Perancangan Sistem Informasi Manajemen Risiko berdasarkan ISO 27001:2013 (Sistem Manajemen Keamanan Informasi)

Ibra Fadilla Nanda Sartika[1], Rahadian Bisma[2]

[1,2] S1 Sistem Informasi, Fakultas Teknik, Universitas Negeri Surabaya
[1]ibra.17051214044@mhs.unesa.ac.id
[2]rahadianbisma@unesa.ac.id

***Abstrak*— Keamanan informasi dapat didefinisikan sebagai perlindungan informasi dari akses penggunaan, pengungkapan, gangguan, modifikasi, atau penghancuran dari pengguna yang tidak sah untuk memberikan kerahasiaan, keutuhan, dan ketersediaan. Salah satu standart yang digunakan dalam keamanan sistem informasi adalah ISO 27001:2013. Salah satu proses yang ada di dalam ISO 27001:2013 adalah manajemen risiko. Manajemen risiko adalah proses untuk melakukan identifikasi, analisis, evaluasi dan pengendalian risiko yang kemungkinan akan terjadi. Untuk melakukan manajemen risiko diperlukan banyak dokumen yang dibutuhkan sehingga saat ini diperlukan suatu platform yang dapat memanajemen dokumen-dokumen tersebut. Dokumen manajemen sistem ISO 27001 adalah platform *Software as a Service* (SaaS) yang mencakup semua yang organisasi butuhkan untuk menerapkan dan memelihara standar, seperti dokumen kerangka, formulir online, kebijakan, prosedur, manajemen risiko, daftar periksa dengan pengingat otomatis, dan banyak lagi. Sistem tersebut nanti dibangun dalam *platfrom Web* dengan menggunakan framework Laravel dan perancangan sistem menggunakan UML. Proses pengembangan menggunakan metode prototipe dimulai dari pengumpulan kebutuhan sampai evaluasi, namun pada artikel ini hanya sampai desain sistem.**

***Kata Kunci*— Keamanan Sistem Infomasi, Manajemen Risiko, ISO 27001:2013, Prototipe, UML.**

I. PENDAHULUAN

Saat melakukan proses bisnis, pahamilah bahwa informasi adalah salah satu aset penting dari sebuah perusahaan. Saat membuat kebijakan strategis, para eksekutif organisasi membutuhkan informasi yang tepat yang dapat digunakan sebagai dasar untuk membuat kebijakan. Informasi juga merupakan faktor penting dalam menjaga agar bisnis tetap berjalan dalam organisasi. Untuk melindungi informasi ini, organisasi harus merancang dan menciptakan lingkungan yang aman untuk informasi tersebut. Untuk menciptakan lingkungan yang aman, organisasi perlu mewaspadai ancaman yang dapat menyerang baik dari luar maupun dari dalam. Kemampuan mengantisipasi berbagai ancaman informasi harus didasarkan pada tiga prinsip, yaitu kerahasiaan, integritas, dan ketersediaan informasi [1]. Dengan menerapkan ketiga prinsip tersebut, perusahaan dapat menciptakan keamanan informasi sesuai ISO 27001.

Dalam skenario persaingan yang ada, setiap organisasi akan berusaha untuk menambah nilai lebih bagi organisasinya. Salah satunya adalah kejujuran dan kepercayaan konsumen. Peran keamanan informasi sangat penting disini guna menjaga dan lebih meningkatkan kepercayaan konsumen. Lagi pula, perusahaan yang menawarkan layanan pelanggan mereka akan tumbuh dengan cepat jika kepercayaan pelanggan meningkat juga. Untuk memastikan keamanan informasi terhadap semua kemungkinan ancaman, perusahaan harus melakukan perlindungan keamanan informasi. Keamanan informasi didefinisikan sebagai perlindungan informasi dan sistem informasi terhadap akses, penggunaan, pengungkapan, manipulasi, perubahan atau penghancuran oleh pengguna yang tidak berwenang untuk memastikan kerahasiaan, integritas, dan kegunaan [1]. *Information Systems Testing and Control Association* (ISACA) menyatakan bahwa informasi dilindungi dari pengungkapan *(confidentiality)*, pengubahan yang tidak sah *(integrity)* dan tidak dapat diakses oleh pengguna saat diperlukan *(availability)* [2]. Keamanan informasi terdiri dari empat bidang: organisasi, orang, proses dan teknologi. Setiap perbatasan berinteraksi tidak hanya dalam hal faktor manusia tetapi juga dalam hal budaya, manajemen, arsitektur, penampilan, aktivasi dan dukungan.

Sistem Manajemen Keamanan Informasi (SMKI) berupa pengendalian, mirip dengan kebijakan, prosedur, dan struktur organisasi yang bertanggung jawab untuk menjaga keamanan informasi. Mekanisme kontrol telah dikembangkan untuk mengantisipasi ancaman terhadap sumber daya informasi dan untuk menerapkan keamanan informasi secara tepat. Salah satu standar SMKI yang ada adalah ISO/IEC 27001:2013. *ISO (International Organization for Standarization)* dan IEC *(International Electrotechnical Commission)* merupakan organisasi yang mengeluarkan berbagai standar salah satunya keamanan informasi. ISO mengeluarkan standar keamanan informasi dalam satu rumpun Sistem Manajemen Keamanan Informasi (SMKI) yang biasa dikenal sebagai standar ISO 27001.

Dengan menerapkan manajemen risiko informasi yang ada dalam SMKI dilindungi berdasarkan aspek kerahasiaan, keutuhan dan ketersediaan [3]. Proses yang dilakukan untuk identifikasi, analisis, evaluasi, dan pengendalian terhadap berbagai kemungkinan risiko yang mungkin terjadi dapat disebut sebagai manajemen risiko. Dalam penerapan ISO 27001:2013 untuk proses penerapan manajemen risiko menggunakan siklus plan-do-check-act (PDCA). Identifikasi aset perlu dilakukan organisasi untuk terhindar dari insiden keamanan informasi yang menyebabkan CIA *(confidentiality, availability,* dan *integrity)* sebuah data menjadi rusak. Proses

manajemen risiko menggunakan ISO 31000 untuk diterapkan dalam Langkah kerja.

Sistem pengelolaan dokumen dilakukan secara digital sehingga proses pendistribusian dokumen menjadi lebih cepat dan mudah. Selain menyederhanakan distribusi, proses pencarian menjadi lebih efisien karena pengguna hanya perlu memasukkan nama dokumen kontrol atau klausa yang diperlukan untuk proses pencarian. Sistem informasi manajemen dokumen memungkinkan untuk membuat tempat di mana dokumen jadi dapat dimasukkan untuk digunakan nanti oleh orang yang berwenang. Dimungkinkan juga untuk meninjau catatan perubahan dokumen dan menetapkan tanggal kedaluwarsa untuk dokumen ini. Keuntungan dari sistem informasi manajemen dokumen adalah meningkatkan produktivitas proses bisnis, meningkatkan waktu respons proses bisnis, mengurangi biaya dokumen secara keseluruhan untuk meningkatkan efisiensi penyimpanan, mengurangi biaya tambahan, mengurangi risiko kehilangan, berbagi dokumen, dokumen yang andal mekanisme keamanan. Dengan bantuan sistem manajemen dokumen (dms), suatu mekanisme dapat diterapkan untuk mengontrol otorisasi akses setiap pengguna ke dokumen yang disimpan dan dengan demikian menjamin kerahasiaan dan tingkat keamanan dokumen-dokumen ini.

Berdasarkan hasil studi kepustakaan yang telah didapatkan terdapat penelitian terdahulu seperti [4]–[6] namun dalam pembuatan aplikasi hanya pada tahap audit tidak melakukan penilaian terhadapt risiko, data risiko, dan melakukan penyimpanan pada dokumen audit. Selain itu ada beberapa aplikasi serupa yang seperti yang ditawarkan oleh comformio (advisera.com) dan dms.com namun server penyimpanananya berada pada server kedua developer tersebut. Sedangkan dalam ISO 27018 mengatur dalam kode praktik untuk perlindungan informasi identitas pribadi atau *personal identifiable information* (PII) di *cloud* publik yang bertindak sebagai pemroses PII [7]. Oleh karena itu, organisasi tidak boleh mempraktikkan penyimpanan cloud untuk dokumen yang menyimpan identitas pribadi seseorang kecuali penyimpanan berbasis cloud telah distandarisasi ke ISO 27001. Dalam aplikasi ini, diharapkan organisasi yang memiliki berbagai dokumen terkait ISO 27001 di penyimpanan internal atau server yang dapat dikelola secara mandiri oleh organisasi.

Berdasarkan permasalahan diatas, penulis menyimpulkan bahwa dibutuhkan sebuah sistem yang dapat memfasilitasi semua proses dan tahapan penyimpanan dokumen yang berhubungan dengan ISO 27001. Dokumen manajemen sistem ISO 27001 adalah platform *Software-as-a-Service* (SaaS) yang mencakup semua yang organisasi butuhkan untuk menerapkan dan memelihara standar, seperti dokumen kerangka, formulir online, kebijakan, prosedur, manajemen risiko, daftar periksa dengan pengingat otomatis, dan banyak lagi.

II. METODOLOGI

A. *Metode Pengumpulan Data*

Untuk mengerjakan artikel ini akan menggunakan metode pengembangan *prototype* dalam membangun aplikasi. *Prototype* adalah sebuah metode pengembangan perangkat lunak yang memiliki fokus pada *user experience*. Seringkali pengguna mendefinisikan serangkaian sasaran umum bagi perangkat lunak, tetapi tidak dapat mengidentifikasi kebutuhan input, pemrosesan, ataupun secara detail[8].

a. Wawancara
   Langkah awal dalam metode *prototype* adalah dengan mengumpulkan kebutuhan sistem yang akan dibuat, dengan cara mewawancarai klien ataupun pengguna. Tahapan ini dilakukan bersama klien atau pengguna untuk mendapatkan informasi tentang kebutuhan yang digunakan untuk analisis kebutuha sistem. Dalam penelitian ini wawancara dan observasi terhadap pengelolaan dokumen yang ada di perusahaan, proses penyimpanan dokumen, keamanan dokumen, dan pemilik akses terhadap suatu dokumen. Setelah melakukan wawancara dan obseravasi untuk mendapatkan informasi, langkah selanjutnya adalah menganalisis informasi yang sudah didapat untuk menyusun spesifikasi dan fungsi pada aplikasi yang akan dibuat.
b. Kepustakaan
   Dari hasil wawancara dan observasi yang didapat hanya garis besarnya saja, sehingga untuk menutupi kekurangan informasi yang didapatkan pengembang melakukan literature referensi dari berbagai jurnal untuk menutupi kekurangan informasi tersebut. Setelah referensi cukup selanjutnya akan melakukan analisis terhadap informasi yang didapat. Metode ini dilakukan dengan cara mempelajari buku maupun jurnal serta pemikiran para ahli. Informasi yang didapat dari metode ini bertujuan untuk mengetahui bagaimana cara membangun sistem informasi dokumen dokumen pada tata kelola sistem manajemen keamanan informasi.

B. *Metode Pengembangan Perangkat Lunak*

Setelah data-data berhasil dikumpulkan, dilanjutkan dengan tahapan yang digunakan dalam membangun sistem. Dalam artikel ini metode pengembangan sistem yang digunakan adalah *prototyping* berdasarkan model [9] sebagai berikut:

1. Pengumpulan kebutuhan
2. Proses desain
3. Membangun prototype
4. Evaluasi dan perbaikan

Namun dalam artikel ini akan membahas hanya sampai pada tahap proses desain.

Untuk metode perancangan sistem informasi manajemen risiko ISO 27001:2013 dalam penelitian ini akan menggunakan *Unified Modeling Language* (UML). *Unified Modeling Language* (UML) adalah bahasa berbasis gambar untuk visualisasi, spesifikasi, konstruksi dan dokumentasi sistem pengembangan perangkat lunak berbasis objek [10].

UML adalah model yang dibuat dan terkait langsung dengan berbagai bahasa pemrograman dan memungkinkan pemetaan.

1. Use Case Diagram

Diagram ini menunjukkan bagaimana sistem atau kelas bekerja dan bagaimana sistem berinteraksi dengan dunia luar. Komponen diagram use case adalah artis dan use case

2. *Activity Diagram*

Berbagai sistem yang telah dirancang, cara kerja sistem dari awal hingga akhir, dan bagaimana suatu kegiatan berakhir, dapat diilustrasikan dalam diagram ini.

3. *Sequence Diagram*

Interaksi antar objek dalam bentuk pesan digambarkan dalam diagram ini. Diagram urutan terdiri dari dimensi vertikal (waktu) dan dimensi horizontal (objek terkait) [10].

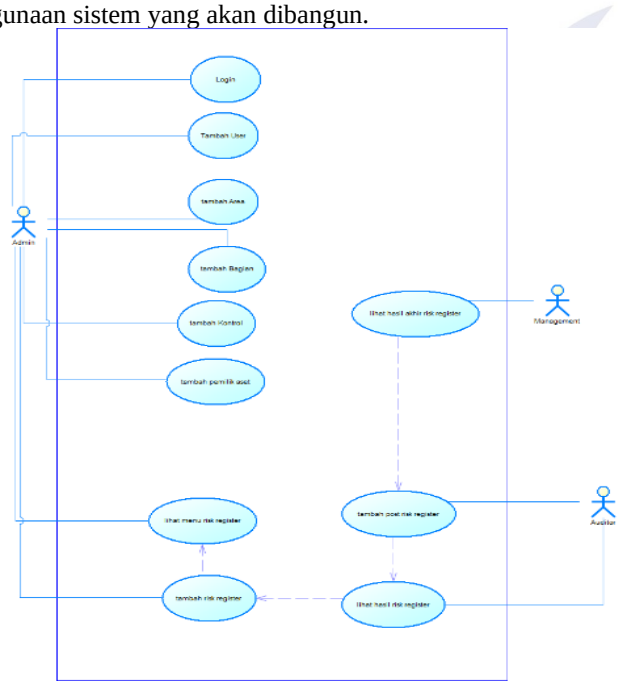
4. Class Diagram

Karena diagram kelas merupakan bentuk visual dari kelas-kelas dari suatu sistem. Diagram ini menunjukkan hubungan antar kelas dan penjelasan rinci dari setiap kelas dalam model desain (dalam pandangan logis) dari suatu sistem. Nama, atribut, dan operasi adalah area utama dari diagram kelas. Nama sebagai pengidentifikasi kelas, atribut yang menunjuk atribut data yang dimiliki suatu objek, dan operasi yang menunjuk fungsi pada suatu objek.

III. HASIL DAN PEMBAHASAN

A. *Use Case Diagram*

Use case merupakan gambaran fungsionalitas dari suatu sistem, sehingga Aktor dari sistem dapat mengerti mengenai kegunaan sistem yang akan dibangun.

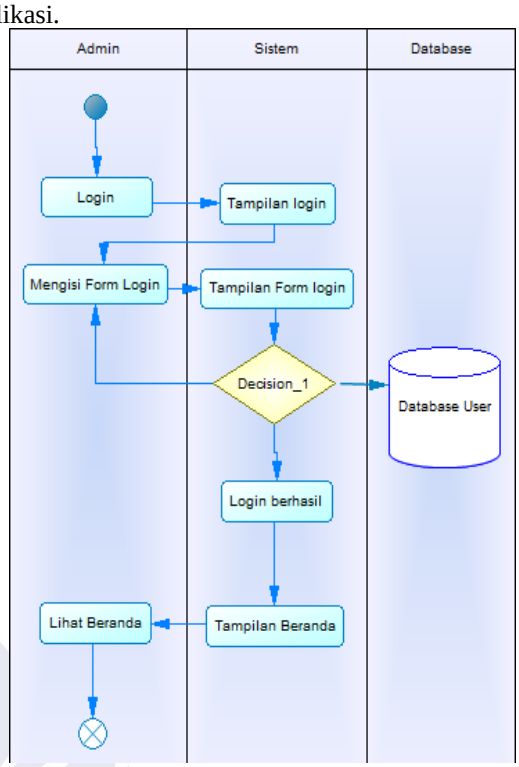


Gbr. 1 *Use Case Diagram*

Berdasarkan Gbr. 1 menjelaskan bahwa pada *use case* tersebut terdapat 3 aktor yaitu admin, manajer, dan auditor internal. Dalam pembagian hak akses, admin merupakan aktor yang memiliki hak akses terbanyak yaitu *upload* dokumen, menambah area, menambah subarea, menambah control, menambah user, menambah *risk register*, dan menambah pemilik asset. Lalu untuk admin dapat melakukan tambah *post risk register* yaitu menu untuk menilai apakah risiko yang sudah ada telah diperbaiki atau belum.

B. *Activity Diagram Login*

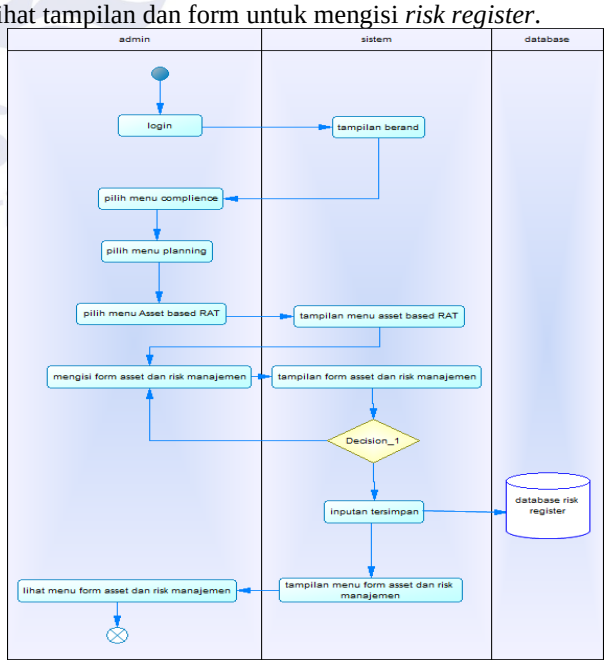
Untuk rancangan *activity diagram* admin akan melakukan *login* terlebih dahulu untuk bisa mengakses menu yang ada pada aplikasi.



Gbr. 2 Activity Diagram Login

C. *Activity Diagram Tambah Risk Register*

Setelah admin melakukan *login* admin harus memilih *complience*, setelah itu admin memilih *planning* lalu akan muncul submenu dan admin memilih *based assets RAT* untuk melihat tampilan dan form untuk mengisi *risk register*.

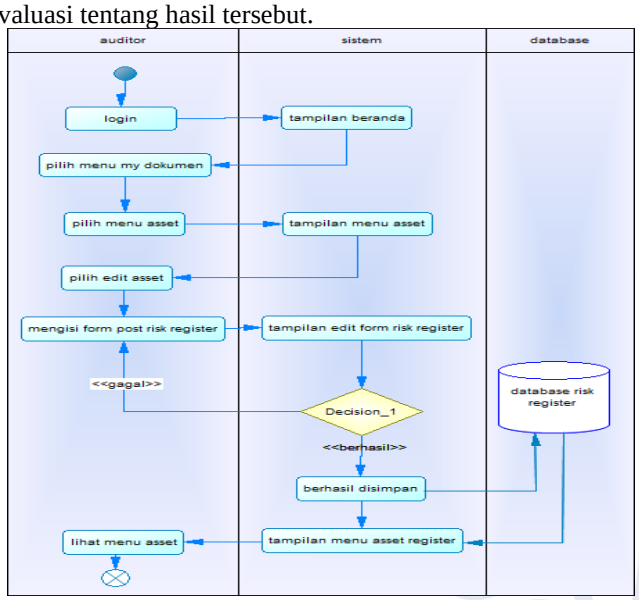


Gbr. 3 *Activity Diagram* Tambah *Risk Register*

Didalam *form risk register* terdapat *form* penilaian Risiko. User hanya perlu menentukan berapa nilai Risiko yang dimiliki oleh aset tertentu akan secara otomatis menampilkan hasilnya. Selain itu user juga dapat melakukan mitigasi Risiko dan Risiko mana yang akan ditangani terlebih dahulu jika Risiko itu muncul.

D. *Activity Diagram Tambah Post Register (Auditor)*

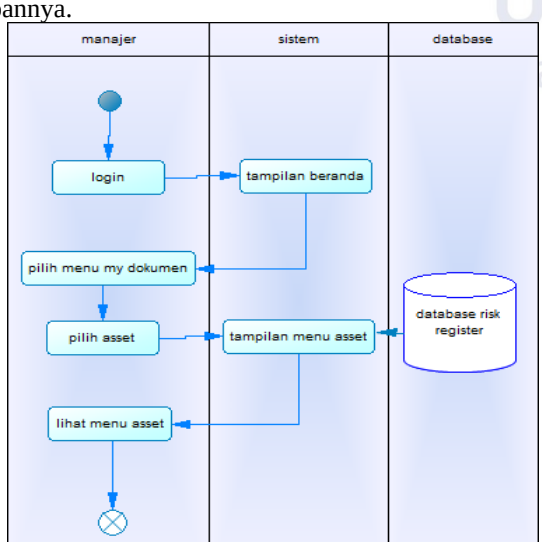
Untuk *post risk register* baru dapat diinput jika sebelummnya admin sudah melakukan inputan pada *risk register*. Karena fungsi dari *post risk register* adalah sarana penilaian yang dilakukan oleh auditor internal apakah terjadi pada *risk register* atau tidak. Jika terjadi perubahan auditor akan mengisi pada *post risk register* dan nantinya hasilnya akan dapat dilihat oleh manajemen untuk melakukan langkah evaluasi tentang hasil tersebut.



Gbr. 4 *Activity Diagram* tambah *Post Register*

E. *Activity Diagram Lihat Risk Register (Manajemen)*

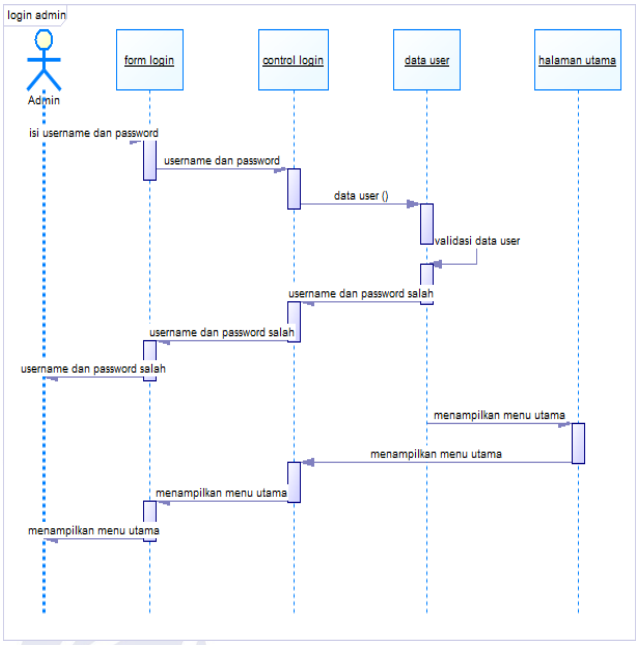
Untuk role manajemen hanya dapat melihat hasil akhir dari *risk register* yang sudah diinput oleh admin maupun *post risk* yang diinput oleh auditor sebagai bahan evaluasi kedepannya.



Gbr. 5 *Activity Diagram Lihat Risk Register*

F. *Sequence diagram Login*

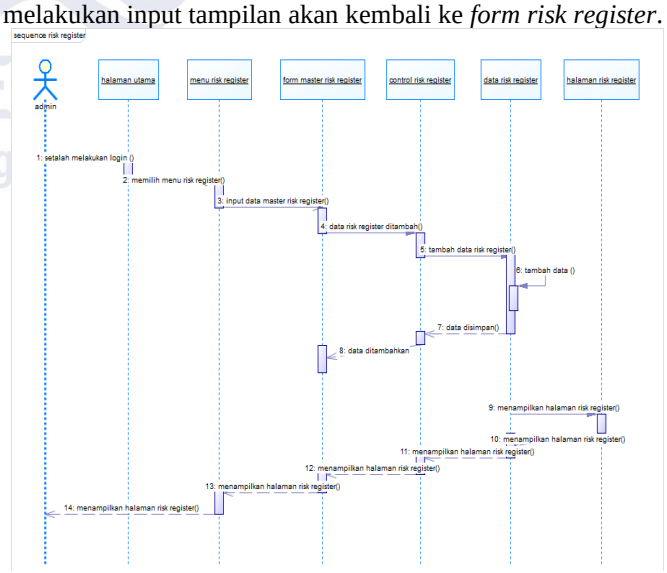
Pada sistem user harus melakukan *login* sebelum bisa mengakses menu yang tersedia. User akan mengisi form login menggunakan username dan password. Jika validasi data sebagai admin halaman utama akan menampilkan menu yang hanya dapat diakses oleh user admin. Karena setiap user akan mendapatkan hak aksesnya sendiri tergantung apa role dari user tersebut.



Gbr. 6 Sequence Diagram Login

G. *Sequence Diagram Risk Register*

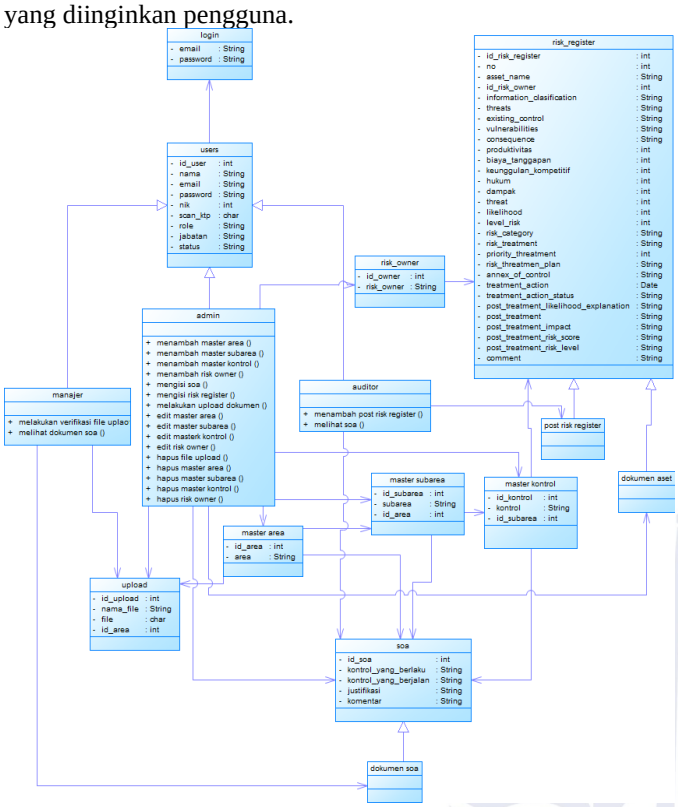
Rancangan admin dalam melakukan input *risk register*. Dalam *risk register* ada beberapa inputan yang harus diinput oleh admin. Dalam risk register akan dibagi menjadi tiga bagian yaitu identifikasi risiko, penilaian risiko, evaluasi risiko, dan *post treatment assessment*. Setelah berhasil melakukan input tampilan akan kembali ke *form risk register*.



Gbr. 7 *Sequence Diagram Risk Register*

H. *Class Diagram*

Diagram class memberikan gambaran statis dari sistem dan beberapa diagram akan menunjukkan subset class dan hubungannya. Diagram kelas membantu pengembang mendapatkan struktur sistem sebelum pengkodean dan membantu memastikan bahwa sistem memenuhi kebutuhan yang diinginkan pengguna.



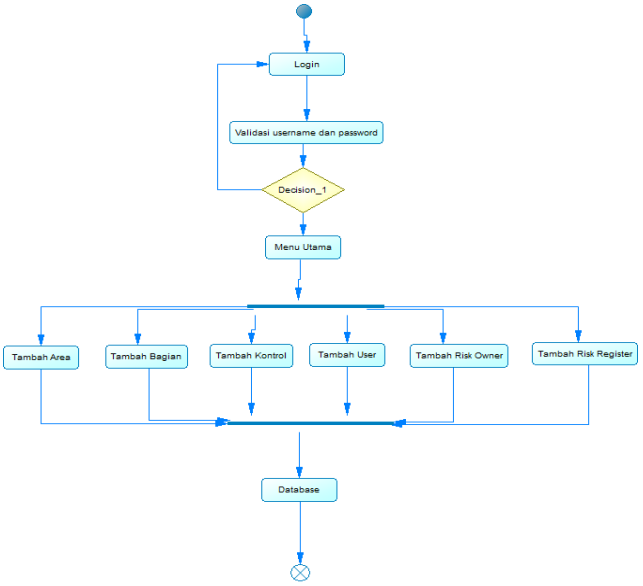
Gbr. 8 Class Diagram

I. *Statechart Diagram*

Pada diagram keadaan di bawah ini, gambarkan transisi dan perubahan keadaan dari satu state ke state lain dalam sistem sebagai akibat dari rangsangan yang diterima.. Perubahan keadaan yang dialami oleh admin adalah setelah melakukan login admin bisa untuk melakukan tambah area, tambah bagian, tambah kontrol, tambah user, tambah *risk owner*, dan tambah *risk register*.

Dokumen manajemen sistem saat ini dibutuhkan oleh berbagai organisasi baik dalam organisasi besar maupun kecil. Karena pada dokumen manajemen sistem akan mengkonversi dokumen-dokumen dari bentuk kertas menjadi bentuk digital sehingga proses distribusi dokumen menjadi lebih cepat dan mudah.

Dokumen manajemen sistem ISO 27001 adalah platform *Software-as-a-Service* (SaaS) yang mencakup semua yang organisasi butuhkan untuk menerapkan dan memelihara standar, seperti dokumen kerangka, formulir online, kebijakan, prosedur, manajemen risiko, daftar periksa dengan pengingat otomatis, dan banyak lagi.



Gbr. 9 Statechart Diagram

IV. KESIMPULAN

Berdasarkan uraian yang ada dalam latar belakang dan pembahasan sebelumnya, dapat diambil kesimpulan bahwa dokumen manajemen sistem ISO 27001 (DMS 27001) akan sangat membantu organisasi dalam melakukan distribusi dokumen seperti dokumen penilaian risiko, daftar risiko, daftar aset yang dimiliki perusahaan, evaluasi terhadap risiko, mitigasi yang dapat dilakukan oleh organisasi. Organisasi juga dapat melakukan audit internal, maupun untuk melakukan penyimpanan dokumen seperti SOP (Standar Operasional Prosedur) yang dimiliki oleh perusahaan. Selain itu tujuan dari aplikasi ini untuk memudahkan organisasi dalam meningkatkan keamanan informasinya karena basis penelitian ini merupakan ISO 27001. Adapun kesimpulan dari analisis dan perancangan sistem informasi adalah:

1. Mendapatkan gambaran tentang sistem yang sedang berjalan dan mengetahui masalah yang akan dihadapi sebagai acuan untuk membentuk sistem aplikasi yang sesuai dengan kebutuhan.
2. Dengan analisis sistem berdasarkan kebutuhan sistem yang akurat berpotensi untuk dikembangkan dan menghasilkan data yang relevan dengan sistem yang sudah ada sebelumnya. Sehingga dapat meningkatkan pelayanan terhadap organisasi kedepannya.

V. SARAN

Perancangan sistem informasi manajemen risiko berhasil dibuat sesuai dengan kebutuhan. Saran dari penelitian ini untuk mengembangkan perancangan yang sudah ada untuk diimplementasikan menjadi aplikasi dan bermanfaat bagi yang menggunakannya.

REFERENSI

[1] Matthew Gladden, *An Introduction to Information Security in the Context of Advanced An Introduction to Information Security in the Context of Advanced Neuroprosthetics*, no. February. 2017.

[2] R. Stroud, "COBIT 5 Information Security," no. November, p. 46, 2012, [Online]. Available: http://www.qualified-audit-

partners.be/user_files/COBIT5forAuditors/COBIT_5_Information_Security-2012-ISACA.pdf.

[3] ISO 27001, "Teknologi informasi – Teknik keamanan – Sistem manajemen keamanan informasi – Persyaratan Information technology – Security techniques – Information security management systems – Requirements," p. 54, 2013.

[4] A. M. Khoiri *et al.*, "RANCANG BANGUN SISTEM INFORMASI AUDIT INTERNAL BERBASIS WEB (STUDI KASUS : BALAI RISET DAN STANDARDISASI INDUSTRI SURABAYA) Dodik Arwin Dermawan," pp. 1–12, 2020.

[5] P. Ubaidillah, F. Teknologi, and D. A. N. Informatika, "DOKUMEN SISTEM PENJAMINAN MUTU INTERNAL BERBASIS WEB DI STIKOM SURABAYA," 2015.

[6] R. Wahyuono, "RANCANG BANGUN APLIKASI PENCATATAN DAN TINDAK LANJUT AUDIT INTERNAL SPI BERBASIS WEB PADA PT. PELINDO MARINE SERVICE," p. 6, 2021.

[7] H. Hoban and I. S. O. S. Order, "INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds," vol. 2014, 2014.

[8] R. S. Pressman, *Software Engineering: A Practitioner's Approach*, vol. 9781118592. 2010.

[9] P. M. Ogedebe and B. P. Jacob, "Software Prototyping : A Strategy to Use When User Lacks Data Processing Experience," vol. 2, no. 6, pp. 219–224, 2012.

[10] Y. Syafitri, "ANALISA DAN PERANCANGAN BERBASIS UML PADA SISTEM INFORMASI SIMPAN PINJAM KOPERASI SWAMITRA BANDAR LAMPUNG," pp. 68–70, 2016.