

PERANCANGAN DAN IMPLEMENTASI SISTEM MANAJEMEN RISIKO BERBASIS *WEB* UNTUK PENGELOLAAN ASET PADA PT. EKSAKTA DIGITAL GEMILAN

Susana Dwi Yulianti¹⁾ Nana Maulana²⁾

¹⁾Dosen Program studi Sistem Informasi
Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl. Asem 2 No.22, Cipete - Jakarta Selatan
<http://www.i-tech.ac.id>
susana@i-tech.ac.id

²⁾ Mahasiswa program studi system informasi
Sekolah Tinggi Teknologi Informasi NIIT I-Tech
Jl. Asem 2 No.22, Cipete - Jakarta Selatan
<http://www.i-tech.ac.id>
nanamaulana93@gmail.com

ABSTRAK

Dalam menangani risiko yang terjadi kita perlu mengambil keputusan terbaik yang terukur dan terencana. Untuk membuat rencana atau keputusan ketika risiko itu terjadi adalah dengan manajemen risiko. Manajemen risiko adalah pendekatan terstruktur untuk mengelola ketidakpastian yang berkaitan dengan ancaman, dengan cara mengidentifikasi potensi sumber kerugian, mengukur konsekuensi keuangan dari kerugian yang terjadi, dan menggunakan kontrol untuk meminimalkan aktual kerugian atau konsekuensi keuangan. Aplikasi sistem manajemen risiko yang menerapkan proses-proses berdasarkan standar best practice, standar yang digunakan dalam pembuatan aplikasi sistem manajemen risiko adalah NIST SP 800-30 Revision 1 berbasis web untuk penerapan manajemen risiko. Dengan adanya sistem manajemen risiko yang dibuat pihak perusahaan memiliki pengelolaan aset yang aman serta dapat mengurangi ancaman dan risiko yang terjadi di masa yang akan datang.

Kata Kunci: Risiko, Manajemen Risiko, NIST SP 800-30 Revision 1

1. PENDAHULUAN

Latar Belakang

Dalam kehidupan sehari-hari, banyak manfaat yang dapat diperoleh dari hadirnya teknologi informasi. Saat ini dunia telah berkembang sangat cepat. Perkembangan tersebut rasanya tidak dipisahkan dengan kemajuan di bidang perkembangan teknologi informasi. Teknologi informasi adalah sarana dan prasarana (*hardware, software, useware*) sistem dan metode untuk memperoleh, mengirimkan, mengolah, menafsirkan, menyimpan, mengorganisasikan, dan menggunakan data secara bermakna. Data yang tersebut bisa digunakan untuk keperluan bisnis dalam pengambilan keputusan. Pengambilan keputusan salah satunya dilakukan terhadap risiko, dimana pengambilan keputusan tersebut bisa menghasilkan dampak baik atau buruk.

PT. Eksakta Digital Gemilang merupakan perusahaan yang menyediakan jasa dalam bidang

digital marketing. Pada perusahaan ini belum melakukan penilaian risiko terhadap setiap aset yang dimiliki, dimana ketika risiko terjadi terhadap suatu aset, tindakan yang dilakukan kurang tepat terhadap risiko tersebut. Kemudian pendataan aset yang belum baik dan terintegrasi menyebabkan kurangnya validitas antar divisi di PT. Eksakta Digital Gemilang. Selain itu perusahaan belum melakukan analisa terhadap risiko yang mungkin terjadi serta belum melakukan langkah prioritas terhadap risiko ketika terjadi.

Berdasarkan hal tersebut maka perlu dibuatkan aplikasi sistem manajemen risiko yang menerapkan proses-proses berdasarkan standar *best practice*, standar yang digunakan dalam pembuatan aplikasi sistem manajemen risiko adalah *NIST SP 800-30 Revision 1*. Aplikasi sistem manajemen risiko yang dibuat adalah aplikasi berbasis *web*, dengan sistem yang terkomputerisasi maka data akan disimpan secara terpusat. Aplikasi yang dibuat memiliki

fungsi menentukan nilai CIA dari setiap aset, menentukan risiko yang mungkin terjadi pada setiap aset, dan menentukan rencana, keputusan atau tindakan yang tepat ketika risiko itu terjadi terhadap aset. Dengan ini bagi perusahaan, penerapan manajemen risiko ini dapat meningkatkan *shareholder value*, serta memberikan gambaran kepada pengelola perusahaan mengenai kemungkinan terjadinya kerugian dimasa yang akan datang.

Metodologi Penelitian

Metodologi pada penelitian ini dilakukan dengan dua metode, yaitu metode pengumpulan data dan metode *development*. Metode pengumpulan data yang digunakan untuk merancang dan membuat sistem manajemen risiko berbasis *web* adalah sebagai berikut:

1. Observasi

Yaitu dengan mengumpulkan data yang dilakukan dengan peninjauan, pengamatan, dan pencatatan secara langsung terhadap perusahaan PT. Eksakta Digital Gemilang sehingga mendapatkan data yang akurat dan relevan.

2. Interview

Yaitu dengan melakukan wawancara langsung kepada pihak perusahaan PT. Eksakta Digital Gemilang, sehingga mendapat data dari pihak yang terkait dengan objek penelitian.

3. Studi Pustaka

Metode studi pustaka mempergunakan buku-buku perpustakaan yang meliputi *literature*, jurnal-jurnal, artikel penelitian terkait yang dapat mendukung dalam penelitian. Selain metode pengumpulan data pada penelitian ini digunakan juga metode *development* untuk merancang dan mengimplementasikan sistem manajemen risiko. Metode *development* yang digunakan untuk merancang dan mengimplementasikan sistem manajemen risiko berbasis *web* adalah dengan menggunakan *Waterfall Model*, dengan melalui beberapa tahap dari *Waterfall Model* tersebut. Beberapa tahapan dari *Waterfall Model* yang digunakan dalam penelitian adalah sebagai berikut:

1. Communication

Melakukan analisis terhadap kebutuhan sistem yang akan dibuat dengan komunikasi langsung dengan pihak terkait.

2. Planning

Lanjutan dari proses *communication*, tahapan ini menghasilkan dokumen kebutuhan sesuai keinginan *user* dalam pembuatan sistem. Pada tahap ini dilakukan perencanaan perancangan dan implementasi sistem.

3. Modeling

Melakukan perancangan desain antarmuka, perancangan *database* dan perancangan alur sistem dengan *tools* masing-masing kebutuhan setiap

perancangan. Misalnya untuk perancangan desain antarmuka digunakan *tools* Sketch.

4. Construction

Melakukan proses kode (*coding*) atau penerjemahan desain dalam bahasa yang dapat dimengerti oleh komputer. Bahasa pemrograman yang digunakan adalah *PHP* dengan database *MySQL*.

5. Deployment

Tahap ini tidak dilakukan pada penelitian ini.

2. LANDASAN TEORI

Prinsip Keamanan Informasi

Menurut Syafrizal (2007), Keamanan informasi terdiri dari tiga prinsip, yaitu:

1. Confidentiality (Kerahasiaan)

Merupakan prinsip yang menjamin, memastikan dan menjaga kerahasiaan informasi agar dapat diakses dan digunakan oleh pihak yang mempunyai wewenang sekaligus menjamin informasi yang dikirim, diterima dan disimpan tersebut terjamin kerahasiaan.

2. Integrity (Integritas/Mutu)

Merupakan prinsip yang menjamin informasi tersebut tidak berubah, dimanipulasi, dimodifikasi maupun dihilangkan tanpa izin dari pihak yang berwenang.

3. Availability (Ketersediaan)

Merupakan prinsip yang menjamin bahwa informasi akan tersedia ketika dibutuhkan serta memastikan bahwa pihak yang berwenang atas informasi tersebut tidak akan mendapat gangguan dari pihak lain.



Gambar 2.1 CIA Triad

NIST SP 800-30 Revision 1

The Information Technology Laboratory (ITL) di National Institute of Standards and Technology (NIST) yang mendukung ekonomi AS dan kesejahteraan masyarakat dengan menyediakan teknis kepemimpinan untuk mengukur bangsa dan standar infrastruktur. NIST juga bekerja sama dengan entitas sektor publik dan swasta untuk membangun pemetaan dan hubungan khusus antara standar keamanan dan pedoman yang dikembangkan oleh NIST dan the International Organization for Standardization

and International Electrotechnical Commission (ISO/IEC). Tujuan Publikasi Khusus NIST 800-30 Revision 1 adalah untuk memberikan pedoman dalam melakukan penilaian risiko terhadap sistem informasi pemerintahan dan perusahaan.

Pendekatan penilaian risiko dijelaskan dalam publikasi ini serta didukung oleh serangkaian standar keamanan dan pedoman yang diperlukan untuk mengelola risiko keamanan informasi. Selain publikasi ini, publikasi khusus dikembangkan oleh Joint Task Force Transformasi Initiative untuk mendukung kerangka keamanan informasi terpadu terhadap pemerintahan yang meliputi:

1. *Special Publication 800-39 - Managing Information Security Risk*
2. *Special Publication 800-37 - Guide for Applying the Risk Management Framework to Federal Information Systems*
3. *Special Publication 800-53 - Recommended Security Controls for Federal Information Systems and Organizations*
4. *Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations*

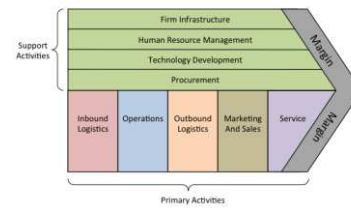
Berikut adalah ringkasan dari NIST 800-30 Revision 1 (Risk Assessment Task):

1. *Prepare for Risk Assessment* (Mempersiapkan Penilaian Resiko)
 - a. *Identify Purpose* (Mengidentifikasi Tujuan)
 - b. *Identify Scope* (Mengidentifikasi Ruang Lingkup)
 - c. *Identify Assumptions and Constraints* (Mengidentifikasi asumsi dan hambatan)
 - d. *Identify Information Source* (Mengidentifikasi Sumber Informasi)
 - e. *Identify Risk Model and Analytic Approach* (Mengidentifikasi risiko model dan Analitik pendekatan)
2. *Conduct Risk Assessment* (Melakukan Penilaian Resiko)
 - a. *Identify Threat Sources* (Mengidentifikasi Sumber Ancaman)
 - b. *Identify Threat Events* (Mengidentifikasi Kejadian Ancaman)
 - c. *Identify Vulnerabilities and Predisposing Conditions* (Mengidentifikasi Kerentanan dan Kondisi yang Mempengaruhi)
 - d. *Determine Likelihood* (Menentukan Kecendrungan)
 - e. *Determine Impact* (Menentukan Dampak)
 - f. *Determine Risk* (Menentukan Risk)
3. *Communicate and Share Risk Assessment Results* (Mengkomunikasikan dan Memberikan Hasil Penilaian Risiko)

- a. *Communicate Risk Assessment Results* (Mengkomunikasikan Hasil Penilaian Risiko)
 - b. *Share Risk-related Information* (Memberikan Risiko Terkait Informasi)
4. *Maintain Risk Assessment* (Memelihara Penilaian Risiko)
 - a. *Monitor Risk Factors* (Mengamati Faktor-faktor Risiko)
 - b. *Update Risk Assessment* (Memperbarui Penilaian Risiko)

Analisis Value Chain

Analisis *value chain* merupakan alat analisis yang berguna untuk memahami aktivitas-aktivitas yang membentuk nilai suatu produk atau jasa dan digunakan untuk menciptakan nilai bagi pelanggannya dalam mencapai suatu keunggulan yang kompetitif. Tujuan analisis *value chain* adalah untuk mengidentifikasi tahap-tahap *value chain* di mana perusahaan dapat meningkatkan *value* untuk pelanggan atau untuk menurunkan biaya.



Gambar 2.2 Porter's Value Chain

3. ANALISA DAN PERANCANGAN SISTEM

Analisa Proses Pendaan Aset sebelum Implementasi Sistem Manajemen Risiko

Pada proses pendaan sebelum implementasi sistem manajemen risiko, proses dilakukan hanya melakukan pendaan aset saja, tidak melakukan analisa risiko-risiko yang mungkin terjadi terhadap setiap aset yang telah didaftarkan. Berikut adalah analisa proses pendaan aset sebelum implementasi sistem manajemen risiko:



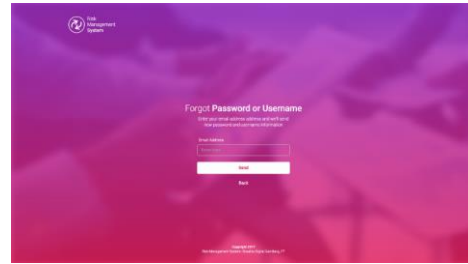
Gambar 3.1 Analisa proses pendaan aset sebelum implementasi sistem manajemen risiko.

Perancangan Proses

Berikut adalah perancangan proses sistem manajemen risiko berbasis *web* berdasarkan NIST 800-30 Revision 1:



Gambar 3.2 Perancangan Proses Sistem Manajemen Risiko berdasarkan NIST 800-30 Revision 1



Gambar 3.5 Rancangan Tampilan *Forgot Password or Username*

ERD (Entity Relationship Diagram)

Berikut adalah ERD (Entity Relationship Diagram) dari sistem yang dibuat:

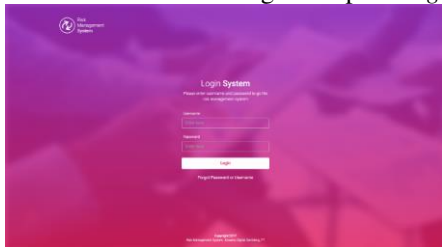


Gambar 3.3 ERD (Entity Relationship Diagram)

3.1. Perancangan Antarmuka Pengguna (User Interface)

1. Rancangan Tampilan Login

Tampilan *login* pada sistem yang dibuat adalah *form* menyediakan *textfield username*, *textfield password*, *button password*, dan *link forgot username or password*. Tampilan *login* dibuat sebagai pintu masuk user ke dalam sistem yang dibuat. Berikut adalah rancangan tampilan *login*:



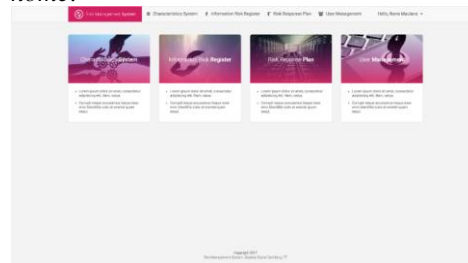
Gambar 3.4 Rancangan Tampilan *Login*

2. Rancangan Tampilan *Forgot Password or Username*

Tampilan *forgot password or username* pada sistem yang dibuat adalah *form* menyediakan *textfield email address*, *button send*, dan *link back*. Berikut adalah rancangan tampilan *forgot password or username*:

3. Rancangan Tampilan Home

Tampilan *home* adalah tampilan ketika *user* berhasil *login*. Terdapat beberapa *menu* untuk menggunakan fungsi yang terdapat pada sistem yang dibuat. Berikut adalah rancangan tampilan *home*:

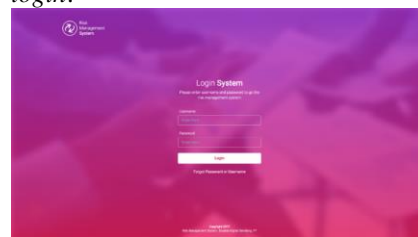


Gambar 3.6 Rancangan Tampilan *Home*

4. IMPLEMENTASI SISTEM Implementasi Sistem

1. Tampilan Login

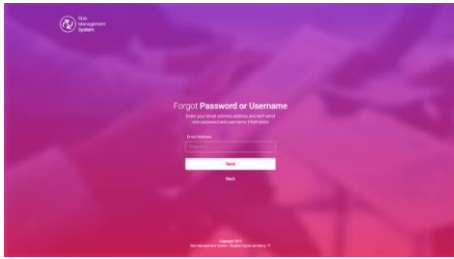
Tampilan *login* pada sistem yang dibuat adalah *form* menyediakan *textfield username*, *textfield password*, *button password*, dan *link forgot username or password*. Berikut adalah tampilan *login*:



Gambar 4.1 Tampilan *Login*

2. Tampilan *Forgot Password or Username*

Tampilan *forgot password or username* pada sistem yang dibuat adalah *form* menyediakan *textfield email address*, *button send*, dan *link back*. Berikut adalah tampilan *forgot password or username*:



Gambar 4.2 Tampilan *Forgot Password or Username*

3. Tampilan *Home*

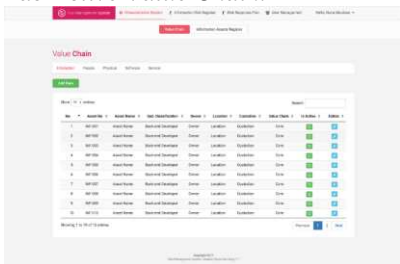
Tampilan *home* adalah tampilan ketika *user* berhasil *login*. Terdapat beberapa *menu* untuk menggunakan fungsi yang terdapat pada sistem yang dibuat. Berikut adalah tampilan *home*:



Gambar 4.3 Tampilan *Home*

4. *Characteristics System - Tab Active Value Chain*

Pada tampilan ini berfungsi menampilkan data aset yang memiliki *value chain* yang telah dimasukkan. Selain itu tampilan ini juga berfungsi untuk masuk ke dalam tampilan *add data* dan *edit data* aset. Berikut adalah tampilan *Characteristics System – Tab Active Value Chain*.



Gambar 4.4 Tampilan *Characteristics System – Tab Active Value Chain*

5. Tampilan *Add Data Value chain*

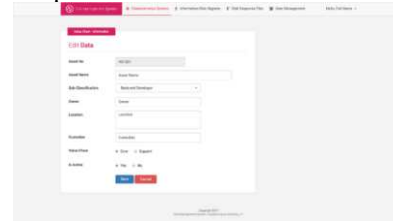
Tampilan ini berfungsi untuk menambah data aset yang memiliki *value chain*. Berikut adalah tampilan *add data value chain*:



Gambar 4.5 Tampilan *Add Data Value Chain*

6. Tampilan *Edit Data Value Chain*

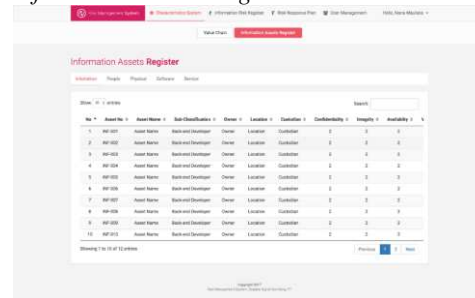
Tampilan ini berfungsi untuk memperbaharui data aset yang memiliki *value chain*. Berikut adalah tampilan *edit data value chain*:



Gambar 4.6 Tampilan *Edit Data Value Chain*

7. Tampilan *Characteristics System - Tab Active Information Assets Register*

Pada tampilan ini berfungsi menampilkan data aset yang memiliki nilai CIA (*Confidentiality, Integrity, Availability*) yang telah dimasukkan. Berikut adalah tampilan *characteristics system – tab active information assets register*:



Gambar 4.7 Tampilan *Characteristics System – Tab Active Information Assets Register*

8. Tampilan *Edit Data Information Assets Register*

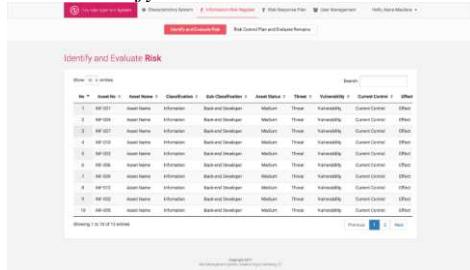
Tampilan ini berfungsi untuk memperbaharui data aset yang memiliki nilai CIA (*Confidentiality, Integrity, Availability*). Berikut adalah tampilan *edit data information assets register*:



Gambar 4.8 Tampilan Tampilan *Edit Data Information Assets Register*

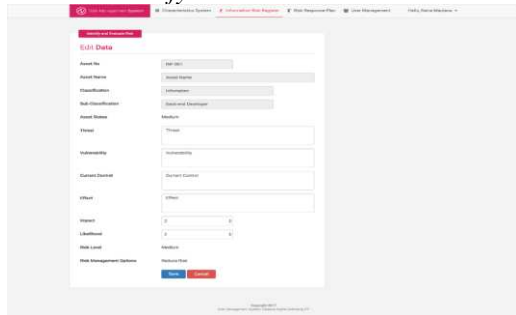
9. Tampilan *Information Risk Register - Tab Active Identify and Evaluate Risk*

Pada tampilan ini berfungsi menampilkan data aset yang memiliki data terkait risiko yang telah dimasukkan. Selain itu tampilan ini berfungsi untuk masuk ke dalam tampilan *edit data* aset. Berikut adalah tampilan *information risk register – tab active identify and evaluate risk*:



Gambar 4.9 Tampilan *Information Risk Register - Tab Active Identify and Evaluate Risk*

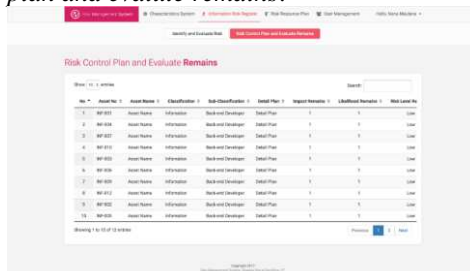
10. Tampilan *Edit Data Identify and Evaluate Risk*
Tampilan ini berfungsi untuk memperbaharui data aset yang memiliki data ancaman, kerentanan, kontrol risiko, akibat, dampak dan kemungkinan terhadap risiko itu terjadi. Berikut adalah tampilan *edit data identify and evaluate risk*:



Gambar 4.10 Tampilan Tampilan *Edit Data Identify and Evaluate Risk*

11. Tampilan *Information Risk Register - Tab Active Identify and Evaluate Risk*

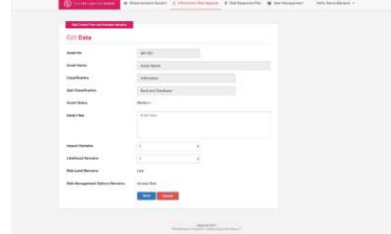
Pada tampilan ini berfungsi menampilkan data aset yang memiliki data terkait risiko setelah adanya kontrol dan evaluasi risiko terhadap aset. Selain itu tampilan ini juga berfungsi untuk masuk ke dalam tampilan *edit data* aset. Berikut adalah tampilan *information risk register – tab active risk control plan and evalute remains*:



Gambar 4.11 Tampilan *Information Risk Register - Tab Active Risk Control Plan and Evalute Remains*

12. Tampilan *Edit Data Risk Control Plan and Evalute Remains*

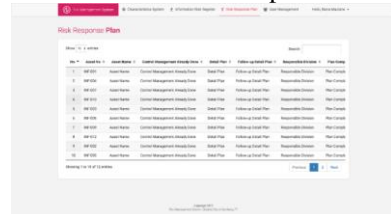
Tampilan ini berfungsi untuk memperbaharui data aset yang memiliki data dampak dan kemungkinan terhadap risiko itu terjadi setelah adanya perencanaan terkait risiko. Berikut adalah tampilan *edit data risk control plan and evalute remains*:



Gambar 4.12 Tampilan *Edit Data Risk Control Plan and Evalute Remains*

13. Tampilan *Risk Response Plan*

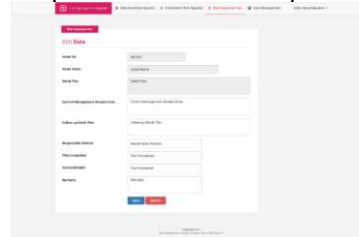
Pada tampilan ini berfungsi menampilkan data aset yang memiliki data terkait perencanaan tindaklanjut terhadap risiko. Selain itu tampilan ini juga berfungsi untuk masuk ke dalam tampilan *edit data* aset. Berikut adalah tampilan *risk response plan*:



Gambar 4.13 Tampilan *Risk Response Plan*

14. Tampilan *Edit Data Risk Response Plan*

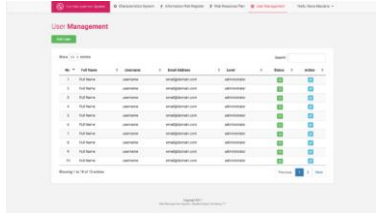
Tampilan ini berfungsi untuk memperbaharui data aset yang memiliki data terkait perencanaan tindaklanjut terhadap risiko. Berikut adalah tampilan *edit data risk response plan*:



Gambar 4.14 Tampilan *Edit Data Risk Response Plan*

15. Tampilan *User Management*

Tampilan *user management* adalah tampilan yang berfungsi untuk melihat data user yang akan menggunakan sistem yang dibuat. Berikut adalah tampilan *user management*:



Gambar 4.15 Tampilan User Management



Gambar 4.17 Tampilan Edit User

16. Tampilan Add User

Tampilan *add user* pada sistem yang dibuat berfungsi untuk menambahkan data *user* yang akan menggunakan sistem. Berikut adalah tampilan *add user*:



Gambar 4.16 Tampilan Add User

18. Tampilan Change Password

Tampilan *change password* pada sistem yang dibuat berfungsi untuk memperbaharui data *password user* yang menggunakan sistem. Berikut adalah tampilan *change password*:



Gambar 4.18 Tampilan Change Password

17. Tampilan Edit User

Tampilan *edit user* pada sistem yang dibuat berfungsi untuk memperbaharui data *user* yang akan menggunakan sistem. Berikut adalah tampilan *edit user*:

4.1. Pengujian Sistem

Pada pengujian sistem yang digunakan untuk menguji sistem yang dibuat adalah dengan metode pengujian *black box*. Pengujian *black box* berfokus pada persyaratan fungsional perangkat lunak.

1. Pengujian Login

Tabel 4.1 Pengujian Login

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masukkan data <i>user</i> , contoh: Username: nanamaulana Password: 123qwe	Masuk ke menu yang diinginkan	Masuk ke menu yang diinginkan	Diterima

2. Pengujian pengolahan data *Characteristics Sytem Value Chain*

Tabel 4.2 Pengujian pengolahan data *Characteristics Sytem Value Chain*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masuk tambah data, kemudian memasukkan data sesuai <i>textfield</i> yang tersedia.	Masuk ke tampilan table yang menampilkan data yang telah dimasukkan sebelumnya.	Masuk ke tampilan table yang menampilkan data yang telah dimasukkan sebelumnya.	Diterima
Masuk ke <i>edit</i> data, kemudian memperbaharui data sesuai <i>textfield</i> yang tersedia	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Diterima

3. Pengujian pengolahan data *Characteristics Sytem Information Assets Register*

Tabel 4.3 Pengujian pengolahan data *Characteristics Sytem Information Assets Register*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masukkan alamat <i>email</i> , contoh: Email: nanamaulana93@gmail.com	Muncul pesan data telah berhasil terkirim	Muncul pesan data telah berhasil terkirim	Diterima

4. Pengujian pengolahan data *Information Risk Register*

Tabel 4.4 Pengujian pengolahan data *Information Risk Register*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masuk ke <i>edit</i> data, kemudian memperbaharui data sesuai <i>textfield</i> yang tersedia	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Diterima

5. Pengujian pengolahan data *Risk Response Plan*

Tabel 4.5 Pengujian pengolahan data *Risk Response Plan*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masuk ke <i>edit</i> data, kemudian memperbaharui data sesuai <i>textfield</i> yang tersedia	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Diterima

6. Pengujian pengolahan data *User Management*

Tabel 4.6 Pengujian pengolahan data *User Management*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masuk tambah data, kemudian memasukkan data sesuai <i>textfield</i> yang tersedia.	Masuk ke tampilan table yang menampilkan data yang telah dimasukkan sebelumnya.	Masuk ke tampilan table yang menampilkan data yang telah dimasukkan sebelumnya.	Diterima
Masuk ke <i>edit</i> data, kemudian memperbaharui data sesuai <i>textfield</i> yang tersedia	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Masuk ke tampilan table yang menampilkan data yang telah diperbaharui.	Diterima

7. Pengujian *Change Password*

Tabel 4.7 Pengujian *Change Password*

Data Masukkan	Yang diharapkan	Pengamatan	Kesimpulan
Masuk ke menu <i>change password</i> , kemudian memperbaharui data sesuai <i>textfield</i> yang tersedia	Muncul pesan password berhasil diperbaharui	Muncul pesan <i>password</i> berhasil diperbaharui	Diterima

5. PENUTUP

Aplikasi sistem manajemen risiko yang dibuat adalah aplikasi berbasis *web*, dengan sistem yang terkomputerisasi maka data akan disimpan secara terpusat yang mengadopsi proses-proses berdasarkan *NIST SP 800-30 Revision 1*. Maka berikut hal yang dapat disimpulkan dari perancangan dan implementasi sistem manajemen risiko berbasis *web* untuk pengelolaan aset:

1. Mengelola risiko-risiko yang ditemukan di PT. Eksakta Digital Gemilang.
2. Menentukan prioritas penanganan terhadap risiko-risiko yang ditemukan di PT. Eksakta Digital Gemilang.
3. Merancang dan membuat sistem manajemen risiko berbasis *web*.
4. Sistem yang dibuat mengadopsi proses-proses yang ada pada standar *NIST SP 800-30 Revision 1* dalam bentuk aplikasi berbasis *web*.

6. DAFTAR PUSTAKA

- [1] A.S Rosa dan Salahuddin M. (2011). *Modul Pembelajaran Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek)*. Bandung: Modula
- [2] Anhar. (2010). *PHP & MySql Secara Otodidak*. Jakarta: PT TransMedia
- [3] Ayuliana. (2009). *Teknik Pengujian Perangkat Lunak Blackbox*.
- [4] Deitel, H.M., Deitel, P, J. (2012). *Java How to Program. Sixth Edition*. New Jersey: Pearson
- [5] Fardil Miftah. (2015). *Fitur Dahsyat Sublime Text 3*
- [6] 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.
- [7] Hidayat, Rahmat. (2010). *Cara Praktis Membangun Website Gratis: Pengertian Website*. Jakarta: PT Elex Media Komputindo Kompas, Gramedia.
- [8] Kustiyahningsih, Y. dan Anamisa, D. R. (2011). *Pemrograman Basis Data Berbasis Web Menggunakan PHP & MySQL. Edisi Pertama*. Yogyakarta: Graha Ilmu.
- [9] Mike Goldberg, Eric Palladini (2010). *Pengelolaan Risiko dan Penciptaan Nilai Melalui Pendanaan Usaha Mikro*, Jakarta.
- [10] Munir Rinaldi. (2011). *Algoritma dan Pemrograman dalam Bahasa Pascal dan C*, Bandung: Penerbit Informatika.