APLIKASI MANAJEMEN RISIKO KEAMANAN INFORMASI BERDASARKAN ISO/IEC 27001:2013 (STUDI KASUS: PT. XYBASE INDONESIA)

Erwin Asriyar [1)], Apridelson Manurung [2)]

Erwin Asriyar [1)]

Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl.Asem 2 No 22, Cipete Jakarta Selatan
http://stti.i-tech.ac.id/

Apridelson Manurung [2)]

Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl.Asem 2 No 22, Cipete Jakarta Selatan
http://stti.i-tech.ac.id/

ABSTRAK

Informasi adalah salah satu aset penting dan sangat berharga bagi suatu organisasi. Salah satu elemen penting dalam tata kelola organisasi yang baik adalah keamanan informasi. Keamanan informasi adalah penjagaan informasi dari seluruh ancaman yang mungkin terjadi dalam upaya untuk memastikan atau menjamin kelangsungan bisnis. Risiko dapat timbul dimana saja dalam organisasi perusahaan, baik proses, aktivitas, unit bisnis dan lokasi geografis yang berada.

Banyak yang beranggapan bahwa untuk pengelolaan risiko merupakan tanggung jawab pimpinan tertinggi perusahaan dan ternyata pada kenyataannya bahwa setiap unit dalam perusahaan memiliki tanggung jawab untuk pengedalian risiko. Standar ISO/IEC 27001:2013 telah dipersiapkan untuk menyediakan persyaratan, pemeliharaan,
peningkatan yang berlanjut tentang masalah manajemen keamanan informasi. Metode penggunaan standar ISO/IEC 27001:2013 memberikan rekomendasi berdasarkan hasil evaluasi yang dilakukan, bagaimana mengambil tindakan untuk menghadapi risiko yang akan datang. Aplikasi manajemen risiko ini dapat digunakan sebagai "tools" untuk membantu mengelola informasi demi keamanan risiko yang dihadapi perusahaan.

Kata Kunci: ISO/IEC 27001:2013, Manajemen Risiko, Keamanan Informasi

1. PENDAHULUAN

Aktivitas suatu perusahaan akan senantiasa berubah dan berkembang seiring dengan perubahan teknologi dalam lingkungan perusahaan. Tuntutan perubahan dan swsssspeningkatan kemampuan perusahaan menjadi peluang yang baik bagi perusahaan atau bahkan dapat memunculkan risiko bagi perusahaan tersebut. Jika perubahan dilakukan ke arah yang positif sesuai dengan tujuan perusahaan maka perusahaan akan mendapatkan keuntungan yang baik, jika tidak maka perusahaan akan hanya mendapatkan kerugian baik finansial, waktu dan sebagainya. Karena hal ini, perusahaan harus berusaha keras untuk melakukan manajemen risiko yang baik. Risiko dapat timbul dimana saja dalam perusahaan, baik proses, aktivitas, unit bisnis dan bahkan lokasi geografis yang berbeda. Banyak yang beranggapan bahwa untuk pengelolaan manajemen risiko merupakan tanggung jawab pimpinan tertinggi perusahaan dan ternyata pada kenyataannya bahwa setiap unit dalam perusahaan harus dapat mengenali risiko yang dapat menghambat pencapaian tujuan. Banyak cara untuk melakukan pendekatan untuk proses mengenali, menilai dan mencegah munculnya risiko tersebut, salah satunya adalah dengan menggunakan standar ISO 27001:2013. Standar internasional ini telah dipersiapkan untuk menyediakan persyaratan, implementasi, pemeliharaan, dan peningkatan yang berlanjut tentang masalah manajemen keamanan

informasi. Adaptasi sistem manajemen keamanan informasi merupakan keputusan yang strategis terhadap risiko yang dihadapi perusahaan.

PT. Xybase merupakan perusahaan penyedia layanan teknologi informasi seperti jasa sistem perangkat lunak dan sistem integrasi untuk mendapatkan solusi terhadap kebutuhan organisasi. PT. Xybase didirikan pada tahun 1992 dengan visi menjadi perusahaan dengan basis teknologi informasi yang unggul dan inovatif demi menjaga peningkatan proses pelayanan.

Informasi dihasilkan dari keterkaitan beberapa elemen, misalnya berupa informasi data (softcopy dan hardcopy), sumber daya manusia (people), wujud fisik (physical), perangkat lunak (software), perangkat keras (hardware) dan lain sebagainya. Informasi yang dihasilkan digunakan sebagai data untuk menghasilkan informasi baru oleh pihak-pihak yang berkepentingan. Pengelolaan berbagai informasi yang ada di PT. XYBASE, masih menggunakan sistem manual (pencatatan data) dan penggunaan informasi yang ada masih belum dianggap aman. Hal tersebut disebabkan karena belum terpenuhinya kriteria CIA (Confidentally, Integrity, Availability) yang menjadi fungsi pada pengelolaan keamanan informasi dan belum tersedianya kebijakan yang dapat digunakan untuk mencegah dan mengantisipasi adanya berbagai risiko yang tidak diharapkan. Dalam penelitian ini, ISO 27001:2013 digunakan dasar untuk racangan aplikasi sistem manajemen keamanan informasi. Hal-hal tersebut akan berguna untuk memberikan arahan manajemen dan dukungan untuk keamanan informasi yang sesuai dengan kebutuhan bisnis, peraturan dan hukum yang berlaku.

2. METODOLOGI PENELITIAN

Metodologi penelitian merupakan proses untuk mendapatkan data yang akan digunakan untuk keperluan penelitian. Sehingga metodologi yang digunakan pada pembuatan tugas akhir dalam rekayasa perangkat lunak adalah sebagai berikut:

1. Metode pengumpulan data

- *Metode studi pustaka*, dengan melakukan pengumpulan informasi dan pembelajaran terhadap berbagai macam literatur yang membahas konsep ISO 27000:2013 dan manajemen risiko.
- *Wawancara dan dokumentasi*, yang dilakukan kepada pihak perusahaan PT.XYBASE di berbagai unit divisi dengan mengajukan pertanyaan-pertanyaan yang berkaitan dengan topik.

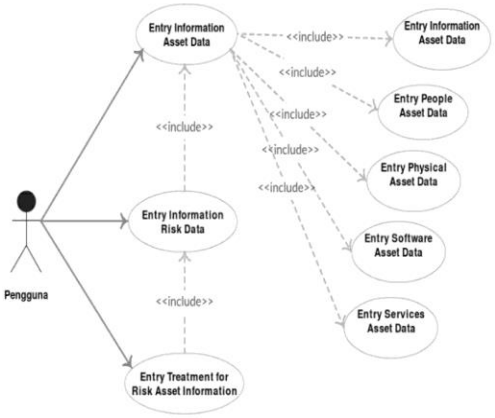
2. Metode analisis dan rancangan perangkat lunak dengan metode waterfall

- *Analisa*, pada tahap analisa dilakukan proses pengumpulan informasi yang berkaitan dengan data – data apa saja yang diperlukan dalam pembuatan aplikasi yaitu tentang data aset informasi dari perusahaan.
- *Desain* dan *Perancangan Sistem*, setelah mengetahui data aset informasi maka selanjutnya melakukan proses desain tampilan dan relasi/rancangan database yang sesuai dengan keterangan data untuk daftar aset informasi.
- *Menulis Bahasa Pemrograman*, pada tahap ini dilakukan penulisan program dengan mewujudkan rancangan desain yang dikembangkan dengan menggunakan bahasa pemograman.
- *Pengujian*, setelah melakukan penulisan bahasa pemograman dan kemudian dilakukan pengujian terhadap sistem yang telah dibuat apakah telah sesuai dengan yang rancangan sebelumnya.
- *Implementasi*, proses implementasi dilakukan dengan menggunakan aplikasi ini pada perusahaan sesuai divisi terkait.

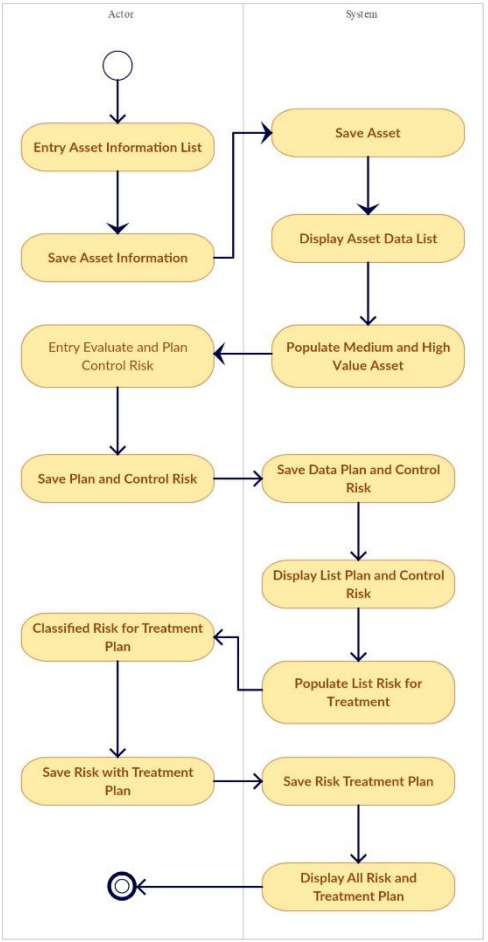
3. RANCANGAN DAN IMPLEMENTASI

3.1 Rancangan Umum

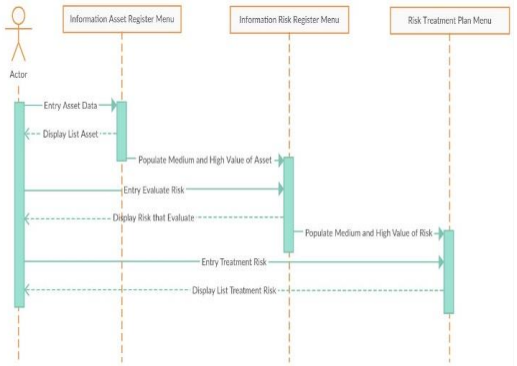
Proses sistem mencakup pengelolaan risiko pada (Information Asset Register) sesuai dengan metode ISO 27001:2013, yaitu pemilihan data aset informasi (Information Asset Register) menjadi data risiko informasi (Information Risk Register). Dari hasil data risiko informasi (Information Risk Register) tersebut akan menghasilkan rencana pengelolaan risiko (Risk Treatment Plan) yang dapat menjadi acuan perusahaan PT. XYBASE dalam mengambil kepssssutusan demi pengelolaan manajemen risiko. Dari hasil analisis kebutuhan ini didapatkan spesifikasi sistem yang akan dikembangkan



Gambar 1. *Use Case Diagram*



Gambar 2*. Activity Diagram*



Gambar 3*. Sequence Diagram*

Pada *use case*, *activity* dan *sequence diagram* menjelaskan aktivitas awal pada menu *Information Asset Register* adalah mengisi data-data asset *Information*, *People*, *Physical*, *Software* dan *Services*. Kemudian sistem akan menampikan data-data yang telah di *input*. Data tersebut akan disaring berdasarkan klasifikasi dan nilai dari *CIA* asset tersebut yang bernilai "*medium*" dan "*high*". Pada saat pengguna (*actor*) memilih menu *Information Risk Register* maka pengguna (*actor*) akan mengisi informasi tentang ancaman dan kemungkinan yang terjadi pada setiap daftar risiko. Kemudian sistem akan menampilakan daftar risiko tersebut beserta nilai tingkat risikonya dan kemudian akan sistem akan filter risiko yang akan diterima atau tidak. Daftar risiko-risiko yang akan *diterima* atau bernilai "*medium*" atau "*high*" akan masuk pada menu *Risk Treatment Plan*. Pada Menu ini pengguna (*actor*) akan mengisi bagaimana cara menanggulangi risiko tersebut berdasarkan *ISO/IEC 27001:2013*, rencana detail, divisi yang bertanggung jawab dan kapan rencana itu akan dikerjakan/selesai.

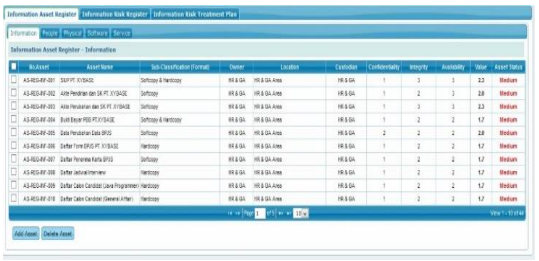
3.2 Implementasi Sistem

Agar aplikasi ini dapat berjalan dengan baik dibutuhkan hardware yang memadai. Untuk kebutuhan sistem membutuhkan spesifikasi seperti dibawah ini:

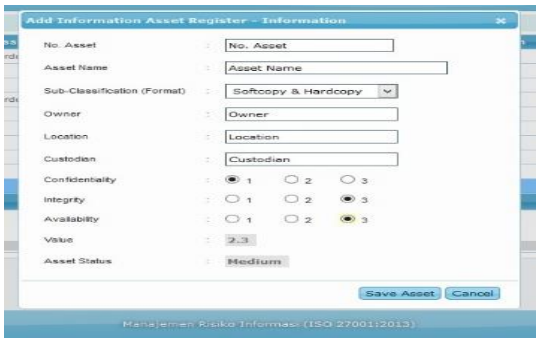
- CPU/Laptop dengan Physical memory (RAM) > 4Gb, Hard disk terisisa minimal 15 GB, CPU Processor 2.3 GHz minimum
- LCD Screen (Monitor PC)
- Mouse

- Keyboard

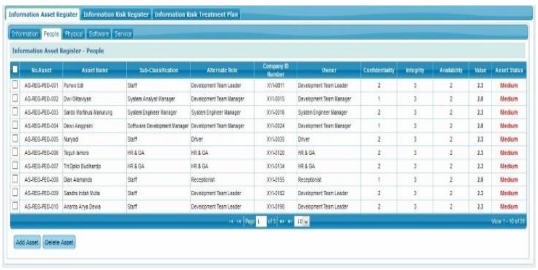
3.3 Hasil Implementasi



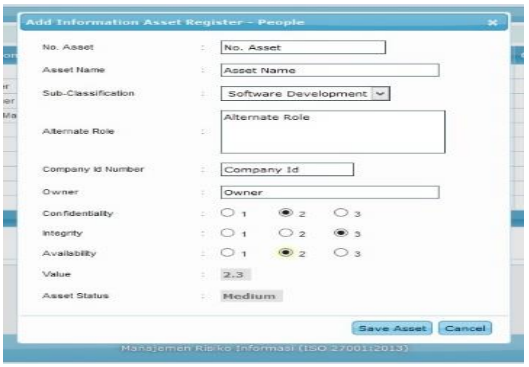
Gambar 4. Tampilan Menu Information Asset Register - Information



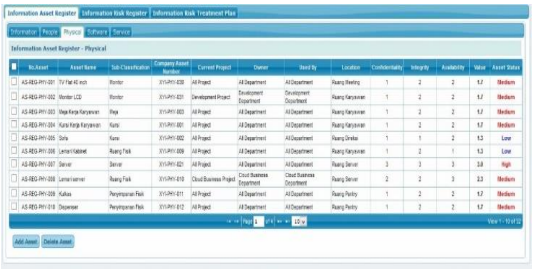
Gambar 5. Tampilan input data Asset Information



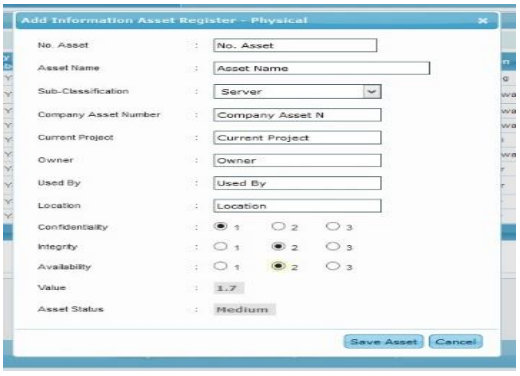
Gambar 6. Tampilan Menu Information Asset Register – People



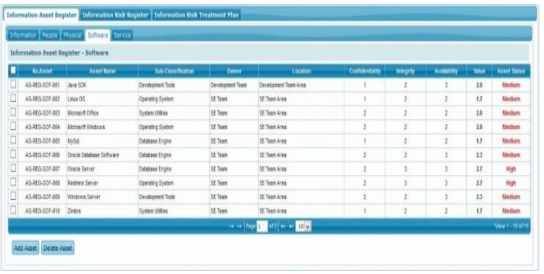
Gambar 7. Tampilan input data Asset People



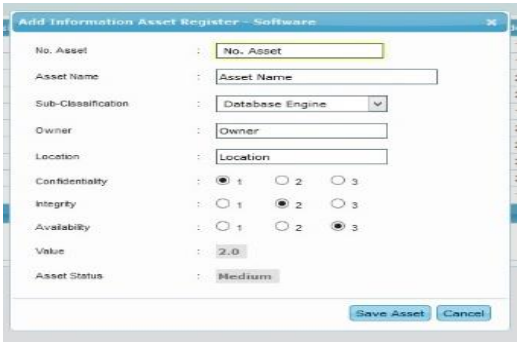
Gambar 8. Tampilan Menu Information Asset Register - Physical



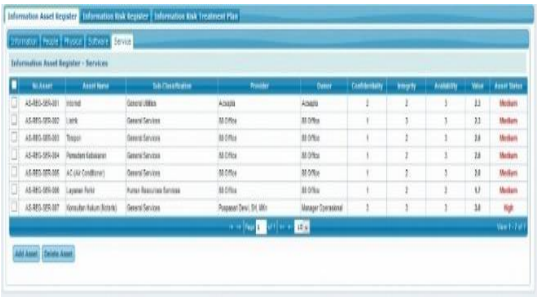
Gambar 9. Tampilan input data Asset Physical



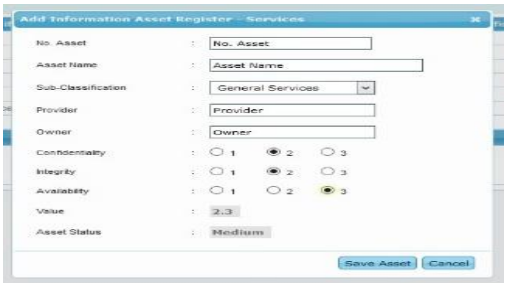
Gambar 10. Tampilan Menu Information Asset Register - Software



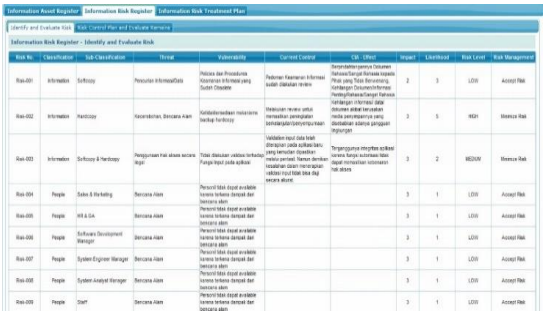
Gambar 11. Tampilan input data Asset Software



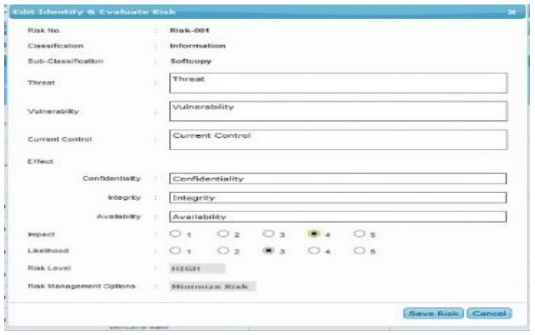
Gambar 12. Tampilan Menu Information Asset Register - Services



Gambar 13. Tampilan input data Asset Services

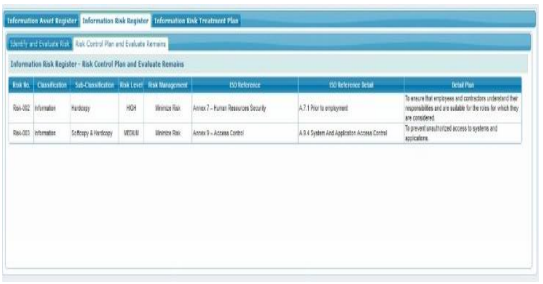


Gambar 14. Tampilan Identify and Evaluate

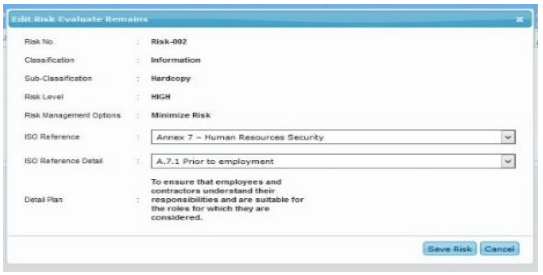


Risk

Gambar 15. Tampilan input data risk identify and evaluate



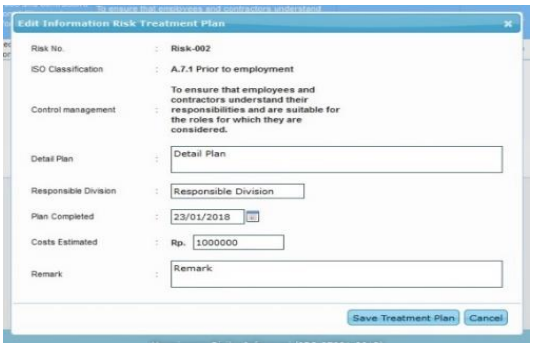
Gambar 16. Tampilan Identify and Evaluate Risk Remains



***Gambar 17**. Tampilan input data evaluate risk*

remain

Gambar 18. Tampilan Menu Risk Treatment Plan



Gambar 19. Tampilan input data risk treatment

3.4 Pengujian Sistem

Kualitas pengujian sebuah aplikasi akan dapat terjamin apabila dalam masa pengembangannya telah dilakukan serangkaian tahapan uji coba yang benar dan sesuai dengan rencana dan strategi uji coba tersebut. Dalam hal ini, maka akan dilakukan pengujian *blackbox* testing. Uji coba *blackbox* testing dipilih karena persyaratan fungsional perangkat lunak yang telah dibuat harus sesuai tujuan pembangunan aplikasi. Berikut ini merupakan beberapa pengujian yang dilakukan dengan metode *blackbox*.

Tabel 1. Black Box Testing

NO	NAMA	HASIL YANG DIHARAPKAN	HASIL PENGUJIAN	STATUS
1	*Add new data Asset Informatio n*	Sistem akan menerima masukan data asset *information* dan menghitung nilai *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	Sistem telah menyimpan data asset *information* dan telah memberi nilai kolom *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	***Valid***
2	*Delete Asset Informatio n*	Sistem akan menghapus daftar aset *information* sesuai dengan daftar yang dipilih.	Sistem telah berhasil menghapus data aset *information* sesuai dengan daftar yang dipilih.	***Valid***
3	*Add new data Asset People*	Sistem akan menerima masukan data asset *people* dan menghitung nilai *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	Sistem telah menyimpan data asset *people* dan telah memberi nilai kolom *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	***Valid***
4	*Delete Asset People*	Sistem akan menghapus daftar aset *people* sesuai dengan daftar yang dipilih.	Sistem telah berhasil menghapus data aset *people* sesuai dengan daftar yang dipilih.	***Valid***
5	*Add new data Asset Physical*	Sistem akan menerima masukan data asset *physical* dan menghitung nilai *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	Sistem telah menyimpan data asset *physical* dan telah memberi nilai kolom *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	***Valid***
6	*Delete Asset Physical*	Sistem akan menghapus daftar aset *physical* sesuai dengan daftar yang dipilih.	Sistem telah berhasil menghapus data aset *physical* sesuai dengan daftar yang dipilih.	***Valid***
7	*Add new data Asset Software*	Sistem akan menerima masukan data asset *software* dan menghitung nilai *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	Sistem telah menyimpan data asset *software* dan telah memberi nilai kolom *value* dan *asset status* sesuai dengan nilai *CIA* yang dipilih.	***Valid***
8	*Delete Asset Software*	Sistem akan menghapus daftar aset *software* sesuai dengan daftar yang dipilih.	Sistem telah berhasil menghapus data aset *software* sesuai dengan daftar yang dipilih.	***Valid***
9	*Add new data Asset Services*	Sistem akan menerima masukan data asset *services* dan menghitung nilai *value* dan *asset*	Sistem telah menyimpan data asset *services* dan telah memberi nilai kolom *value* dan *asset status* sesuai dengan	***Valid***

		status sesuai dengan nilai *CIA* yang dipilih.	nilai *CIA* yang dipilih.	
10	*Delete Asset Services*	Sistem akan menghapus daftar aset *services* sesuai dengan daftar yang dipilih.	Sistem telah berhasil menghapus data aset *services* sesuai dengan daftar yang dipilih.	***Valid***
11	*Populate Medium* dan *High Value* pada menu *Information Asset Register*	Sistem akan mengelompokkan daftar risiko dengan nilai asset *medium* dan *high* berdasarkan klasifikasi aset pada menu *Information Asset Register*	Sistem telah berhasil mengelompokan (*filter)* daftar risiko yang bernilai *medium* dan *high.*	***Valid***
12	*Edit* daftar risiko	Sistem akan menampilkan data detail tiap risiko sehingga data tersebut dapat ditambahkan dengan nilai dampak dan kemungkinan yang terjadi sehingga sistem akan menghitung nilai level risiko dan menentukan opsi penanganan risiko.	Sistem telah menampilkan detail tiap risiko sesuai yang dipilih, telah berhasil menyimpan data dampak dan kemungkinan yang terjadi pada risiko tersebut serta berhasil menentukan nilai level risiko dan opsi penanganan risiko.	***Valid***
13	*Populate Medium* dan *High Value* pada menu *Risk Treatment Plan*	Sistem akan mengelompokkan daftar risiko dengan nilai risiko *medium* dan *high* atau mengelompokkan data berdasarkan opsi penanganan risiko.	Sistem telah berhasil mengelompokan (*filter)* daftar risiko yang bernilai *medium* dan *high* atau opsi penanganan yang bernilai "*Minimize Risk*"	***Valid***
14	*Edit* daftar risiko untuk pengendalian berdasarkan *ISO/IEC 27001*	Sistem akan menampilkan daftar risiko sehingga data tersebut dapat ditambahkan dengan opsi penanganan risiko berdasarkan referensi dokumen *ISO/IEC 27001*	Sistem telah menampilkan daftar tiap risiko telah berhasil menyimpan opsi penanganan pada risiko tersebut.	***Valid***

4. KESIMPULAN DAN SARAN

4.1 Kesimpulan

Berdasarkan analisa dan implementasi yang dilakukan, dapat disimpulkan bahwa:

1. Pembangunan dan implementasi aplikasi telah berhasil dilakukan sesuai dengan tujuan dan sesuai dengan tahap perancangan.
2. Dengan adanya aplikasi Manajemen Risiko Informasi berdasarkan ISO/IEC 27001:2013 maka pendaftaran aset informasi menjadi mudah dan rapi (terkelompokan).
3. Dapat membantu menghitung tingkat risiko dan mengelompokkan daftar risiko yang sedang terjadi pada perusahaan. Karena hal tersebut maka akan dapat menanggulangi risiko terhadap klasifikasi aset yang bernilai risiko tinggi.

4.2 Saran

Selain menarik beberapa kesimpulan, juga disertakan saran-saran yang bisa menjadi pertimbangan dalam pengembangan aplikasi kedepan, antara lain:

1. Aplikasi ini dapat dijadikan bersifat komersial, sehingga memungkinan untuk penambahan menu yang perlu, seperti menu untuk menambahkan klasifikasi/penggolongan aset, menu print report dan lain sebaginya.
2. Pada sistem apliasi belum hak akses pengguna dimana hal ini sangat dibutuhkan untuk menjaga keamanan data tentang perusahaan.

3. Jika hak akses sudah dibangun maka ada baiknya jika aplikasi ini dibuat secara online sehingga pengguna dapat menggunakan dimanapun berada selama terkoneksi dengan internet.
4. Penambahan fungsi *reporting* untuk mempermudah pengguna melakukan *print* formulir yang dapat dibagi berdasarkan divisi yang bertanggung jawab.

5. DAFTAR PUSTAKA

Ahmed, Md. Z. (2014). *Which one is better - JavaScript or jQuery* (Vols. 3). Hyderabad: Mahaveer Institute of Science and Technology, Department of SE

Bharthan, A. & Bharathan, D. (2014). International Journal of Computer Applications. RelationalJSON, An Enriched Method to Store and Query JSON Records (Vols. 98). India: Delhi

Crockford, D (2008). *JavaScript: The Good Parts* (1st ed). California: O'Reilly Media, Inc

Elmasri, Ramez. B. Navathe, Shaamkant (2004): Fudamentals of Database system, 4thn Edition. London:Addison Wesley

Hidayat, M. N, (2011): "Kajian Tata Kelola Keamanan Informasi Berdasarkan Information Security Management System (ISMS) ISO 27001:2005 untuk Outsourcing Teknologi Informasi Pada PT. Kereta Api Indonesia (Persero)," Program Studi Magister Teknologi Informasi Fasilkom UI, Jakarta

ISACA, in Certified Information Security Manager (2011) : Review Manual 200, USA, ISACA, pp. 38-29

Leo Willyanto Santoso (2014), Perancangan dan Pembuatan Aplikasi ERD Generator Notasi ORM dari Skrip Basis Data Oracle berbasis J2EE, Jawa Timur: Universitas Kristen Petra

McLeod, R., Jr & Schell, G. P. (2007): Management Information Systems (10th Edition). New Jersey: Pearson Prentice Hall.

Informasi Data," Jurnal Transformatika, vol. VI, no. 2, p. 80.

Whitman, M.E., & Mattord, H.J, (2010): Management of Information Security, Third Edition, Boston: Course Technology

O'Brien, J. A. (2007). Pengantar Sistem Informasi, edisi ke-12. Terjemahan Dewi dan Deny. Jakarta: Salemba Empat

Rosa A.S – M.Shalahuddin (2011), Rekayasa Perangkat Lunak, Penerbit modula

Safaat, N. H. (2012). *Android: Pemrograman Aplikasi Mobile Smartphone dan Tablet PC* (revisi ed.). Bandung: Informatika

Sri Dharwiyanti, Romi Satria Wahono, (2003): "Pengantar Unified Modeling Language (UML)" Kuliah Umum IlmuKomputer.Com

Syafrizal, M (2007): Standar Sistem Manajemen Keamanan Informasi, Yogyakarta, Seminar Nasional Teknologi, p. 10

Udayakumar, R., & Thooyamani, K.P., & Khanaa, V. (2013). A Comparison of J2EE and .NET as Platforms for Developing E-Government Applications (Vols. 7). Bharath: Bharath University

Wijaya, S.F, & Darudiato, S (2009): ERP (Enterprise Resource Planning & Solusi Bisnis (1st Edition), Yogyakarta: Graha Ilmu.

Zhang, X. (2010). Assessing Students' Structured Programming Skills with Java (Vols. 9) Florence, Alabama: University of North Alabama

Penulis adalah
1. Dosen pada Sekolah Tinggi Teknologi Informasi NIIT I-Tech
2. Alumni Sekolah Tinggi Teknologi Informasi NIIT I-Tech