BAB 2

LANDASAN TEORI

2.1 Pengukuran

Pengukuran kinerja merupakan hal yang paling penting dan selayaknya dilakukan oleh setiap perusahaan untuk dapat bertahan dan menjadi pemenang dalam persaingan global di pasar internasional. Pengukuran kinerja merupakan suatu proses penilaian kemajuan pekerjaan terhadap pencapaian tujuan dan sasaran yang telah ditentukan, termasuk informasi atas efisiensi penggunaan sumber daya dalam menghasilkan barang dan jasa, kualitas barang dan jasa, perbandingan hasil kegiatan dengan target, dan efektifitas tindakan dalam mencapai tujuan. Dalam hal ini penting untuk ditentukan apakah tujuan pengukuran adalah untuk menilai hasil kinerja (performance outcome) ataukan menilai perilaku (personality) (Hidayat, 2015). Pengukuran kinerja merupakan pendekatan sistematik dan terintegrasi untuk memperbaiki kinerja organisasi dalam rangka mencapai tujuan strategi organisasi dan mewujudkan visi dan misinya (Umairoh, 2015). Menurut penulis, pengukuran kinerja dapat dijadikan sebagai ukuran keberhasilan suatu organisasi dan hasil pengukuran kinerja dapat dijadikan sebagai masukan untuk perbaikan dan peningkatan suatu organisasi di masa yang akan datang.

2.2 Sistem Informasi

Sistem adalah sekumpulan komponen yang saling berhubungan, yang bekerja sama untuk mencapai suatu tujuan dengan menerima masukan dan menghasilkan keluaran melalui proses transformasi yang teratur. Hal ini juga dikemukakan oleh (Satzinger, Jackson, dan Burd, 2010:6), yang mengatakan bahwa sistem adalah kumpulan dari komponen yang tidak berhubungan satu sama lain, yang digunakan bersama-sama untuk mencapai beberapa tujuan. Sistem terbagi menjadi tiga komponen dasar yang saling berinteraksi atau fungsi dasar, yaitu:

a. Input, yaitu bagian yang mencakup pengambilan elemen yang masuk ke dalam sistem untuk di proses
b. Process, yaitu bagian yang mencakup perubahan input menjadi output.
c. Output, yaitu bagian yang mencakup elemen yang dihasilkan dari proses untuk mencapai tujuan yang diinginkan.

Informasi adalah data yang diolah sedemikian rupa sehingga menjadi suatu hasil yang mempunyai arti bagi user tertentu. Hal ini juga dikemukakan oleh (Satzinger, Jackson, & Burd,2010), informasi adalah data yang telah diproses atau diorganisir menjadi sesuatu yang bermakna untuk seseorang. Informasi dibentuk dari kombinasi daya yang diharapkan dapat memiliki makna bagi penerimanya.

Berdasarkan pendapat para ahli diatas, dapat disimpulkan bahwa sistem informasi adalah kumpulan komponen yang tidak berhubungan satu sama lain, namun digunakan bersamasama, diproses, disimpan dan menghasilkan hasil akhir yaitu informasi untuk mencapai tujuan atau memenuhi kebutuhan. Hal ini disampaikan juga oleh Satzinger, Jackson, dan Burd (2010), yang mengatakan

bahwa sistem informasi adalah kumpulan komponen yang saling berhubungan satu sama lain yang dikumpulkan, di proses, di simpan, dan menghasilkan informasi yang dibutuhkan sebagai output, dimana yang dibutuhkan untuk menyelesaikan sebuah tugas bisnis.

2.3 Keamanan Informasi

(ISACA COBIT 5 For information security, 2012) mendefinisikan keamanan informasi sebagai sesuatu yang memastikan bahwa di dalam sebuah enterprise, informasi terlindungi dari pembukaan / penyungkapan oleh pengguna yang tidak berwenang (confidentiality), Modifikasi yang tidak tepat (integrity) dan tidak adanya akses ketika diperlukan (availability).

a. Confidentiality berarti melindungi pembatasan akses dan pengungkapan, termasuk juga melindungi privasi dan kepemilikan informasi.
b. Integrity berarti menjaga terhadap modifikasi atau perusakan informasi dan termasuk juga memastikan tidak-tersangkalnya informasi dan keasliannya
b) Availability berarti memastikan ketepatan dan akses yang handal dalam penggunaan informasi.

2.4 Website

Menurut penjelasan (Suryayusra, 2014) Website adalah sekumpulan halaman informasi yang disediakan melalui jalur internet sehingga dapat diakses seluruh dunia selama terkoneksi dengan jaringan internet tanpa terbatas ruang dan waktu. Website merupakan sebuah komponen yang terdiri dari teks, gambar, suara animasi sehingga menjadi media informasi yang menarik untuk dikunjungi oleh banyak orang.

Dikutip dari *http://www.pengertianku.net* dan ditulis oleh (Saputro, Hendra, W. 2007), Pengertian *website* dan jenisnya – *Website* adalah sering juga disebut *Web*, dapat diartikan suatu kumpulan-kumpulan halaman yang menampilkan berbagai macam informasi teks, data, gambar diam ataupun bergerak, data animasi, suara, video maupun gabungan dari semuanya, baik itu yang bersifat statis maupun yang dinamis, yang dimana membentuk satu rangkaian bangunan yang saling berkaitan dimana masing-masing dihubungkan dengan jaringan halaman atau *hyperlink*.

Atau definisi *website* adalah kumpulan dari berbagai macam halaman situs, yang terangkum didalam sebuah domain atau juga subdomain, yang lebih tempatnya berada di dalam *WWW* (*World Wide Web*) yang tentunya terdapat di dalam Internet.

Halaman *website* biasanya berupa dokumen yang ditulis dalam format *Hyper Text Markup Language* (*HTML*), yang bisa diakses melalui *HTTP*, *HTTP* adalah suatu protokol yang menyampaikan berbagai informasi dari server *website* untuk ditampilkan kepada para *user* atau pemakai melalui *web browser*.

2.5 *CVSS (Common Vulnerability Scoring System)*

Menurut (M. Khan,2015) Security metrics merupakan pengukuran kuantitatif untuk menilai operasi keamanan di organisasi membantu organisasi untuk membuat keputusan tentang berbagai aspek keamanan yang meliputi arsitektur keamanan dan kontrol untuk efektivitas dan efisiensi operasi keamanan.

Menurut (Radack,2008) Security metrics dapat diukur dengan skala 1-10 dimana 10 adalah sistem sangat tidak aman dan bisa ditembus penyerang selain itu, security metrics berharga untuk tingkat manajerial TI dan stakeholder yang mempertanyakan dampak keamanan terhadap bisnis proses dan kegiatan. NIST (National Institute of Standards and Technology) mengkategorikan security metrics menjadi 3 tipe sebagai berikut :

a. implementation metrics yaitu dimaksudkan untuk menunjukkan kemajuan dalam mengimplementasikan informasi program keamanan, kontrol keamanan, dan kebijakan prosedur yang terkait
b. effectiveness/efficiency metrics yaitu dimaksudkan untuk memantau apakah program tingkat proses dan sistem tingkat kontrol keamanan diterapkan dengan benar, operasi sebagaimana yang dimaksud serta memperoleh hasil yang diinginkan
c. impact metrics yaitu dimaksudkan untuk mengartikulasikan dampak keamanan informasi pada misi organisasi.

Menurut First.org (2018) security metrics pada Proyek Akhir ini dinilai dengan parameter yaitu vulnerability assessments yang dimaksud dengan vulnerability adalah suatu kelemahan program/infrastruktur yang memungkinkan

terjadinya exploitasi sistem. Kerentanan(vulnerability). Selanjutnya dilakukan perhitungan Common Vulnerability Scoring System menggunakan metode sebagai berikut.

a. Base score/overall score mewakili karakteristik intrinsik dan mendasar dari kerentanan yang konstan seiring waktu dan lingkungan pengguna.
b. Temporal score mewakili karakteristik kerentanan yang berubah dari waktu ke waktu namun tidak diantara lingkungan pengguna.

Environmental score mewakili karakteristik kerentanan yang relevan dan unik bagi lingkungan pengguna tertentu.

2.5.1 *Base metrics*

2.5.1.1 *Exploitability Metrics*

Seperti disebutkan sebelumnya, metrik Eksploitasi mencerminkan karakteristik dari hal yang rentan, yang kami sebut secara formal sebagai komponen rentan. Oleh karena itu, setiap metrik Eksploitasi yang tercantum di bawah ini harus diberi skor relatif terhadap komponen rentan, dan mencerminkan sifat kerentanan yang mengarah pada serangan yang berhasil.

Saat mencetak metrik Basis, harus diasumsikan bahwa penyerang memiliki pengetahuan tingkat lanjut tentang kelemahan sistem target, termasuk konfigurasi umum dan mekanisme pertahanan default (mis., Firewall bawaan, batas kecepatan,

kebijakan lalu lintas). Sebagai contoh, mengeksploitasi kerentanan yang menghasilkan keberhasilan deterministik yang berulang dan masih harus dianggap sebagai nilai Rendah untuk Kompleksitas Serangan, terlepas dari pengetahuan atau kemampuan penyerang. Selain itu, mitigasi serangan spesifik target (mis., Filter firewall khusus, daftar akses) mestinya dicerminkan dalam grup penilaian metrik lingkungan.

Konfigurasi spesifik tidak boleh memengaruhi atribut apa pun yang berkontribusi pada Skor Dasar CVSS, yaitu, jika konfigurasi spesifik diperlukan agar serangan berhasil, komponen yang rentan harus diberi skor dengan asumsi berada dalam konfigurasi itu.

2.5.1.1 *Access Vector*

Access vector (AV) menunjukkan bagaimana kerentanan dapat dieksploitasi. Metrik ini mencerminkan konteks di mana eksploitasi kerentanan dimungkinkan.

Tabel 2.1 *Access Vector*

Value	Description
Local (L)	Penyerang harus memiliki akses fisik ke sistem yang rentan (mis. Serangan firewire) atau akun lokal (mis. Serangan dengan menggunakan akun yang sudah terdaftar).
Adjacent Network (A)	Penyerang harus memiliki akses ke domain broadcast (mis. ARP spoofing, serangan bluetooth).
Network (N)	*User interface* yang rentan bekerja di lapisan 3 atau di atas Jaringan OSI. Jenis kerentanan ini sering digambarkan sebagai yang dapat dieksploitasi dari jarak jauh (mis. Buffer overflow jarak jauh dalam layanan jaringan)

2.5.1.2 *Attack Complexity*

Attack complexity (AC) metrik menggambarkan betapa mudah atau sulitnya untuk mengeksploitasi kerentanan yang ditemukan.

Tabel 2.2 *Attack Complexity*

Value	Description
High (H)	Ada kondisi khusus, seperti persyaratan untuk metode rekayasa sosial yang akan segera diperhatikan oleh orang yang berpengetahuan.
Medium (M)	Ada beberapa persyaratan tambahan untuk level ini, seperti batas serangan, atau persyaratan agar sistem rentan dijalankan dengan konfigurasi non-default yang tidak umum.
Low (L)	Tidak ada kondisi khusus untuk mengeksploitasi kerentanan, seperti ketika sistem tersedia untuk pengguna tanpa adanya pembatasan akses, atau konfigurasi yang rentan ada di mana-mana.

2.5.1.3 *Authentication*

Menjelaskan berapa kali penyerang harus mengautentikasi ke target untuk mengeksploitasinya.

Tabel 2.3 *Authentication*

Value	Description
Multiple (M)	Eksploitasi kerentanan mengharuskan penyerang mengotentikasi dua atau lebih kali, bahkan jika kredensial yang sama digunakan setiap kali.
Single (S)	Penyerang harus mengautentikasi sekali untuk mengeksploitasi kerentanan.
None (N)	Tidak ada persyaratan bagi penyerang untuk mengotentikasi.

2.5.2 *Impact Metrics*

Metrik Dampak menangkap efek dari kerentanan yang berhasil dieksploitasi pada komponen yang menderita hasil terburuk yang paling langsung dan dapat diprediksi terkait dengan serangan itu. Analis harus membatasi dampak pada hasil akhir yang masuk akal yang mereka yakini mampu dicapai oleh penyerang.

Hanya peningkatan akses, hak istimewa yang diperoleh, atau hasil negatif lainnya sebagai hasil dari eksploitasi yang berhasil yang harus dipertimbangkan ketika menilai metrik Dampak dari kerentanan. Misalnya, pertimbangkan kerentanan yang memerlukan izin hanya baca sebelum dapat mengeksploitasi kerentanan. Setelah eksploitasi berhasil, penyerang mempertahankan tingkat akses baca yang sama, dan

memperoleh akses tulis. Dalam hal ini, hanya metrik dampak Integritas yang harus dinilai, dan metrik Dampak Kerahasiaan dan Ketersediaan harus ditetapkan sebagai Tidak Ada.

Perhatikan bahwa saat membuat skor perubahan dampak delta, dampak akhir harus digunakan. Misalnya, jika penyerang mulai dengan akses parsial ke informasi terbatas (Kerahasiaan Rendah) dan eksploitasi kerentanan yang berhasil mengakibatkan hilangnya kerahasiaan (Kerahasiaan Tinggi), maka Skor Pokok CVSS yang dihasilkan harus merujuk pada nilai metrik dampak "end game" (Kerahasiaan Tinggi).

Jika perubahan ruang lingkup belum terjadi, metrik Dampak harus mencerminkan dampak Kerahasiaan, Integritas, dan Ketersediaan terhadap komponen yang rentan. Namun, jika perubahan ruang lingkup telah terjadi, maka metrik Dampak harus mencerminkan dampak Kerahasiaan, Integritas, dan Ketersediaan untuk komponen rentan, atau komponen yang terkena dampak, yang mana yang menderita hasil paling parah.

2.5.2.1 *Confidentiality*

Confidentiality (C) metric menjelaskan dampak pada kerahasiaan data yang diproses oleh sistem.

Tabel 2.4 *Confidentiality*

Value	Description
None (N)	Tidak ada dampak pada kerahasiaan sistem.
Partial (P)	Ada banyak pengungkapan informasi, tetapi ruang lingkup kerusakan dibatasi sehingga tidak semua data tersedia.
Complete (C)	Ada total pengungkapan informasi, menyediakan akses ke semua / semua data pada sistem. Atau, akses ke hanya beberapa informasi terbatas diperoleh, tetapi informasi yang diungkapkan menyajikan dampak langsung dan serius.

2.5.2.2 *Integrity*

Integrity (I) metric menjelaskan dampak pada integritas sistem yang dieksploitasi

Tabel 2.5 *Integrity*

Value	Description
None (N)	Tidak ada dampak pada integritas sistem.
Partial (P)	Modifikasi beberapa data atau file sistem dimungkinkan, tetapi ruang lingkup modifikasi terbatas.
Complete (C)	Ada total integritas yang hilang; penyerang dapat memodifikasi file atau informasi apa pun pada sistem target.

2.5.2.3 *Availability*

The availability (A) metric menjelaskan dampak pada ketersediaan sistem target. Serangan yang menggunakan bandwidth jaringan, siklus prosesor, memori atau sumber daya lainnya memengaruhi ketersediaan sistem.

Tabel 2.6 *Availability*

Value	Description
None (N)	Tidak ada dampak pada ketersediaan sistem.
Partial (P)	Ada penurunan kinerja atau hilangnya beberapa fungsi.
Complete (C)	Ada total kehilangan ketersediaan sumber daya yang diserang.

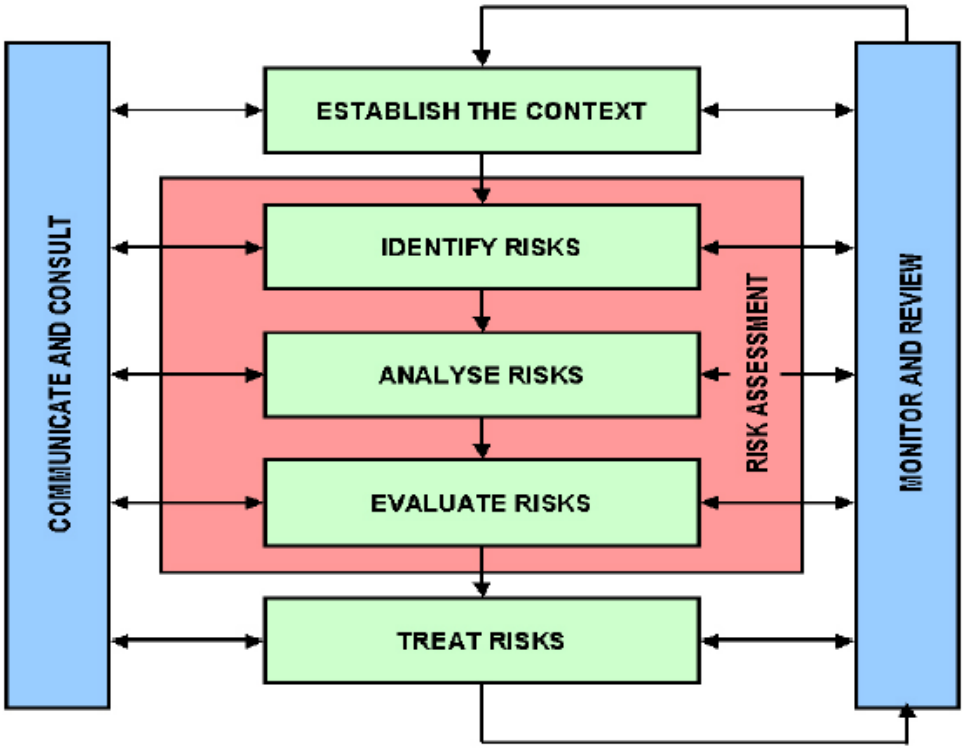
2.6 *Vulnerability*

Menurut (Rainer,2012:83) berkata vulnerability adalah kemungkinan bahwa sistem akan dibahayakan nantinya oleh threat atau ancaman. Menurut Rainer, saat ini terdapat lima faktor kunci yang berkontribusi terhadap meningkatnya kerentanan sumber informasi organisasi, sehingga jauh lebih sulit untuk mengamankan mereka.

a. Lingkungan bisnis saat ini yang sudah online, yang saling terkait dan saling bergantung satu sama lain.
b. Komputer dengan perangkat yang lebih kecil, lebih cepat dan lebih murah.
c. Kebutuhan skill yang menurun untuk menjadi hacker komputer.
d. Kejahatan terorganisir internasional yang mengambil alih cybercrime.
b. Kurangnya dukungan manajemen.

2.7 *E-Satisfaction*

Menurut (Jawaharlal Nehru,2011) mengatakan bahwa bahwa ISO 31000: 2009 memberikan prinsip, kerangka kerja dan proses untuk mengelola risiko. Ini bisa digunakan oleh organisasi manapun terlepas dari ukuran, aktivitas atau sektornya. Menggunakan ISO 31000 dapat membantu organisasi meningkatkan kemungkinan pencapaian tujuan, memperbaiki identifikasi peluang dan ancaman dan mengalokasikan dan menggunakan sumber daya secara efektif untuk penanganan risiko.



Gambar 2.1 Gambaran Umum Risk Management ISO 31000:2009

Seperti yang telah disebutkan di atas tata kelola resiko merupakan salah satu opsi untuk mengelola keamanan informasi. Risk Management (Manajemen Resiko) menurut (Evan Wheeler,2011:46) mempunyai aliran proses kerja (workflow) yang terdiri dari:

a. Resource Proffiling, mendeskribsikan sumber daya dan sensitifitasnya terhadap resiko
b. Risk Assesment, identifikasi dan menilai ancaman (threats), kerentanan (vulnerability) dan resiko.
c. Risk Evaluation. Keputusan untuk menerima, mencegah, memindahkan, atau meminimalisir resiko.
d. Document, mendokumentasikan keputusan resiko dari proses Risk Evaluation.

e. Risk Mitigation, implementasikan pengurangan resiko dengan kontrol yang spesifik
f. Validation, tes kontrol untuk memastikan bahwa risk mitigation yang telah diimplementasikan sesuai dengan penilaian resiko yang telah dibuat
g. Monitoring and Audit

Workflow tersebut merupakan bentuk dasar dari tata kelola resiko yang biasa digunakan oleh perusahaan. Nama Risk Management diciptakan untuk menggambarkan tindakan yang dilakukan untuk mengamankan sumber informasi perusahaan dari resiko yang dihadapi dengan meminimalisir dampak dari ancaman yang ada sehingga membuat tingkat resiko semakin kecil dampaknya.

2.8 *BCP (Business Continuity Plan*

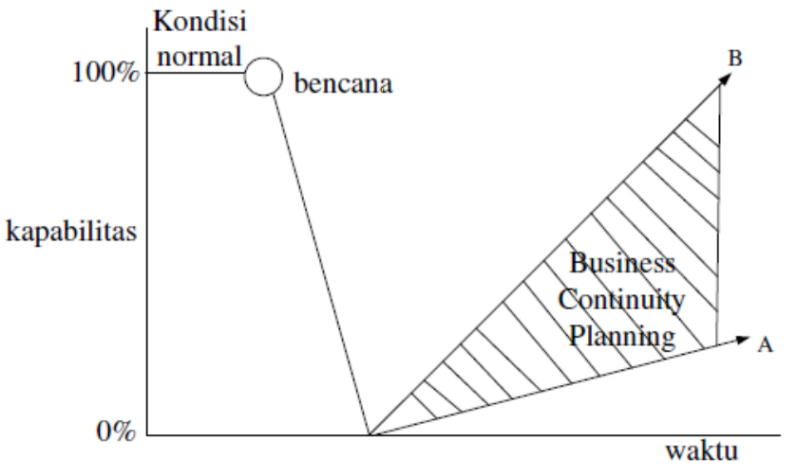
Business Continuity Plan merupakan sebuah metode untuk mengidentifikasi,memperoleh, mengembangkan dan mendokumentasikan sumber daya dan prosedur yang diikuti dengan pengujian untuk memastikan keberlangsungan critical operation dari sebuah organiasasi ketika sebuah musibah menyerang. Sebuah Business Continuity Plan dikatakan berhasil ketika tercipta rencana yang membantu sebuah organisasi untuk tetap bisa menjalankan critical business processnya setelah terkena bencana (Dushie, 2014)

Business Continuity Plan ditujukan untuk memenuhi kebutuhan bisnis dalam menghadapi ancaman-ancaman terhadap operational perusahaan. Business Continuity Plan dan Disaster recovery Plan meliputi beberapa tahap antara lain persiapan, pengujian dan pemutakhiran aktivitas-aktivitas yang diperlukan untuk

melindungi proses bisnis perusahaan yang bersifat kritikal terhadap dampak dari kegagalan jaringan dan sistem utama yang dimiliki.

Prioritas utama dari semua perencanaan keberlangsungan bisnis dan pemulihan bencana adalah sumber daya manusia.Terlepas dari pentingnya kekuatan modal, serta kembali beroperasinya aktivitas bisnis normal, serta issue seputar keberlanjutan bisnis lainya, perhatian utama yang harus ditangani dalam sebuah perencanaan adalah menghindarkan manusia dalam hal ini adalah karyawan/pegawai dari bahaya atau ancaman dalam sebuah bencana. Jika dalam kondisi tertentu terdapat pertentangan apakah menyelamatkan hardware atau data dibandingkan manusia dari ancaman bahaya, maka keselamatan terhadap manusia harus lebih diutamakan. Keselamatan dan proses evakuasi personel harus menjadi komponen pertama dalam perencaaan menghadapi sebuah bencana.

Berikut adalah gambaran pemulihan proses bisnis menggunakan BCP



Gambar 2.2 *Business Continuity Planning* (Puspitasari, 2011)

Menjelaskan ketika dalam kondisi normal, kapabilitas proses bisnis dapat mencapai 100%. Namun pada saat bencana ataupun gangguan yang menimpa perusahaan, kelangsungan bisnis organisasi akan mengalami gangguan untuk beberapa saat. Garis A menunjukan pemulihan proses bisnis tanpa melalui BCP, sedangkan garis B menunjuakkan pemulihan proses bisnis menggunakan BCP. Tampak jelas pada gambar tersebut, dengan menggunakan BCP, kelangsungan proses bisnis organisasi dapat terjaga.(Puspitasari, 2011)

2.9 *E-Government*

Menurut (Samodra Wibawa 2009:113), E-Government adalah penggunaan teknologi informasi oleh instansi pemerintah seperti wide area Networks (WAN) internet, moble competing, yang dapat digunakan untuk membangun hubungan dengan masyarakat, dunia usaha dan instansi pemerintah lainnya.

Sedangkan menurut (Falih Suaedi, Bintoro Wardianto 2010:54), E-Government ialah sebagai upaya pemamfaatan informasi dan teknologi komunikasi untuk meningkatkan efesiensi dan efektivitas, transfaransi dan akuntabilitas pemerintah dalam memberikan pelayanan publik secara lebih baik.

Menurut Clay G. Weslatt (15 Agustus 2007) dalam website, E-Government adalah menggunakan teknologi informasi dan komunikasi untuk mempromosikan pemerintah yang lebih effisien dan penekanan biaya yang efektif, kemudian pasilitas layanan terhadap masyarakat umum dan membuat pemerintah lebih bertanggung jawab kepada masyarakat.

2.10 Penelitian Terdahulu

Refresi pertama berjudul, "Pemeringkatan Risiko Keamanan Sistem Jaringan Komputer Politeknik Kota Malang Menggunakan CVSS dan FMEA" penelitian ini dilakukan oleh (Betta Wahyu Retna Mulya & Avinanta Tarigan). Tujuan dari penelitian ini menghasilkan suatu Penelitian ini akan dilihat bagaimana memastikan bahwa penggunakan Common Vulnerability Scoring System (CVSS) dan Failure Mode and Effect Analysis (FMEA) memungkinkan untuk menilai, membandingkan, memahami, serta memprioritaskan patching vulnerability pada sistem jaringan komputer, dengan demikian mampu memprioritaskan penanganannya sesuai dengan tingkat risikonya. Analisis menggunakan CVSS digunakan untuk mengetahui dampak potensial akibat vulnerability sedangkan FMEA digunakan untuk mengetahui urutan prioritas penanganan potensi kegagalan yang ditimbulkan oleh celah keamanan.

Hasil penelitian, berikut ini merupakan beberapa hasil yang dapat diambil :

1. Penggunaan Metode CVSS hanya memperhatikan segi vulnerability saja tanpa memperhatikan celah keamanan dari faktor user awareness dan sistem infrastruktur jaringan komputer.
2. Hasil analisis dari penggabungan dua metode CVSS dan FMEA dapat menentukan peringkat penanganan berdasarkan dampak potensial yang ditimbulkan akibat kerentanan dan celah keamanan disistem jaringan komputer Politeknik Kota Malang.

Refresi kedua berjudul, *"Common vulnerability scoring system"* penelitian ini dilakukan oleh (Mell, P., Scarfone, K., Romanosky, S). Tujuan dari penelitian ini adalah memastikan CVSS dapat memberikan scoring sesuai dengan tingkat kerentanan suatu objek penelitian.

Hasil penelitian, berikut ini merupakan beberapa hasil yang dapat diambil : CVSS dapat diandalkan sebagai media pengukuran tingkat kerentanan suatu objek dengan nggolongkan subscorenya ke dalam berbagai aspek seperti :

1. Access vector (AV) menunjukkan bagaimana kerentanan dapat dieksploitasi.
2. Attack complexity (AC) metrik menggambarkan betapa mudah atau sulitnya untuk mengeksploitasi kerentanan yang ditemukan.
3. Authentication (Au) menjelaskan berapa kali penyerang harus mengautentikasi ke target untuk mengeksploitasinya.
4. Confidentiality (C) metric menjelaskan dampak pada kerahasiaan data yang diproses oleh system.
5. Integrity (I) metric menjelaskan dampak pada integritas sistem yang dieksploitasi.
6. The availability (A) metric menjelaskan dampak pada ketersediaan sistem target.

Refresi Ketiga berjudul, "*The Common Vulnerability Scoring System (CVSS) generations – usefulness and deficiencies*" penelitian ini dilakukan oleh (Attila Horváth, Péter Máté Erdősi, dan Ferenc Kiss). Tujuan dari penelitian ini menerangkan fungsi dan kekurangan dari pengunaan CVSS secara keseluruhan dengan nilai pengukuran yang konsisten hasil yang dapat diandalkan

Hasil penelitian, berikut ini merupakan beberapa hasil yang dapat diambil :

Jadi CVSS sangat berguna, tetapi tidak untuk mengukur keamanan keseluruhan, bahkan dalam hal teknologi perangkat lunak. CVSS adalah cara alternatif penilaian risiko

Refresi Keempat berjudul, "*Risk Assessment in Online Banking System*" penelitian ini dilakukan oleh (K.V.D. Kiran, P.Sruthi, P.S. Neema, G.V.S. Manju Vani, dan Rishikesh Sahu). Tujuan dari penelitian ini adalah menerangkan manfaat penggunaan CVSS dalam Banking system,

Hasil penelitian, berikut ini merupakan beberapa hasil yang dapat diambil :

Penilaian Risiko memainkan peran penting dalam memberikan keamanan informasi perbankan. Sektor perbankan adalah salah satu aplikasi utama sistem terdistribusi. Berbagai aset dan kerentanan yang terlibat dalam aplikasi perbankan terdistribusi diidentifikasi. Metodologi dan alat penilaian risiko yang digunakan juga memainkan peran penting dalam menilai risiko dalam keamanan informasi. Dalam kasus ini penggunaan metode CVSS dapat memberikan peringkat akumulasi kerentanan untuk menentukan prioritas penanganan yang harus dilakukan oleh perusahaan.