Prototype Information Security Risk Assessment Tool Berbasis Lotus Notes Dalam Rangka Penerapan Sistem Manajemen Keamanan Informasi ISO 27001

Hadi Syahrial
Universitas Budi Luhur, Jakarta
E-mail : hadisyahrial@gmail.com

ABSTRAK

Makalah ini membahas tentang pengembangan prototype sebuah aplikasi yang dapat digunakan untuk menyimpan dan melakukan penilaian risiko keamanan informasi yang diberi nama Information Security Risk Assessment Tool yang disesuaikan dengan kebutuhan dalam rangka implementasi Sistem Manajemen Keamanan Informasi (SMKI) ISO 27001. Protoype ini dibuat dengan menggunakan Lotus Notes agar mudah dalam penyimpanan, penelusuran, dan kolaborasi. Dengan sistem ini diharapkan dapat membantu dalam melakukan penilaian risiko keamanan informasi menjadi lebih efisien dan efektif.

Kata kunci : Risk Assessment, SMKI, Lotus Notes, Manajemen Risiko Keamanan Informasi, ISO 27001

1. PENDAHULUAN

Informasi merupakan aset yang sangat penting untuk dijaga kerahasiaan, keutuhan, dan ketersediannya atau yang dikenal dengan CIA (Confidentiality, Integrity, Availability). Ketiga hal ini dapat terancam. Mulai dari ancaman yang paling umum seperti malware sampai ancaman berupa pencurian informasi rahasia dan lain-lain. Ancaman-ancaman ini bisa bersumber dari dalam maupun dari luar. Ancaman-ancaman yang masih bersifat potensial ini setiap saat dapat berubah menjadi serangan nyata apabila kelemahan-kelemahan keamanan yang terdapat pada perangkat keras, perangkat lunak, gedung, bisnis proses, dan lain-lain tidak segera diatasi.

Ancaman-ancaman ini dapat menimbulkan risiko kerugian mulai dari yang kecil sampai yang besar seperti hilangnya reputasi organisasi atau perusahaan. Oleh karena itu risiko keamanan informasi perlu dikelola dengan baik. Salah satu tahap yang harus dilakukan dalam manajemen risiko keamanan informasi adalah melakukan penilaian risiko. Dengan dikembangkannya sebuah tool menggunakan Lotus Notes untuk melakukan penilaian risiko diharapkan dapat lebih mudah dikerjakan secara bersama-sama dalam sebuah tim dan dapat disimpan untuk keperluan penelusuran.

2. LANDASAN TEORI

Informasi merupakan salah satu asset bagi institusi bisnis dan non bisnis yang sangat berharga. Kehilangan informasi rahasia dapat menyebabkan rusaknya reputasi dan kerugian finansial yang besar. Oleh karena itu keamanan informasi merupakan kebutuhan bisnis perusahaan dari sekedar untuk memberikan jaminan atas terkelolanya risiko bisnis sampai dengan penciptaan keunggulan bersaing bagi perusahaan.

Menurut Alan Calder [1] dalam bukunya A Business Guide to Information Security disebutkan “Information Security is, according to the internationally recoqnized code of information security best practices, ISO 17799:2005, the preservation of the confidentiality, integrity and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also can be involved”.

Keamanan informasi adalah menurut praktek-praktek terbaik dalam bidang keamanan informasi yang sudah dikenal secara internasional yaitu ISO 17799:2005, perlindungan terhadap kerahasiaan, keutuhan dan ketersediaan informasi, hal lain yang dapat ditambahkan seperti keaslian, pertanggung jawaban, tidak dapat disangkal dan kepercayaan.

ISO 27001 merupakan dokumen standar Sistem Manajemen Keamanan Informasi (SMKI) atau Information Security Managemen System (ISMS) yang memberikan gambaran secara umum mengenai apa saja yang harus dilakukan oleh sebuah perusahaan dalam usaha mereka mengimplementasikan sistem manajemen keamanan informasi di organisasi.

Standar ISO 27001dikembangkan dengan pendekatan proses yaitu sebagai suatu model bagi penetapan, penerapan, pengoperasian, pemantauan, tinjau ulang (review), pemeliharaan dan peningkatan suatu SMKI. Pendekatan proses mendorong organisasi menekankan pentingnya:

1. Pemahaman persyaratan keamanan informasi organisasi dan kebutuhan terhadap kebijakan serta sasaran keamanan informasi
2. Penerapan dan pengoperasian kontrol untuk mengelola risiko keamanan informasi dalam konteks risiko bisnis organisasi secara keseluruhan
3. Pemantauan dan tinjau ulang kinerja dan efektivitas SMKI, dan
4. Peningkatan berkelanjutan berdasarkan pada pengukuran tingkat ketercapaian sasaran Model PLAN – DO – CHECK – ACT (PDCA)

PLAN: Menetapkan kebijakan SMKI, sasaran, proses dan prosedur yang relevan untuk mengelola risiko dan meningkatkan keamanan informasi agar memberikan hasil sesuai dengan keseluruhan kebijakan dan sasaran.
DO: Menerapkan dan mengoperasikan kebijakan-kebijakan SMKI, kontrol, proses dan prosedur-prosedur.
CHECK: Mengkaji dan mengukur kinerja proses terhadap kebijakan, sasaran, praktek-praktek dalam menjalankan SMKI dan melaporkan hasilnya kepada manajemen untuk ditinjau efektivitasnya.
ACT: Melakukan tindakan perbaikan dan pencegahan, berdasarkan hasil evaluasi, audit internal dan tinjauan manajemen tentang SMKI atau kegiatan pemantauan lainnya untuk mencapai peningkatan yang berkelanjutan.

Untuk implementasi SMKI, organisasi perlu menerapkan manajemen risiko sebagai salah satu persyaratan. ISO mengeluarkan standar ISO 27005 yang dinamakan Information technology – Security techniques – Information security risk management. Standar ini memberikan pedoman untuk Manajemen Risiko Keamanan Informasi dalam suatu organisasi yang mendukung khususnya persyaratan Sistem Manajemen KeamananInformasi (SMKI) sesuai dengan ISO/lEC 27001.

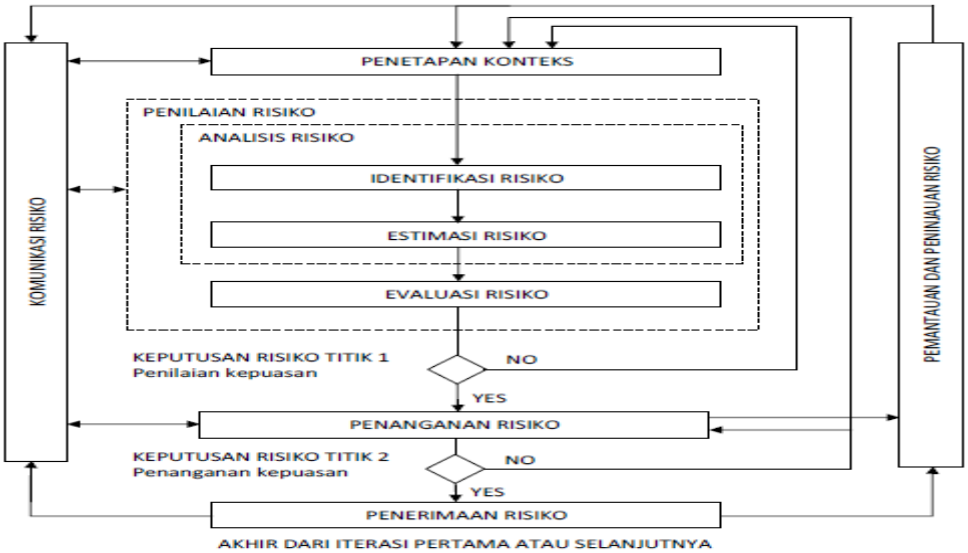
ISO/IEC 27001 menetapkan bahwa pengendalian yang diterapkan dalam ruang lingkup, batasan-batasan dan konteks SMKI harus berbasis risiko. Penerapan proses manajemen risiko keamanan informasi dapat memenuhi persyaratan ini. Ada banyak pendekatan dimana proses dapat berhasil dilaksanakan dalam suatu organisasi. Organisasi harus menggunakan apa pun pendekatan yang paling sesuai dengan keadaan mereka untuk setiap aplikasi yang spesifik dari proses.

Manajemen risiko keamanan informasi harus menjadi proses yang berkelanjutan. Proses ini harus menetapkan konteks, menilai resiko dan penanganan resiko menggunakan rencana perlakuan untuk melaksanakan rekomendasi dan keputusan. Manajemen risiko menganalisa apa yang bisa terjadi dan apa konsekuensi yang mungkin bisa, sebelum memutuskan apa yang harus dilakukan dan kapan, untuk mengurangi risiko ke tingkat yang dapat diterima.

Risiko manajemen keamanan informasi adalah potensi bahwa ancaman yang diberikan akan mengeksploitasi kerentanan aset atau kelompok aset dan dengan demikian menyebabkan kerugian kepada organisasi [2].

Dari definisi di atas, risiko keamanan informasi terkait erat dengan aset atau kelompok aset yang dimiliki organisasi atau perusahaan. Aset adalah sesuatu yang bernilai bagi organisasi dan karenanya membutuhkan perlindungan. Untuk identifikasi aset itu harus diingat bahwa sistem informasi terdiri dari lebih dari perangkat keras dan perangkat lunak.

Kerangka kerja manajemen risiko keamanan informasi menurut ISO 27005 adalah sebagai berikut:



Gambar 2.1 Kerangka kerja manajemen risiko keamanan informasi [3]

Seperti yang digambarkan pada Gambar 2.1, proses manajemen risiko keamanan informasi merupakan proses yang berulang untuk penilaian risiko dan/atau kegiatan perlakuan risiko. Pendekatan berulang untuk melakukan penilaian risiko dapat meningkatkan kedalaman dan rincian dari penilaian pada setiap pengulangan. Pendekatan berulang ini memberikan keseimbangan yang baik antara meminimalkan waktu dan usaha yang dihabiskan dalam mengidentifikasi kontrol, sementara masih memastikan bahwa risiko tinggi dinilai dengan tepat.

Setelah mengetahui probabilitas dan dampak dari suatu risiko, maka kita dapat mengetahui nilai suatu risiko [3]. Dengan demikian risk bisa dihitung dengan menggunakan rumus berikut:

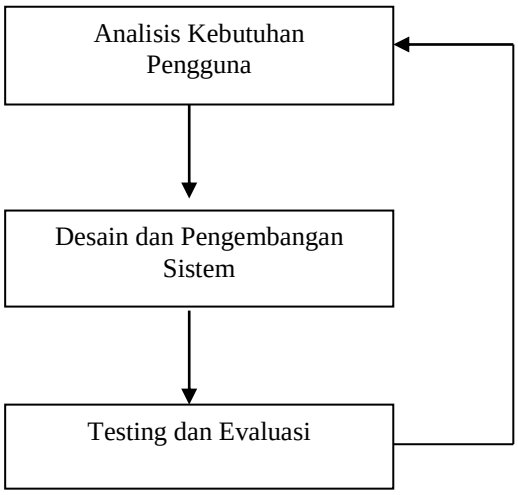
Risk = Impact x Probability.

Nilai risiko untuk berbagai risiko dapat dibandingkan antara satu dengan lainnya untuk mengetahui tingkat kepentingan masing-masing risiko.

3. METODE PENELITIAN

Metode yang digunakan untuk mengembangkan Information Secutity Risk Assessment Tool adalah metode eksperimental yaitu dengan tahapan-tahapan pengembangan sistem sebagai berikut yaitu: tahap analisis kebutuhan, tahap desain dan pengembangan prototipe, dan tahap testing dan evaluasi.

Tahapan-tahapan yang dilakukan dalam pengembangan sistem adalah [4]:
1. Analisis Kebutuhan Pengguna
2. Desain dan Pengembangan Sistem
3. Testing



Gambar III.1 Tahapan penelitian

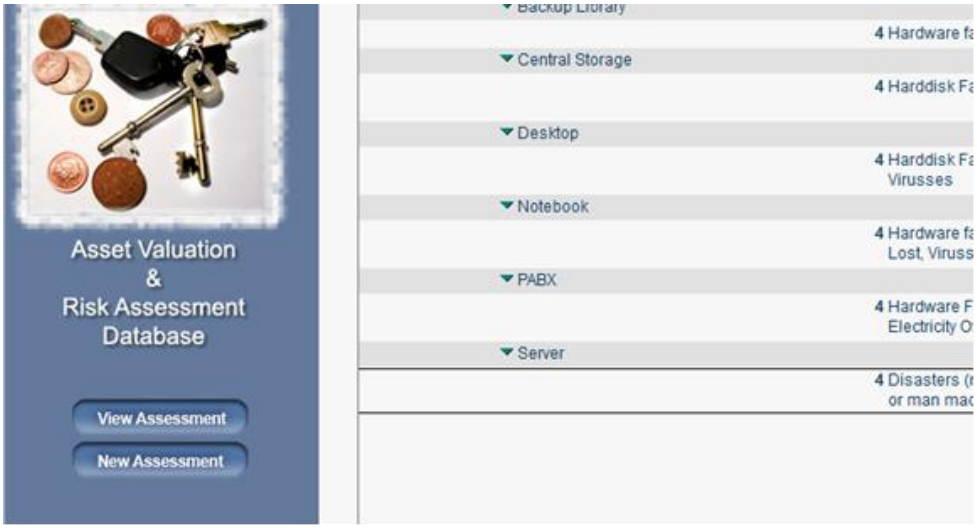
4. HASIL DAN PEMBAHASAN

4.1 Analisis Kebutuhan Pengguna

Pada tahap analisis kebutuhan telah dilakukan wawancara tentang kebutuhan fungsional dan non fungsional dari sistem yang akan dibangun. Sistem ini dikembangkan dengan menggunakan Lotus Notes. Dari hasil analisis kebutuhan ini didapatkan spesifikasi sistem yang akan dikembangkan.

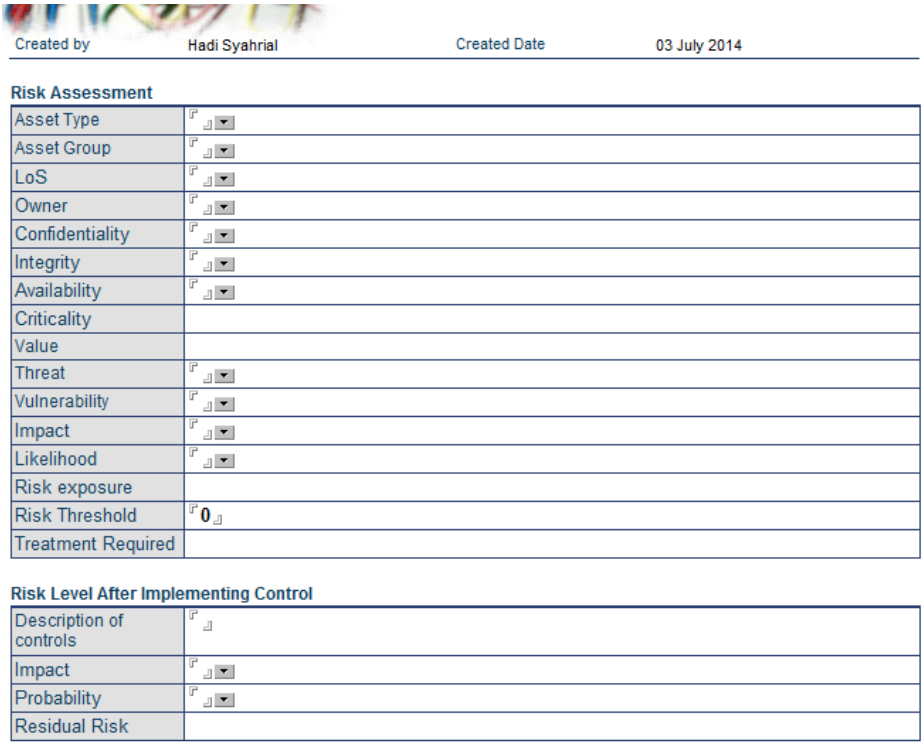
4.2 Desain dan Pengembangan Sistem

Pada tahap desain dan pengembangan sistem telah dihasilkan sebuah prototipe Information Secutity Risk Assessment Tool. Prototipe sistem ini memiliki tampilan antarmuka pengguna seperti gambar di bawah ini:



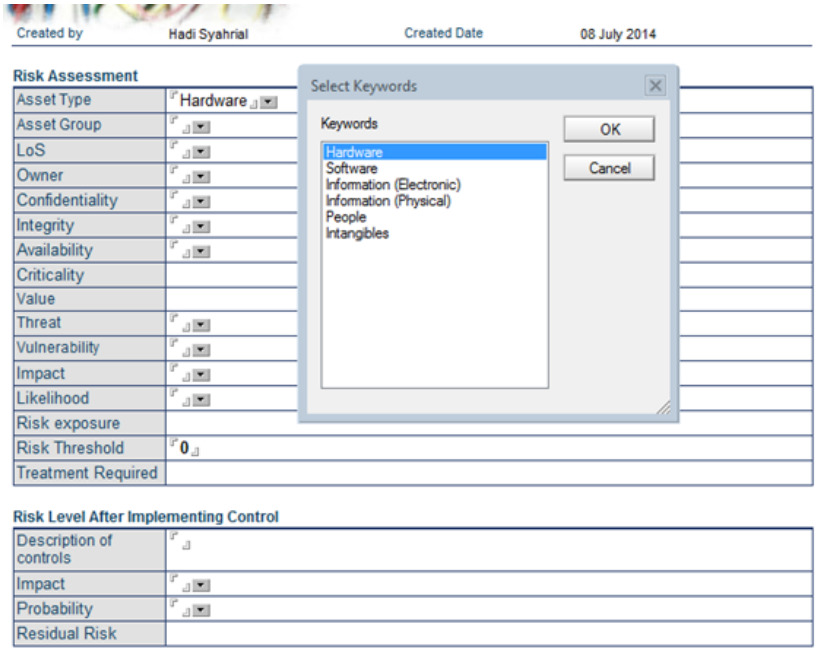
Gambar 4.1 Antarmuka pengguna

Dari antarmuka pengguna ini terdapat dua pilihan yang dapat dilakukan oleh pengguna yaitu: *View Assessment* dan *New Assessment.* Apabila tombol *New Assessment* di tekan maka akan muncul sebuah formulir yang harus diisi seperti gambar di bawah ini.



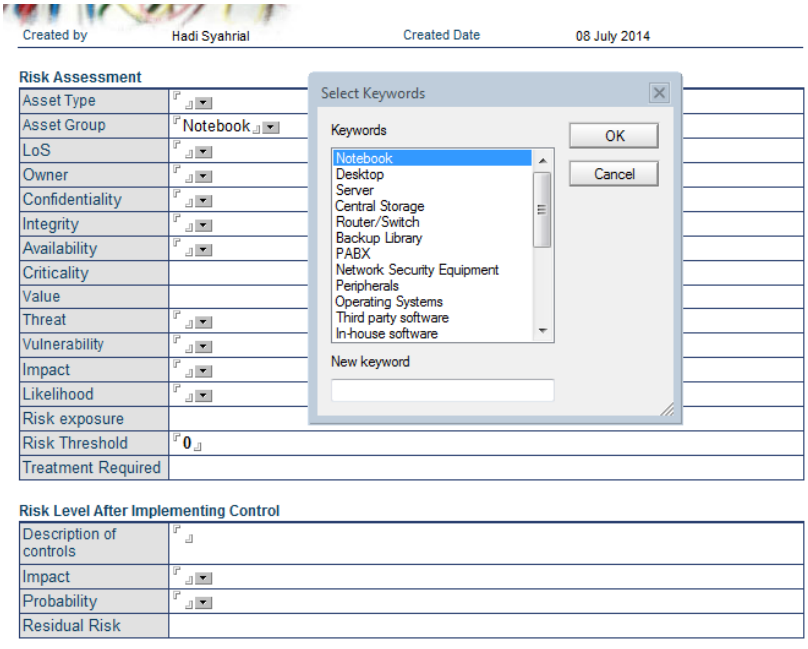
Gambar 4.2 Formulir New Assessment

Untuk *Asset Type* sudah tersedia pilihan dimana pengguna harus memilih salah satu jenis aset yang akan dinilai risikonya.



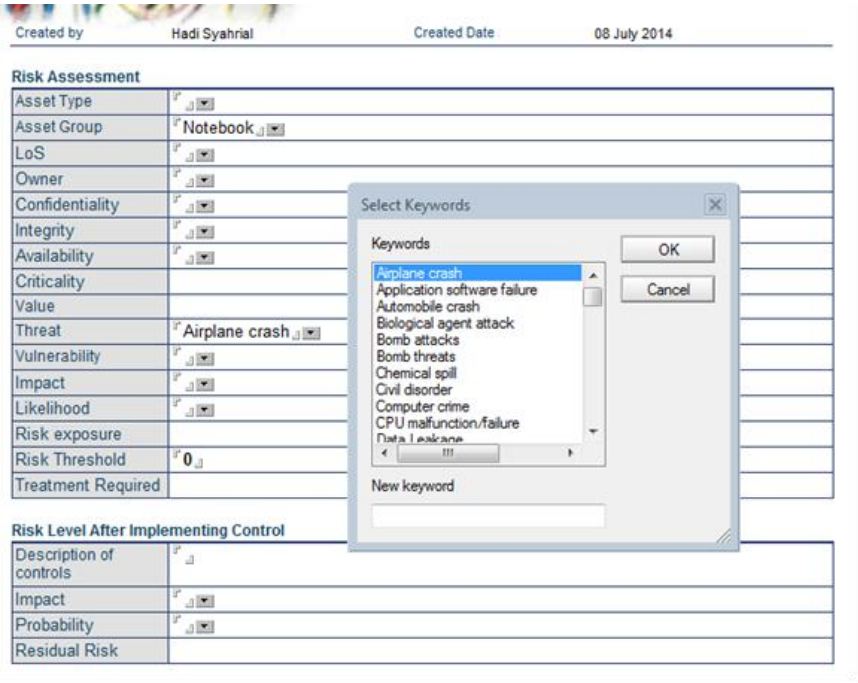
Gambar 4.3 *Asset Type*

Contoh *field* lain yang perlu diisi adalah *Asset Group*. Pada *Asset Group* sudah tersedia pilihan sehingga memudahkan pengguna untuk memilih.



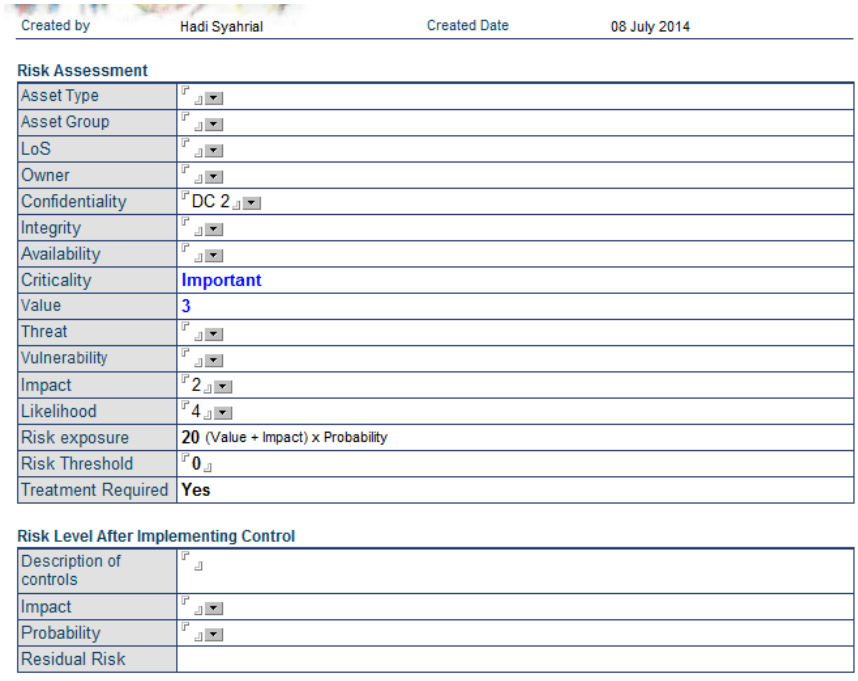
Gambar 4.4 Asset Group

Pilihan lain yang juga sudah tersedia adalah untuk *Threat* yang bisa dilihat pada gambar di bawah ini.



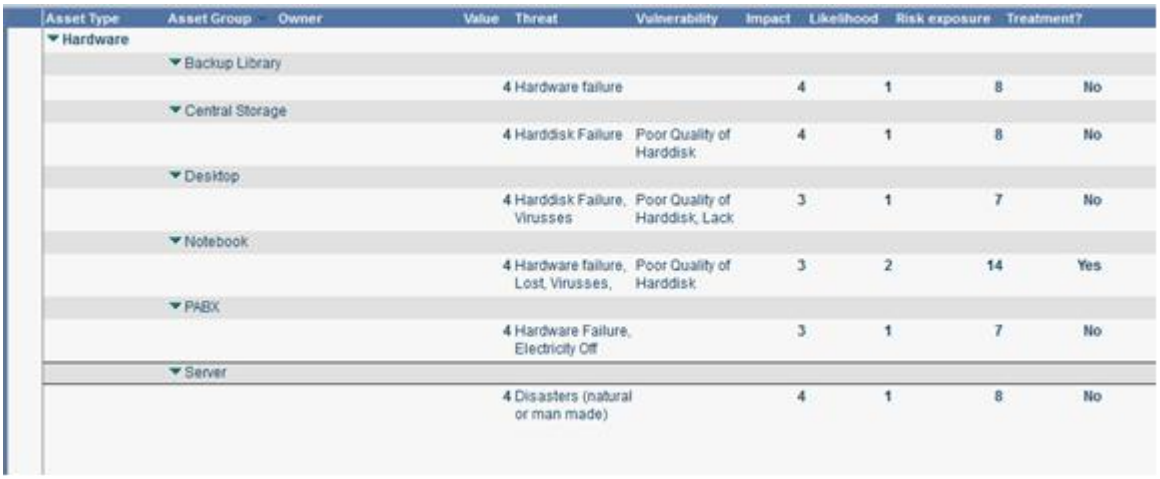
Gambar 4.5 *Threat*

Langkah berikutnya dalam melakukan penilaian risiko adalah memasukkan nilai-nilai value, impact, dan likehood. Setelah nilai-nilai ini dimasukkan maka akan muncul hasil risiko secara otomatis. Seperti terlihat pada gambar di bawah ini.



Gambar 4.6 *Risk exposure*

Gambar di bawah ini adalah *View Assessment* yang merupakan daftar dari penilaian risiko untuk setiap aset yang sudah dinilai.



Asset Type	Asset Group	Owner	Value	Threat	Vulnerability	Impact	Likelihood	Risk exposure	Treatment?
Hardware									
	Backup Library								
			4	Hardware failure		4	1	8	No
	Central Storage								
			4	Harddisk Failure	Poor Quality of Harddisk	4	1	8	No
	Desktop								
			4	Harddisk Failure, Virusses	Poor Quality of Harddisk, Lack	3	1	7	No
	Notebook								
			4	Hardware failure, Lost, Virusses,	Poor Quality of Harddisk	3	2	14	Yes
	PABX								
			4	Hardware Failure, Electricity Off		3	1	7	No
	Server								
			4	Disasters (natural or man made)		4	1	8	No

Gambar 4.7 *View Assessment*

4.3 Testing dan Evaluasi

Untuk memastikan prototipe ini sudah sesuai dengan kebutuhan pengguna maka perlu dilakukan pengujian dan evaluasi terhadap sistem ini. Pengujian ini dinamakan *User Acceptance Test* (UAT).

5. PENUTUP

Dengan menggunakan metode pengembangan sistem telah dihasilkan sebuah prototipe Information Security Risk Assessment Tool berbasiskan Lotus Notes. Sistem ini telah dapat digunakan oleh pihak-pihak yang terlibat dalam penerapan ISO 27001. Sistem serupa dapat dikembangkan dengan menggunakan *platform* yang berbeda seperti menggunakan .NET.

DAFTAR PUSTAKA

[1] Calder, Alan, A Business Guide to Information Security, Kogan Page, 2005
[2] ISO 27005: Information technology – Security techniques – Information security risk management (Terjemahan).
[3] Vasile Dumbravă, Vlăduț - Severian Iacob, "Using Probability – Impact Matrix in Analysis and Risk Assessment Projects," *Journal of Knowledge Management, Economics and Information Technology*, December. 2013.
[4] Rajendra Ganpatrao Sabale, Dr. A.R. Dani, "Comparative Study of Prototype Model For Software Engineering With System Development Life Cycle," IOSR Journal of Engineering (IOSRJEN), ISSN: 2250-3021 Volume 2, Issue 7(July 2012), PP 21-24

Hak Cipta