Analisis dan Implementasi Operasional *Security Management* pada Pusat Komputer Universitas Kristen Petra

Hartanto Rusli[1],Agustinus Noertjahyana[2],Ibnu Gunawan[3]
Program Studi Teknik Informatika,Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131, Surabaya 60236
Telp (031) – 2983455, Fax. (031) - 8417658
bblivelogin@gmail.com[1],agust@petra.ac.id[2],ibnu@petra.ac.id[3]

ABSTRAK: Dalam menjalankan kegiatan operasional yang berbasis teknologi informasi menggunakan jaringan komputer, suatu organisasi perlu memperhatikan faktor keamanan dalam sistem informasi. Keamanan jaringan komunikasi mutlak diperlukan untuk mampu memberikan pelayanan terus menerus bagi para penggunanya. Sebagian besar staf yang berkecimpung dalam pembuatan kebijakan keamanan ini, seringkali merasa kebingungan dalam memulai pekerjaannya, dikarenakan belum memiliki pengalaman yang cukup atau merasa belum memerlukan suatu kebijakan dikarenakan belum ada kejadian yang terkait dengan suatu kebijakan keamanan.
Untuk mengatasi masalah ini,diperlukansebuah aplikasi untuk membantu staf dalam membuat desain sistem keamanan yang terstruktur dengan modul pelaksanaan yang bersumber dari modul kebijakan keamanan dan manajemen risiko sehingga dapat dipantau jika terjadi kesalahan.

Output yang dihasilkan aplikasi bukan hanya bisa berlaku pada satu organisasi saja tetapi bisa dipakai ke organisasi lain karena sifatnya *general*. Pengujian dilakukan dengan menggunakan *engine* untuk melakukan pembuatan *planning* CISSP (*Certified Information System Security Professional*), perhitungan kuesioner, dan hasil dari perhitungan risiko.

Kata Kunci : CISSP, *Security*, *Planning* dan operasional

ABSTRACT: *In carrying out operations using information technology-based computer network, it is an organization needs to consider factors in information systems security. The Security of communication networks is absolutely necessary to be able to provide continuous service to its users. Most of the staff were involved in the making of this security policy, often feel confused in starting to work, due to not having enough experience or feeling that it will not require a policy because there was no incident related to a security policy.*
To resolve these problems, we need a tool to help the staff in making the security system design that is structured with implementation modules sourced from security policy and risk management module so that it can be monitored if an error occurs.

Output generated by application not only applied to one organization alone but can be used to other organizations because it is general. Testing is done by using a search engine to perform the manufacturing CISSP (Certified Information System Security Professional) planning, calculation of the questionnaire, and the results of the risk calculation.

Keywords **:** CISSP, *Security, Planning and Operational*

1. PENDAHULUAN

Semakin meningkatnya teknologi saat ini, membuat kebutuhan akan keamanan teknologi tersebut juga meningkat. Berbagai standar dan kebijakan keamanan menjadi pertimbangan berbagai organisasi untuk mendukung tingkat keamanan.

Untuk dapat membangun kebijakan keamanan yang memberikan landasan bagus di masa mendatang, maka langkah awal yang harus dikembangkan adalah membuat kebijakan keamanan yang dapat mengurangi risiko terjadinya penyalahgunaan terhadap sumber daya yang ada pada organisasi.

Sebagian besar staf yang berkecimpung dalam pembuatan kebijakan keamanan ini, seringkali merasa kebingungan dalam memulai pembuatannya, dikarenakan memang belum memiliki pengalaman yang cukup atau merasa belum memerlukan suatu kebijakan keamanan dikarenakan belum ada kejadian yang terkait dengan suatu kebijakan keamanan

2. TINJAUAN PUSTAKA

Seiring dengan perubahan dunia, kebutuhan untuk peningkatan keamanan dan teknologi terus tumbuh. Keamanan pernah menjadi isu panas hanya di bidang teknologi, namun sekarang hal ini menjadi lebih dan lebih menjadi bagian dari kehidupan sehari-hari. Keamanan merupakan perhatian dari setiap organisasi, instansi pemerintah, perusahaan, dan unit militer.

Tujuan dari keamanan informasi adalah untuk melindungi sumber daya organisasi, seperti informasi, *hardware*, dan *software*. Pelalui pemilihan dan pengaplikasian usaha perlindungan yang sesuai, *security* dapat membantu organisasi untuk memenuhi tujuan bisnis atau misi dengna melindungi sumber daya fisik, finansial, reputasi, pegawai, dan aset yang dapat dihitung maupun tidak dapat dihitung [1].

CISSP membantu perusahaan mengidentifikasi individu yang memiliki kemampuan, pengetahuan, dan pengalaman yang diperlukan untuk menerapkan praktek-praktek keamanan yang solid, melakukan analisa resiko, mengidentifikasi penanggulangan yang diperlukan, dan membantu organisasi secara kesuluruhan untuk melindungi fasilitas, sistem, jaringan, dan informasi yang dimiliki oleh perusahaan [2].

2.1. CISSP

CISSP (*Certified Information Security System Professional*) meliputi sepuluh mata pelajaran yang berbeda, yang lebih

dikenal dengan domain. 10 domain pada CISSP meliputi *Information Governance and Risk Management, Access Control, Cryptography, Environmental (Physical) Security, Security Architecture and Design, Bussiness Continuity and Disaster Recovery Plan, Telecommunication and Network Security, Application Development Security, Operation Security, and Legal, Regulation, Investigation, and Compliance.*

2.1.1. *Information Governance and Risk Management*

Domain ini mengidentifikasikan aset perusahaan, cara yang baik untuk menentukan level perlindungan yang dibutuhkan, dan buget yang dibutuhkan untuk implementasi keamanan. *Domain* ini mengarah pada klasifikasi data, kebijakan, prosedur, standar, *risk assestment*, dan manajemen resiko.

Penanganan insiden keamanan komputer telah menjadi komponen penting dalam teknologi informasi. Serangan yang terkait dengan *Cybersecurity* tidak hanya lebih banyak dan beragam, tetapi lebih merusak dan menggangu. Jenis insiden baru yang berhubungan dengan keamanan sering muncul. Kegiatan pencegahan berdasarkan hasil penilaian resiko dapat mengurangi kejadian, namun tidak semua insiden dapat dicegah. Oleh karena itu, kemampuan mendeteksi insiden diperlukan untuk dapat dengan cepat mendeteksi insiden, meminimalkan kerugian dan kerusakan, mengurangi kelemahan yang dieksploitasi, dan memulihkan layanan teknologi informasi [3].

2.1.2 *Access Control*

Domain ini memperhatikan tentang mekanisme dan metode yang digunakan oleh *administrator* untuk mengontrol subjek mengenai apa saja yang dapat diakses, apa yang dapat dilakukan setelah proses otorisasi dan otentikasi dan memonitor aktifitasnya. *Domain* ini lebih berbicara tentang model access control dari suatu sistem keamanan, cara administrasinya, dan teknologi apa saja yang dipakai untuk proses identifikasi dan otentikasi.

2.1.3 *Cryptography*

Domain ini memperhatikan metode dan teknik menyembunyikan data untuk tujuan keamanan. Tindakan ini melibatkan teknik kriptografi, pendekatannya, dan teknologinya. Secara umum domain ini fokus pada protokol enkripsi dan implementasinya, *Public Key Infrastructure* dan fungsi *hashing.*

2.1.4 *Environmental (Physical) Security*

Domain ini memperhatikan resiko dan ancaman, prosedur keamanan, dan keamanan fasilitas dengan memperhatikan lingkungannya. *Domain* ini berfokus pada *restricted areas*, metode untuk otentikasi dan kontolnya, *fire detection*, *fencing*, dan *intrusion detection.*

2.1.5 *Security Architecture and Design*

Domain ini memperhatikan konsep, standar untuk desain dan implementasi aplikasi yang *secure*, sistem operasi, dan sistem itu sendiri. Domain ini fokus pada model keamanan, arsitektur, evaluasi, serta sertifikasi dan akreditasi.

2.1.6 *Bussiness Continuity and Disaster Recovery Plan*

Domain ini memperhatikan tindakan mempertahankan aktifitas bisnis ketika menghadapi masalah. *Domain* ini fokus pada analisa dampak pada bisnis, prediksi dari kehilangan akibat dampak, prioritas unit dan manajemen krisis.

2.1.7 *Telecommunication and Network Security*

Domain ini berfokus terhadap sistem komunikasi seperti *internal*, *eksternal*, *public*, *private*, dan administrasi *remote management*. *Domain* ini juga membahas tentang teknologi LAN, WAN, *internet*, *intranet*, *Virtual Private Network* (VPN), *firewall*, dan topologi dari jaringan komunikasi.

Networking adalah salah satu topik yang lebih kompleks di bidang komputer, terutama karena begitu banyak teknologi yang terlibat dan berkembang. Teknologi sekarang ini meningkat dalam hal funsionalitas dan keamanan secara eksponensial, yang mana harus selalu dipelajari, diimplementasikan, dan diamankan. [4]

2.1.8 *Application Development Security*

Domain ini memperhatikan komponen keamanan dari bagaimana sistem itu bekerja dan bagaimana untuk mengembangkan dengan cara yang terbaik dan mengukur efektifitasnya. *Domain* ini mengarah pada keamanan dari aplikasinya yang berfokus pada *data mining*, *data warehousing*, komponen *software* dan titik lemahnya.

2.1.9 *Operation Security*

Domain ini memperhatikan kontrol dari personil, *hardware*, sistem, teknik *auditing* dan *monitoring*. *Domain* ini fokus pada tanggung jawab administratif terkait dengan personil dan fungsi pekerjaan juga kontrol tindakan preventif, detektif, korektif dan *recovery*.

2.1.10 *Legal, Regulation, Investigation, and Compliance*

Domain ini memperhatikan tindakan kriminal, hukum, dan peraturan pada komputer. Domain ini berfokus pada tipe hukum, tipe peraturan, tipe kriminalitas, Licensing, pembajakan, peraturan ekspor impor, dan tindakan yang dilakukan ketika ada insiden [5].

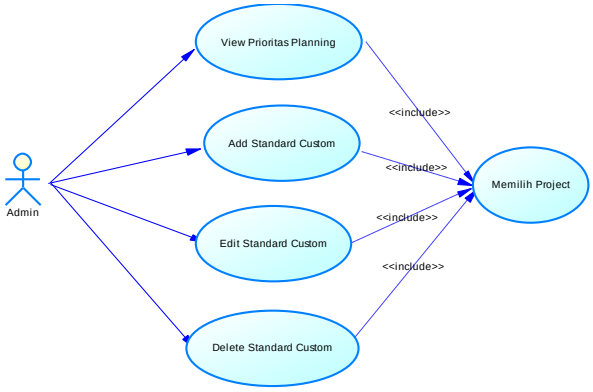
Domain ini juga membahas tentang privasi dari informasi. Ada beberapa contoh yang jelas dari informasi pribadi, seperti nama dan alamat seseorang. Informasi pribadi dapat juga termasuk catatan medis, rincian rekening bank, foto, video, informasi biometrik (seperti jempol cetak atau scan iris) dan bahkan informasi tentang apa yang orang-orang seperti individu, pendapat mereka dan di mana mereka bekerja [6].

3. DESAIN SISTEM

Secara umum, desain sistem akan dibagi menjadi tiga bagian yaitu desain pembuatan laporan operasional, penilaian kuesioner, pembuatan laporan penilaian risiko dan manajemen standar CISSP.

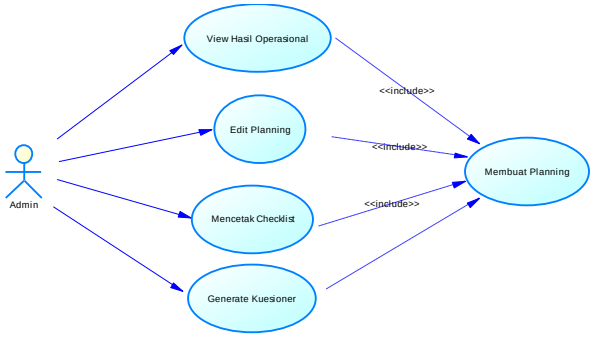
3.1. Desain Pembuatan Laporan Operasional

Pada komponen bagian ini*admin* dapat membuat *planning* berdasarkan standar CISSP dan menambahkan standar sendiri sesuai dengan kebutuhan *project* terebut. Untuk lebih detailnya dapat dilihat pada gambar *Use CaseAdmin* pada pembuatan *planning*.Gambar *Use Case Admin* pada pembuatan *planning* dapat dilihat pada Gambar 1.



Gambar 1*Use Case Admin* pada Pembuatan *Planning*

Seperti pada *use case* diagram diatas, *admin* dapat menampilkan standar CISSP, menambah, mengubah, dan menghapus standar *custom*. Semua fitur tersebut dapat dilakukan setelah *admin* memilih *project*. Setelah *planning* dibuat, hasil *planning* tersebut dibawa ke halaman operasional. Gambar *Use Case Admin* pada Halaman Operasional dapat dilihat pada Gambar 2.

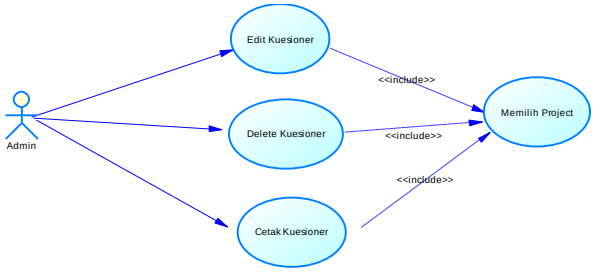


Gambar 2 *Use CaseAdmin* pada Halaman Operasional

Seperti pada *use case diagram* diatas, *admin*dapat menampilkan hasil operasional, mengubah *planning*, mencetak *checklist*, dan melakukan*generate* kuesioner.

3.2 Desain Penilaian Kuesioner

Pada bagian ini *admin* dapat melakukan proses penilaian kuesioner. Untuk mencapai hasil penilaian kuesioner, *admin* harus melakukan *generate* kuesioner dari halaman operasional. Gambar *Use Case Admin*pada Halaman Kuesioner dapat dilihat pada Gambar 3.

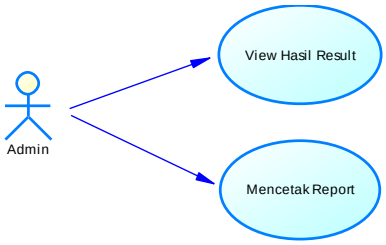


Gambar 3*Use Case* Admin pada Halaman Kuesioner

Seperti pada *use case* diagram diatas, *admin* dapat menampilkan standar CISSP, *admin* dapat mengubah, menghapus, dan mencetak kuesioner. Setelah kuesioner selesai dibuat, kuesioner tersebut di *publish* agar dapat diisi oleh responden. Untuk melihat hasil penilaian kuesioner, *admin* dapat mengakses melalui halaman *history*.

3.3 Desain Pembuatan Laporan Penilaian Risko

Pada bagian ini *admin* dapat menampilkan hasil penilaian risiko dari *project* yang telah dipilih. hasil penilaian standar dikelompokan dari setiap prioritas *domain*. Untuk lebih Gambar *Use Case Admin* pada Halaman *Result*dapat dilihat pada Gambar 4.

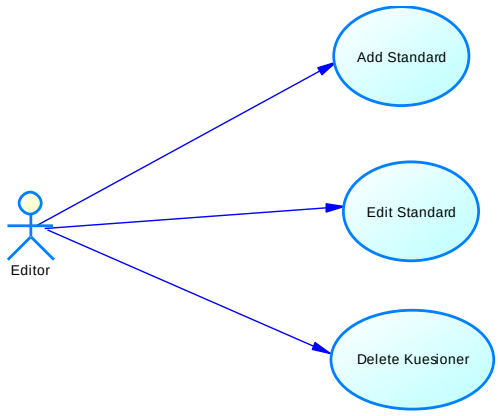


Gambar 4*Use Case Admin* pada Pembuatan *Planning*

Seperti pada *use case diagram* diatas, *admin*dapat menampilkan hasil penilaian risiko dan mencetak laporan dari hasil penilaian risiko. Hasil penilaian risiko yang di cetak memiliki warna-warna sesuai dengan tingkatan risikonya. Warna tersebut berguna untuk memudahkan pembaca membedakan tingkatan risiko dari standar.

3.4 Desain Manajemen Standar CISSP

Pada desain ini, pengguna sebagai editor dapat melakukan menajemen pada standar CISSP sesuai dengan keinginan editornya. Gambar *Use CaseEditor* terhadap Standar CISSP dapat dilihat pada Gambar 5.



Gambar 5*Use Case Editor* pada Standar CISSP

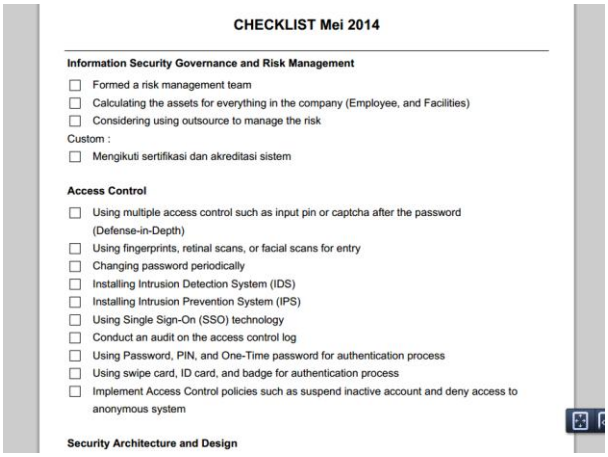
Sesuai dengan *Use Case* diatas, *editor* dapat melakukan *create*, *edit*, *delete* pada standar CISSP. Standar yang diubah akan mempengaruhi proses *planning* yang dipakai oleh *admin*. Jadi sebaiknya, setiap ada perubahan, *editor* selalu memberi tahu tentang adanya perbahan pada standar CISSP.

4. PENGUJIAN SISTEM

Pada bagian ini, akan dilakukan pengujian sistem pada aplikasi pembuatan laporan operasional, penilaian hasil kuesioner, penilaian hasil risiko, dan manajemen standar CISSP.

4.1. Pengujian Hasil Laporan Operasional

Pada aplikasi perhitungan kuesioner ini hanya akan berhasil setelah *admin* membuat *planning* lalu mencetak hasil laporan operasional dengan *output* sebuah *checklist* dari hasil standar yang telah dipilih oleh *admin.Checklist* Hasil Operasional dapat dilihat pada Gambar 6.



CHECKLIST Mei 2014

Information Security Governance and Risk Management

- ☐ Formed a risk management team
- ☐ Calculating the assets for everything in the company (Employee, and Facilities)
- ☐ Considering using outsource to manage the risk

Custom :

- ☐ Mengikuti sertifikasi dan akreditasi sistem

Access Control

- ☐ Using multiple access control such as input pin or captcha after the password (Defense-in-Depth)
- ☐ Using fingerprints, retinal scans, or facial scans for entry
- ☐ Changing password periodically
- ☐ Installing Intrusion Detection System (IDS)
- ☐ Installing Intrusion Prevention System (IPS)
- ☐ Using Single Sign-On (SSO) technology
- ☐ Conduct an audit on the access control log
- ☐ Using Password, PIN, and One-Time password for authentication process
- ☐ Using swipe card, ID card, and badge for authentication process
- ☐ Implement Access Control policies such as suspend inactive account and deny access to anonymous system

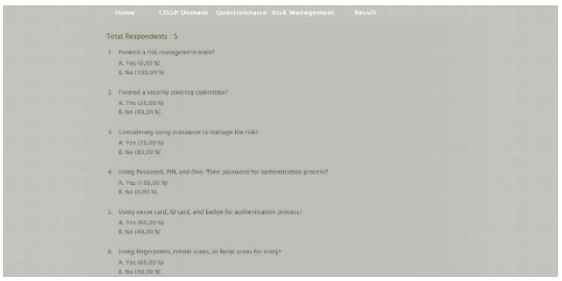
Security Architecture and Design

Gambar 6*Checklist* Hasil Operasional

Pada Gambar 6, pembuatan *checklist* dengan file berekstensi .pdf telah berhasil ditampilkan pada *browser*. Hasil standar yang terdapat pada*checklist* telah sesuai dengan *planning* yang telah dibuat pada halaman operasional.

4.2. Pengujian Penilaian Hasil Kuesioner

Pada aplikasi penilaian hasil kuesioner diasumsikan telah diisi oleh beberapa responden dan hasil tersebut dapat dilihat pada halaman *history* dari kuesioner yang ada. Penilaian Hasil Kuesioner dapat dilihat pada Gambar 7.

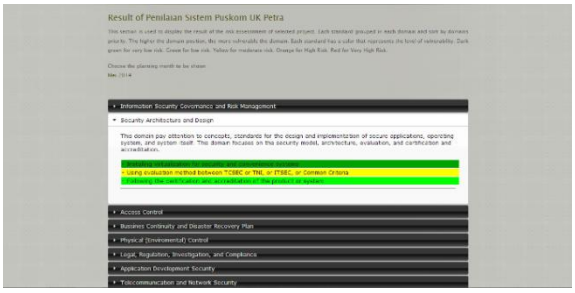


Gambar 7Penilaian Hasil Kuesioner

Pada Gambar 7, dapat dilihat terdapat jumlah total responden yang mengisi kuesionerdan hasil dari tiap pilihan jawaban berupa presentase jawaban responden pada setiap soal kueioner tersebut.

4.3. Pengujian Penilaian Hasil Risiko

Pada aplikasi penilaian hasil risiko, hasil akan ditampilkan setelah aplikasi melakukan penilaian risiko terhadap hasil jawaban kuesioner. Halaman hasil penilaian risiko tersebut dapat diakses setelah melewati bagian *risk management*.Penilaian Hasil Risiko dapat dilihat pada Gambar 8.



Gambar 8 Penilaian Hasil Risiko

Pada Gambar 8, hasil penilaian risiko yang ditampilkan dikelompokan berdasarkan prioritas per *domain*. Setiap standar yang ditampilkan memiliki warna tersendiri agar memudahkan *admin*membedakan tingkatan resiko dari setiap standar tersebut.

4.4. Pengujian Manajemen Standar CISSP

Pengujian ini merupakan pengecekan terhadap fungsi *add*, *edit*, *delete* pada halaman *editor* standar CISSP. Hasil Manajemen Standar CISSP dapat dilihat pada Gambar 9.

Gambar 9 Hasil Manajemen Standar CISSP

Dapat dilihat pada Gambar 9, hasil penambahan standar CISSP telah berhasil dilakukan dan masuk kedalam *database*.

5. KESIMPULAN

Berdasarkan hasil pengujian dapat disimpulkan beberapa hal sebagai berikut :

- *Engine* yang dibuat menyediakan standar yang tidak baku dari CISSP pada *Security Administrator* sehingga bisa dirubah atau di *custom* oleh pengguna sesuai dengan kebutuhan.
- Waktu yang dibutuhkan *engine* untuk melakukan akses ke *database* memakan waktu cukup lama. Penyebab hal ini dapat diasumsikan dari program *localhost* XAMPP yang tidak kompatibel dengan windows 8atau karena versiprogram XAMPP tersebut tidak kompatibel. Hal tersebut dapat dibuktikan dengan akses ke *website* yang lebih cepat dibandingkan ketika menggunakan *localhost*.
- Hasil *riskmanagement* menyatakan risiko dalam kategori moderate risk dengan standar CISSP pada bagian result. Beberapa hal yang perlu diperhatikan oleh Pusat Komputer Universitas Kristen Petra adalah seperti tidak memiliki tim khusus untuk manajemen risiko, menggunakan akses kontrol ganda pada resource yang bersifat sensitif, perlu memaksimalkan IDS dan IPS, memiliki *policy* untuk mengganti *password* secara berkala, memiliki detektor panas atau asap, dan mengimplementasikan XSS Filter pada aplikasi yang dibuat.

6. DAFTAR PUSTAKA

[1] Peltier, Thomas R. (2013). *Information Security Fundamentals – Second Edition.* Florida: CRC Press.

[2] Haris, Shon. (2010). *All-in-One CISSP Exam Guide* Fifth Edition. New York:McGraw-Hill Companies

[3] National Institute of Standards and Technology. 2012. *Computer Securtiy Incident Handling Guide, NIST SP 800-61 Revision 2*

[4] Harris, Shon. 2013. CISSP. *All-in-One CISSP Exam Guide* Sixth Edition.New York: McGraw-Hill Companies

[5] Conrad, Eric. (2011). *Eleventh Hour CISSP Study Guide.* Amsterdam: Elsevier.

[6] Office of The Australian Information Commissioner. (2013). '*Reasonable steps*' *to protect personal information.* Australia:Office of the Australian Information Commisioner