Studi Literatur Perubahan Antara CISSP 10 Domain dengan 8 Domain

Michael Perkasa[1], Agustinus Noertjahyana[2], Silvia Rostianingsih [3]
Program Studi Teknik Informatika, Fakultas Teknologi Industri, Universitas Kristen Petra
Jl. Siwalankerto 121-131, Surabaya 60236
Telp (031) – 2983455, Fax. (031) - 8417658
johannes.michael1992@yahoo.com[1], agust@petra.ac.id[2], silvia@petra.ac.id [3]

ABSTRAK

Gelar adalah salah satu yang sedang dicapai oleh sebagian manusia dalam pekerjaannya, guna mempengaruhi potensi yang dimiliki oleh seorang karyawan atau karyawati. Maka dengan berkembangnya teknologi, manusia semakin membutuhkan gelar ataupun sertifikasi guna mengasah dan meningkatkan kemampuannya.

Dengan dibahasnya tentang perbedaan perubahan domain CISSP dari 10 domain menjadi 8 domain yang di masing-masing domain memiliki ciri masing-masing dan fungsi kegunaan masing-masing. CISSP 8 domain merupakan domain baru yang telah di update masing-masing fungsinya dan menjadi lebih efisien karena lebih sedikit tetapi fungsinya lebih terfokus.

Oleh karena itu domain 8 lebih diunggulan dibandingkan domain 10 karena faktor-faktor pendukung tersebut.

Kata Kunci: Jaringan, Manajemen Jaringan, Sertifikasi

ABSTRACT

Degree is one that is being achieved by most people in their work, in order to influence the potential possessed by an employee or the employee. So with the development of technology, people increasingly need a degree or certification in order to hone and enhance its capabilities.

With the changes under discussion on the differences of the 10 CISSP domains domain into 8 domains in each domain has the characteristics of each and their respective utility functions. CISSP 8 domain is a new domain that have updated their respective functions and become more efficient because fewer but more focused functions.

Therefore, domain 8 is more favored than 10 domain due to factors such support.

***Keywords**: Network, Network Management, Certification*

1. PENDAHULUAN

Seiring dengan semakin tingginya ketergantungan organisasi tekonologi informasi dan kesadaran akan pentingnya data pada sistem informasi, maka meningkat pula kebutuhan akan ahli di bidang keamanan sistem informasi yang memiliki kualifikasi internasional.

Kebutuhan profesional di bidang keamanan informasi terus meningkat. Banyak organisasi yang kesulitan mendapatkan tenaga profesional keamanan informasi yang kompeten. Salah satu ukuran yang paling mudah untuk melihat kompetensi seseorang adalah melalui sertifikasi apa yang dimiliki.

Tentu perusahaan ingin mencari tenaga profesional yang kompeten. Salah satu hal yang memudahkan perusahaan mencari profesional yang kompeten adalah dengan sertifikat yang dimiliki. Pengetahuan yang luas dan mendalam di banyak bidang keamanan informasi amat dibutuhkan karena CISSP diperuntukkan berada di posisi *middle management* yang mengharuskan dapat bekerjasama dengan Top Management.

Bagaimana perusahaan bisa membuat desain sistem keamanan menggunakan platform tertentu sehingga dapat tercipta sistem keamanan yang baik.

2. LANDASAN TEORI

CISSP **(***Certified Information Sistem Security Professional***)** merupakan sertifikasi di bidang keamanan sistem informasi yang secara independen dikeluarkan oleh *International Information Sistems Security Certification Consortium*. Maksud dari independen disini adalah sertifikasi tidak tergantung pada vendor tertentu seperti misalnya Microsoft, Cisco, Oracle, dan sebagainya. [2] [4]

Tujuan dari keamanan informasi adalah untuk melindungi sumber daya organisasi, seperti informasi, *hardware*, dan *software*. melalui pemilihan dan pengaplikasian usaha perlindungan yang sesuai, *security* dapat membantu organisasi untuk memenuhi tujuan bisnis atau misi melindungi sumber daya fisik, finansial, reputasi, pegawai, dan aset yang dapat dihitung maupun tidak dapat dihitung. [2][4]

CISSP membantu perusahaan mengidentifikasi individu yang memiliki kemampuan, pengetahuan, dan pengalaman yang diperlukan untuk menerapkan praktek-praktek keamanan, melakukan analisis resiko, mengidentifikasi penanggulangan yang diperlukan, dan membantu organisasi secara kesuluruhan untuk melindungi fasilitas, sistem, jaringan, dan informasi yang dimiliki oleh perusahaan. [2][4]

3. Perubahan CISSP Domain 10 dan Domain 8

Pada bab ini terdapat analisis mengenai perubahan nama domain dari domain lama ke domain baru. Tersedia nama-nama gabungan CISSP domain 10 menjadi domain 8 yang dimana gabungan domain ini berubah menjadi domain baru.

3.1 Nama perubahan domain

Nama-nama perubahan 10 domain lama ke 8 domain baru terdapat pada tabel. Nama-nama domain lama dan baru dapat dilihat pada Tabel 1. [1][3]

Tabel 1. Nama perubahan domain

10 Domain (OLD)	8 Domain (NEW)
Information Security Governance & Risk Management Business Continuity and Disaster Recovery Planning Legal, Regulation, Compliance and Investigation	Security and Risk Management
Physical Security	Asset Security
Security Architecture and Design Cryptography	Security Engineering
Telecommunication & Network Security Cryptography	Communications & Network Security
Access Control	Identity and Access Management
Security Architecture and Design	Security Assessment and Testing
Operations Security	Security Operations
Application Development Security	Software Development Security

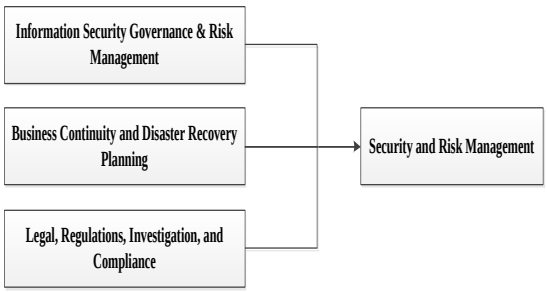
3.2 Perubahan 10 domain menjadi 8 domain

CISSP mengalami perubahan dari 10 domain menjadi 8 domain mulai efektif sejak 15 April 2015. CISSP 10 domain terdiri dari : Access Control, Application Security, Business Continuity and Disaster Recovery Planning, Cryptography, Information Security and Risk Management, Legal, Regulations, Compliance, and Investigation, Operations Security, Physical (environmental) Security, Security Architecture and Design, Telecommunications and Network Security. [5][6]

CISSP 8 domain terdiri dari : Security and Risk Management (Security, Risk, Compliance, Law, Regulations, Business Continuity), Asset Security (Protecting Security of Assets), Security Engineering (Engineering and Management of Security), Communications and Network Security (Designing and Protecting Network Security), Identity and Access Management (Controlling Access and Managing Identity), Security Assessment and Testing (Designing, Performing, and Analyzing Security Testing), Security Operations (Foundational Concepts, Investigations, Incident Management, Disaster Recovery), Software Development Security (Understanding, Applying, and Enforcing Software Security).[5] [6]

3.2.1 Domain Security and Risk Management

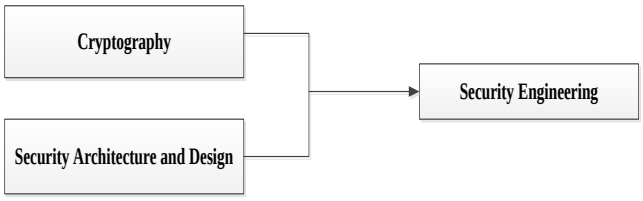
Domain Security and Risk Management adalah penggabungan dari topik domain lama *Information Security Governance & Risk Management* dan *Legal, Regulations, Investigations, & Compliance*. Penggabungan domain terjadi karena domain baru membahas tentang keamanan dan management resiko. Domain lama merupakan domain yang memiliki fungsi masing-masing dari tiap domain yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 1. [1][8]



Gambar 1. Domain Security and Risk Management

3.2.2 Domain Security Engineering

Domain Security Engineering adalah penggabungan dari topik domain lama *Cryptography*, *Security Architecture and Design* , dan Keamanan Fisik. Penggabungan domain terjadi karena domain baru membahas tentang keamanan, desain, arsitektur keamanan, kerentanan, ancaman. Domain lama merupakan domain yang memiliki fungsi masing-masing dari tiap domain yang kemudian digabung menjadi 1 domain baru. Penggabungan Perubahan domain dapat diliat pada Gambar 2. [1][8]



Gambar 2. Domain Security Engineering

3.2.3 Domain Security Assessment and Testing

Domain *Security Assessment and Testing* ini adalah penggabungan dari domain Access Control dan *Business Continuity and Disaster Recovery*. Namun mayoritas domain ini tidak berisi gabungan domain lama. Penggabungan domain terjadi karena domain baru membahas . Domain lama merupakan domain yang memiliki fungsi masing-masing dari tiap domain yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 3. [1][8]

Gambar 3. Domain Security Assessment and Testing

3.2.4 Domain Asset Security

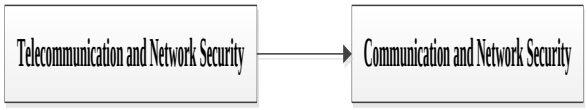
Domain Asset Security adalah penggabungan dari topik domain lama *Cryptography*, *Operations Security*. Penggabungan domain terjadi karena domain baru membahas tentang pengumpulan, penanganan, dan melindungi informasi. Domain lama merupakan

domain yang memiliki fungsi memperhatikan resiko dan ancaman, prosedur keamanan, dan keamanan fasilitas dengan memperhatikan lingkungannya yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 4. [1][8]

Gambar 4. Domain Asset Security

3.2.5 Domain Communication and Network Security

Domain *Communication and Network Security* adalah domain yang terdiri dari konten domain Telecommunication and Network Security. Penggabungan domain terjadi karena domain baru membahas tentang komputer dan jaringan muncul dari integrasi perangkat komunikasi, perangkat penyimpanan, perangkat pengolahan, perangkat keamanan, perangkat input, perangkat output, sistem operasi, perangkat lunak, layanan, data. Domain lama merupakan domain yang memiliki fungsi berfokus terhadap sistem komunikasi seperti *internal*, *eksternal*, *public*, *private*, dan administrasi *remote management* yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 5. [1][8]



Gambar 5. Domain Communication and Network Security

3.2.6 Domain Identity and Access Management

Domain Identity and Access Management adalah penggabungan dari topik domain lama *Access Control* dan juga mencakup beberapa topik dari domain *Physical (Environment) Security*. Penggabungan domain terjadi karena domain baru membahas tentang berfokus pada isu-isu yang berkaitan dengan pemberian dan pencabutan hak untuk mengakses data atau melakukan tindakan pada sistem. Domain lama merupakan domain yang memiliki fungsi mekanisme dan metode yang digunakan oleh *administrator* untuk mengontrol subjek mengenai apa saja yang dapat diakses yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 6. [1][8]

Gambar 6. Domain Identity and Access Management

3.2.7 Domain Security Operations

Domain Security Operations adalah penggabungan dari topik domain lama *Business Continuity and Disaster Recovery Planning*, *Legal / Regulations / Investigations, & Compliance*, dan *Physical (Environmental) Security*. Penggabungan domain terjadi karena mencakup berbagai konsep dasar keamanan dan praktik terbaik. Domain lama merupakan domain yang memiliki fungsi memperhatikan kontrol dari personil, *hardware*, sistem, teknik *auditing* dan *monitoring* yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 7. [1][8]

Gambar 7. Domain Security Operations

3.2.8 Domain Software Development Security

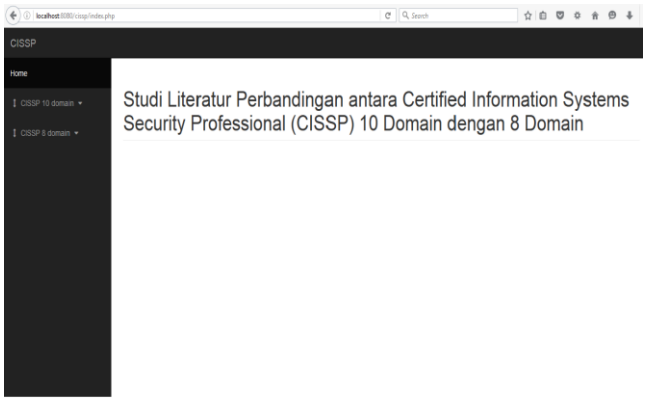
Domain Software Development Security terdiri dari konten yang termasuk dalam domain lama Software Development Security. Penggabungan domain terjadi karena domain baru membahas tentang pengumpulan, penanganan, dan melindungi informasi. Domain lama merupakan domain yang memiliki fungsi memperhatikan resiko dan ancaman, prosedur keamanan, dan keamanan fasilitas dengan memperhatikan lingkungannya yang kemudian digabung menjadi 1 domain baru. Perubahan domain dapat diliat pada Gambar 8. [1][8]

Gambar 8. Domain Software Development Security

4. IMPLEMENTASI SISTEM

4.1 Tampilan Home

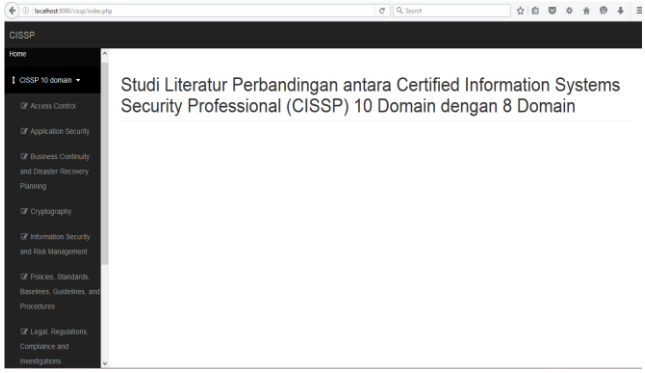
Pada tampilan ini terdapat halaman home dari sebuah *website* domain cissp. Tampilan dapat dilihat pada Gambar 9.



Gambar 9. *Home*

4.2 Tampilan Menu 10 Domain

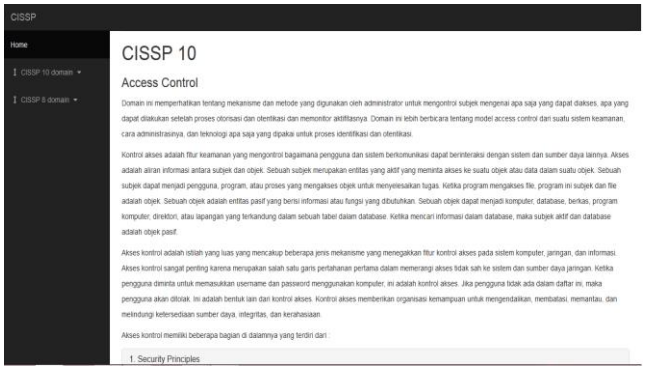
Pada halaman ini terdapat tampilan nama macam-macam domain. Tampilan dapat dilihat pada Gambar 10.



Gambar 10. Menu 10 domain

4.3 Macam-macam nama bagian 10 domain

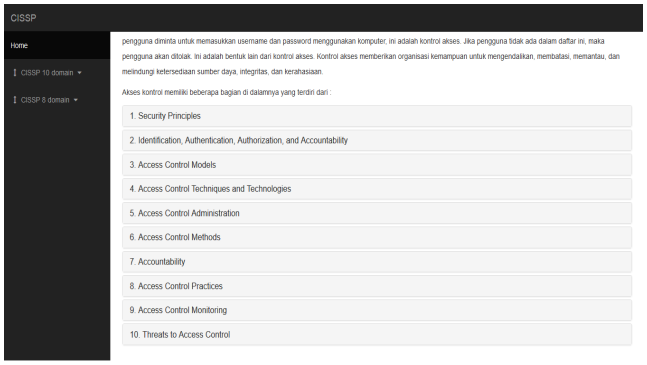
Pada halaman ini terdapat nama bagian dari 10 domain. Tampilan dapat dilihat pada Gambar 11.



Gambar 11. Nama bagian 10 domain

4.4 Bagian dari salah 1 domain

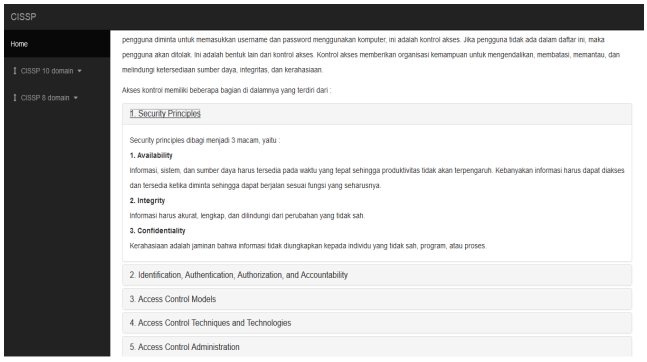
Pada halaman ini terdapat nama bagian-bagian dari suatu domain. Tampilan dapat dilihat pada Gambar 12.



Gambar 12. Bagian dari salah 1 domain

4.5 Pengertian salah 1 domain

Pada halaman ini terdapat model pengertian dari salah 1 domain. Tampilan dapat dilihat pada Gambar 13.



5. KESIMPULAN

5.1 Kesimpulan

Berdasarkan hasil pengujian dapat disimpulkan beberapa hal berikut:

1. CISSP 8 domain merupakan penyempurnaan dari 10 domain.
2. CISSP 8 domain merupakan gabungan dari CISSP 10 domain beserta gabungan dari fungsi-fungsi masing-masing domain.
3. CISSP 8 domain lebih efisien apabila digunakan karena masing-masing domain lebih terfokus kepada apa yang ingin dilakukan dan sudah jelas fungsi dari domain tersebut.

6. DAFTAR REFERENSI

[1] cccure.training. 2016, May 20. Retrieved from CISSP® CBK® 2012 VERSUS THE NEW CISSP® CBK® 2015 MAPPING: https://cccure.training/m/articles/view/CISSP-CBK-2012-VERSUS-THE-NEW-CISSP-CBK-2015-2015-04-12

[2] CISSP (ISC). 2015. CISSP. *Certified Information Systems Security Professional Official Study Guide* Seventh Edition.

[3] CISSP 2015. 2015. Retrieved April 20, 2016, from https://transcender.wordpress.com/tag/cissp/

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

[5] Harris, Shon. 2010. *All-in-One CISSP Exam Guide* Fifth Edition. New York:McGraw-Hill Companies

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

[7] Intl Information System Security Certification Consortium, Inc. 2016, June 1. Retrieved from CISSP® Domains: https://www.isc2.org/cissp-domains/default.aspx

[8] Old vs New CISSP CBK Domains. 2015. Retrieved March 14, 2016, from : https://www.studynotesandtheory.com/cissp-exam-domains-old-vs-new/#.V0fRI-Tl8Qv