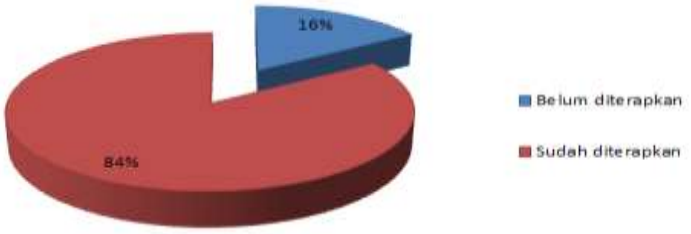
Gambar 5. Hasil observasi

4. *Interview* yang dilakukan dalam menggali informasi dan *feedback* baik dari pengguna maupun penggembang, menghasilkan sebuah saran dari pengguna yakni "*Integrasi Single Sign On* dengan akun *google*", sedang dari pengembang didapatkan pernyataan bahwa Aufratia belum memikirkan tahapan keamanan pengguna, saat ini pengembangan hanya dalam fase minimum *running* sesuai fungsi utamanya.

Berdasarkan 11 *klausa annex A* ISO 27001, disusun *checklist* dan daftar pertanyaan yang akan ditanyakan kepada responden, yaitu pengembang dan pengguna Aufratia. Dari daftar pertanyaan yang telah ditanyakan, ternyata hanya 16% saja yang sudah diterapkan oleh Aufratia, sedangkan sebesar 84% belum diterapkan oleh Aufratia sebagaimana pada gambar 4.

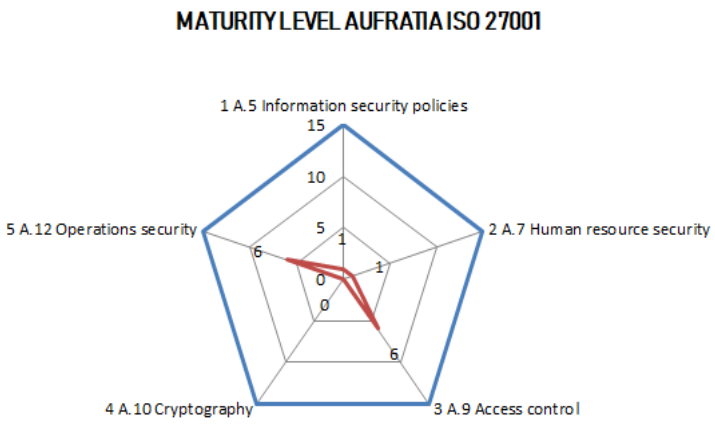
http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732



Gambar 6
Presentase hasil interview

Dari data hasil *interview*, dilakukan analisis menggunakan Skala Likert. Analisis dilakukan terhadap 5 klausa yang dinilai memegang peranan paling penting dalam keamanan informasi. Hasil analisis menunjukkan bahwa hanya 2 klausa yang berada dalam kategori cukup dengan prosentase 40%, sedangkan 3 klausa lainnya berada dalam kategori sangat tidak baik dengan nilai persentase antara 0%-6,67% sebagaimana pada gambar 5.

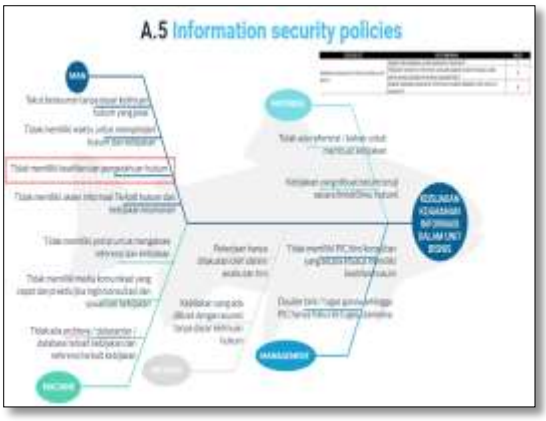


Gambar 7
Maturity level

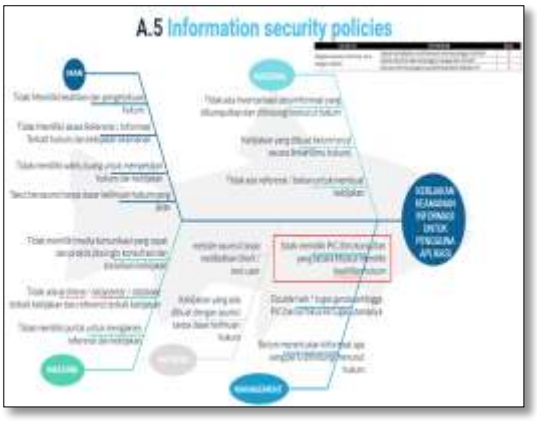
Analisa selanjutnya adalah untuk mengetahui penyebab utama atau akar permasalahan dalam keamanan informasi Aufratia. Analisis ini menggunakan diagram fishbone dan dilakukan untuk masing-masing klausa yang sudah dianalisa menggunakan skala likert pada tahap sebelumnya. Diagram fishbone dari analisa Aufratia sebagaimana gambar 8, 9, 10, 11, 12.

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

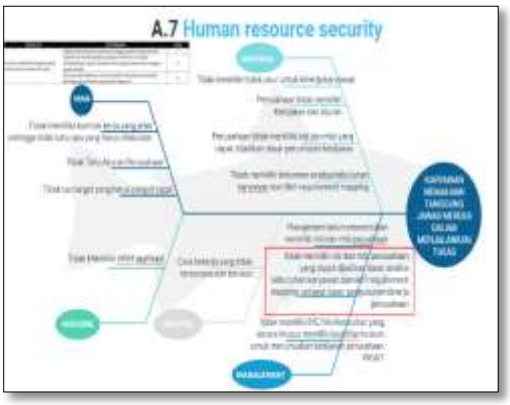
E-ISSN : 2722-4759
P-ISSN : 2722-4732



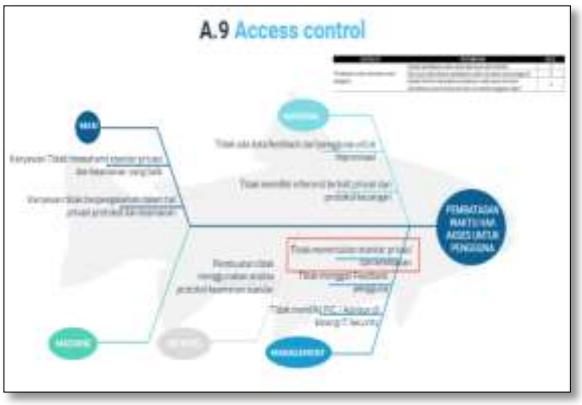
Gambar 8
Diagram Fishbone untuk Klausa
Information Security Policies



Gambar 9
Diagram Fishbone untuk Klausa
Information Security Policies



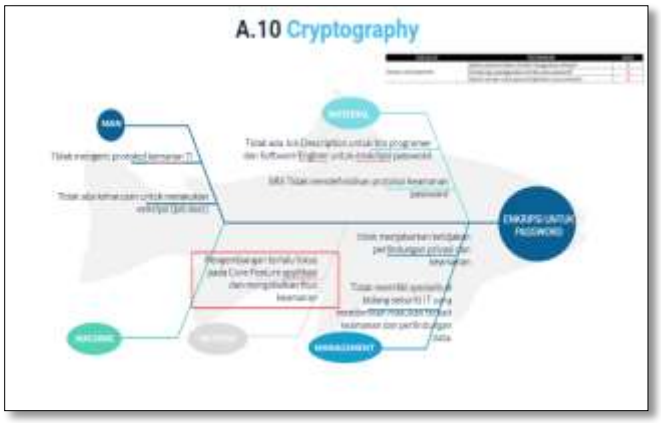
Gambar 10
Diagram Fishbone untuk Klausa
Human Resource Security



Gambar 11
Diagram Fishbone untuk Klausa
Information Security Policies

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732



Gambar 12
Diagram Fishbone untuk Klausa Cryptography

V. KESIMPULAN

Aplikasi Aufratia masih belum memenuhi Standar ISO 27001. perlindungan informasi yang sangat minimal dan hampir tidak ada, menjadikan aufratia tidak layak menjadi aplikasi *release* dan saat ini lebih pantas untuk dijadikan applikasi *beta version (tested)*. Permasalahan utama pada unit bisnis Aufratia disebabkan pada sisi management, Management belum mempunyai visi misi sehingga kesulitan menerjemahkan kebijakan ke dalam *job desc*, dan hal itu mengakibatkan tidak adanya target kerja dan pemetaan kebutuhan staf, terutama tim legal dan tim *IT Security*.

DAFTAR PUSTAKA

Asriyanik. (2016). Penilaian Keamanan Sistem Informasi Akademik Universitas Muhammadiyah Sukabumi Dengan Menggunakan ISO 27001. Jurnal Ilmiah Sains Dan Teknologi, 6(2), 501–506.

Azis, M. S. (2017). Audit Keamanan Informasi pada PDAM Tirta Tarum Karawang Menggunakan Indeks KAMI SNI ISO/ IEC 27001:2009 dan Fishbone. Jurnal Inovasi Informatika, II(2), 41–57.

Bakri, M., & Irmayana, N. (2017). Analisis Dan Penerapan Sistem Manajemen Keamanan Informasi Simhp Bpkp Menggunakan Standar Iso 27001. Jurnal Tekno Kompak, 11(2), 41. https://doi.org/10.33365/jtk.v11i2.162

Eloksari, E. A. (The J. P. (2020). Indonesian Telkom Record Data Traffic Surges as People Start Staying Home. https://www.thejakartapost.com/news/2020/03/24/ indonesian-telcoms-record-data-traffic-surges-as-people-start-staying-home.html

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787

E-ISSN : 2722-4759
P-ISSN : 2722-4732

International Organization for Standardization. (2018). ISO / IEC 27000:2018. -. https://www.iso.org/standard/73906.html

Kemp, S. (Datareportal). (2020). Digital 2020: Indonesia - Data Reportal - Global Digital Insight. -. https://datareportal.com/reports/digital-2020-indonesia

Maingak, A. Z., & Harsono, L. D. (2018). Information Security Assessment Using Iso / Iec 27001 : 2013 Standard. Trikonomika, 17(1), 28–37. http://journal.unpas.ac.id/index.php/trikonomika/article/view/1138/618

Office, E., & Merdeka, S. (2005). Penilaian Keamanan Jaringan Menggunakan Standar ISO/IEC 27001 Pada Kantor Redaksi Harian Suara Merdeka. Journal of Information System, 1–10.

Periyadi, P. (2015). Analisis Resiko Teknologi Informasi Sistem Terintegrasi iGracias Berbasis Risk Assesment Menggunakan SNI ISO-IEC 27001-2009 Periyadi. Jurnal Teknologi Informasi, 2(3), 70–78.

Putra, A. A., Nurhayati, O. D., & Windasari, I. P. (2016). Perencanaan dan Implementasi Information Security Management System Menggunakan Framework ISO/ IEC 27001. Jurnal Teknologi Dan Sistem Komputer (JTsiskom), 4(1), 60.

http://dx.doi.org/10.30587/mahasiswamanajemen.v1i2.1787