Vulnerability Assessment untuk Meningkatkan Kesadaran Pentingnya Keamanan Informasi

Anjar Priandoyo
Technology and Security Risk Services - Ernst & Young
Jakarta Stock Exchange Building, Tower 2, 6th floor.
Jl Jend Sudirman, Kav. 52-53 Jakarta 12190
Email : anjar.priandoyo@id.ey.com

Abstract

The information security awareness is just become priority after data loss or damage happen. This makes the information system user is not ready to solve or minimize the risk that could be happen. Vulnerability assessment or a process to measure the system weaknesses from outsider attack could be the effective way for preventive control implementation against the risk that could be happen.

This paper describe how vulnerability assessment as a phase in information security framework, how to perform vulnerability assessment, analyzing the result and how deliver the result to the management and give significant impact for the information technology activity and for the business activity in the company.

Keywords: *Vulnerability assessment, Security awareness, Preventive control*

1. Pendahuluan

Pengukuran atau *assessment* adalah hal yang mutlak dilakukan untuk mendapatkan peningkatan kualitas. Suatu perusahaan dapat meningkatkan penjualannya bila mengetahui bagaimana tingkat penjualannya, bagaimana efisiensinya. Dengan adanya pengukuran maka perusahaan dapat mengetahui kelemahan yang ada, membandingkannya dengan contoh penerapan di perusahaan lain dan ujungnya adalah peningkatan keuntungan perusahaan.

VA adalah salah satu cara pengukuran terhadap keamanan sistem. VA merupakan salah satu bagian pengendalian preventif dalam keseluruhan rangkaian pengendalian TI, disamping berbagai metode pengendalian terhadap keamanan yang lain seperti detektif dengan IDS (*Intrusion Detection System*), atau preventif dengan firewall dan antivirus. VA diharapkan dapat menjadi acuan bagaimana seharusnya pengawasan dan pengendalian akan keamanan informasi dalam perusahaan.

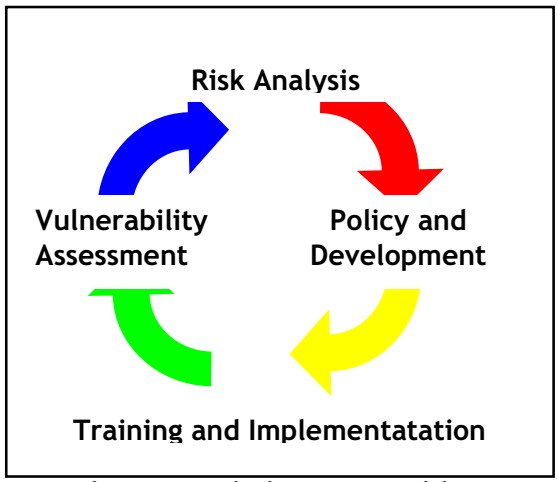
Proses VA bisa diselenggarakan oleh internal departemen TI ataupun oleh pihak ketiga seperti firma audit TI atau konsultan TI. Dapat diselenggarakan dengan dana terbatas ataupun dengan spesialis dalam jumlah besar. Pelaksanaaan VA disesuaikan dengan kondisi perusahaan, jenis industri hingga kebutuhan perusahaan tersebut.

Pada prakteknya di industri, permintaan akan VA umumnya datang setelah terjadi proses pemeriksaan TI yang kemudian berlanjut pada pemeriksaan keamanan data. VA seringkali merupakan tindak lanjut dari proses perencanaan strategi keamanan informasi, kelengkapan standar industri hingga faktor regulasi. Di Indonesia sebagian besar permintaan VA datang dari industri yang memiliki ketergantungan tinggi pada TI seperti industri perbankan atau telekomunikasi atau pun dari industri yang sudah matang dalam pengelolaan TI-nya.

2. Vulnerability Assessment

VA merupakan bagian dari proses *risk assessment* seperti digambarkan Michael Greg dalam sebuah lingkaran siklik antara:

- Analisa Resiko (*Risk analysis*)
- *Policy development*
- *Training & implementation*
- *Vulnerability assessment & penetration testing*



Gambar 1. Lingkaran Siklik Vulnerability Assessment

Sebagai sebuah proses yang terus menerus dan membentuk suatu kerangka siklik maka hasil dari VA akan digunakan untuk mengimplementasikan strategi keamanan informasi di perusahaan tersebut. Begitupun strategi keamanan yang telah dibuat harus tetap dievaluasi.

Sebagai suatu proses VA sebaiknya dilakukan secara kontinu dan terus menerus, umumnya VA ini dilakukan :

- Saat implementasi program baru, pada implementasi program baru biasanya departemen TI akan membuka akses ke mesin *production* oleh pihak ketiga seperti *programmer*, *vendor* ataupun *consultant*. Implementasi ini dimungkinkan menyebabkan terbukanya lubang kerawanan baru yang belum ada.

- Secara periodik dalam waktu-waktu tertentu, digunakan untuk memantau apabila ada perubahan yang dilakukan oleh pengguna akhir. VA secara periodik inilah yang dinilai sebagai cara yang paling baik.

Proses VA sendiri memiliki berbagai tingkatan, sehingga perusahaan dapat memilih tingkatan mana yang akan digunakan dalam pengukurannya. Tingkatan ini dapat di sesuaikan dengan kondisi di masing-masing tempat.

- Tingkat I: Pengukuran peraturan dan kebijakan (*Policy assessment*)
  Pengukuran ini meliputi peraturan, kebijaksanaan, standar operasi di *client* dalam cakupan keamanan informasi.

- Tingkat II: Evaluasi Jaringan
  Pengukuran ini meliputi kinerja jaringan, keamanan jaringan hingga ancaman-ancaman terhadap jaringan kerja. Pengukuran jenis ini memerlukan alat bantu seperti *scanning* atau *data capture*. Evaluasi jaringan ini bertujuan untuk mendapatkan informasi mengenai kondisi sebenarnya yang terjadi dilapangan, bagaimana tingkat kesadaran akan keamanan informasi yang sudah diterapkan selama ini.
- Tingkat III: Test penetrasi (*Penetration Test*)
  Penetration test sebenarnya menggunakan prinsip yang sama dengan network evaluation dimana pembedanya bahwa *penetration test* dilakukan dalam kondisi gelap, tanpa mengetahui konfigurasi dan kondisi sebenarnya seperti apa. Pada test penetrasi maka assesor akan menjumpai sistem sebagai sebuah kotak tertutup menghadapi penetrasi yang datang dari luar.

3. Proses *Vulnerability Assessment*

Dalam tataran konsep proses VA merupakan proses yang sangat kompleks karena melibatkan seluruh komponen dalam TI. Dalam tataran teknis pun merupakan proses yang beresiko mengingat adanya peluang untuk merusak atau mengganggu kinerja sistem yang berlangsung.

Proses VA secara garis besar dapat dibagi dalam tiga tahapan :

1. Penentuan batasan proyek
2. Pelaksanaan *assessment*

3. Pelaporan akhir

Proses VA ini dilaksanakan secara terkendali dimana tahapan yang satu tidak bisa mendahului tahapan yang lain. Setiap tahap yang dilakukan harus didasari atas koordinasi setiap pihak yang terkait dalam proses bisnis.

3.1 Batasan proyek

Penentuan batasan proyek merupakan tahapan yang paling kritikal, penentuan batasan ini harus diikuti oleh semua pihak yang terkait. Mulai dari manager TI, manager keuangan / pengguna akhir, hingga operator itu sendiri, bila proses *assessment* melibatkan pihak ketiga maka tentunya selain harus dihadiri assesor yang sudah melakukan survey awal sebelumnya.

Pembatasan proyek ini diperlukan agar VA tidak terlalu luas sehingga merambah ke hal-hal lain yang kurang signifikan atau agar VA tidak terlampau sempit sehingga melewatkan hal-hal yang lebih kritikal. Pembatasan proyek ini juga meliputi besarnya dana yang akan diperlukan, hingga jumlah tenaga yang akan mengerjakannya.

Langkah yang harus dilakukan untuk dapat menentukan batasan VA dengan baik adalah:

1. Pemahaman terhadap proses bisnis
   Pemahaman proses bisnis merupakan hal yang paling penting, dari proses bisnis yang telah dipahami maka assesor dapat menentukan strategi pengukuran yang harus dilakukan.

   Sebagai contoh, sebuah perusahaan ISP tentunya memiliki bisnis *bandwith* yang pemrosesan pendapatannya (*revenue processor*) adalah sistem *billling*. Sehingga ketersediaan layanan merupakan hal yang paling penting dalam proses bisnis sementara kerusakan dalam sistem billing merupakan komponen yang paling signifikan untuk diperiksa dalam VA, mengingat proses keuntungan perusahaan dilihat dari titik ini.

   Namun dalam kasus yang berbeda seperti perusahaan manufaktur maka proses ketersediaan barang merupakan hal yang paling penting dalam proses bisnis. Sementara kerusakan atau pencurian data pada sistem ERP merupakan komponen yang paling signifikan untuk diperiksa.

   Strategi VA pada sistem TI dengan fokus utama sistem billing dengan strategi pada sistem dengan fokus utama manufaktur tentunya berbeda. Dalam perspektif yang lebih luas maka industri perbankan dengan *Core Banking System*-nya, industri telekomunikasi dengan

Billing System dan manufaktur dengan ERP-nya akan menjadi dasar batasan VA ini.

2. Pemahaman kompleksitas sistem
   Sebuah perusahaan dengan tiga lokasi, sistem komunikasi dengan jaringan optik. Tentunya akan memiliki kompleksitas yang berbeda dibandingkan dengan perusahaan yang memiliki 70 lokasi dan ribuan sub lokasi seperti perbankan. Kompleksitas bisa dilihat dari luasan jaringan komunikasi yang digunakan, banyaknya sistem yang ada hingga jumlah orang yang ada.

   Kompleksitas dan proses bisnis kemudian menjadi bekal assesor untuk menentukan proses VA yang akan dikerjakan seperti apa. Dengan data seperti ini assesor pun dapat menentukan dari sistem mana ia akan memulai, bagaimana alat-alat yang digunakan hingga tenaga ahli apa yang harus ada.

   Sebagai studi kasus pada client dengan skala menengah dengan satu sistem ERP dan tiga lokasi kerja misalnya, maka assesor bisa membagi cakupan VA dalam beberapa periode. Misalkan untuk periode bulan januari dilakukan pengukuran pada server aplikasi dan database. Kemudian pada bulan berikutnya dilakukan pengukuran terhadap keamanan dan kinerja jaringan.

3. Penentuan biaya dan waktu.

3.2 Pelaksanaan *Assessment*

Setelah batasan proyek ditentukan maka proses VA masuk dalam tahap pelaksanaan. Dalam tahapan ini diasumsikan semua kebutuhan *assessment* telah didefinisikan sebelumnya. Jika perusahaan menginginkam pengukuran akan SOP (standar operasional dan prosedur) tentunya sudah ada standar penerapan dilapangan yang akan dijadikan acuan.

Begitu juga bila pengukuran terhadap standar keamanan sistem maka sudah ada acuan bagaimana standar keamanan sistem yang diterapkan dilapangan. Data-data acuan ini tersedia dalam ranah publik, dikeluarkan oleh vendor produk maupun dikeluarkan oleh organisasi independen yang melakukan rating terhadap resiko keamanan.

Tingkat I : Peraturan dan kebijakan (*Policy assessment*)

Dilihat dari beban kerjanya, *policy assessment* merupakan tingkat yang paling ringan, karena berupa pengumpulan berkas-berkas administrasi. Namun hal ini juga perlu diperhatikan dengan baik oleh assessor untuk juga melihat efektivitas dari *policy* dan *procedure* yang dibuat. Apakah informasi yang tersedia sudah mampu menggambarkan kondisi yang sebenarnya dilapangan atau tidak. Apakah informasi yang tersedia sudah

jelas dan mudah dipahami, tidak malah membuat pengguna semakin bingung.

Peraturan yang sebaiknya ada adalah yang terkait dengan:

1. Penggunaan layanan TI seperti: *email, domain account, internet*
2. Permohonan akses pada layanan, permohonan perubahan program, permohonan perbaikan sistem

Dalam prakteknya dilapangan peraturan ini dibuat bervariasi dalam sebuah dokumen terkendali yang terintegrasi, dalam sebuah dokumen yang terpisah baik secara formal dengan persetujuan dari pimpinan tertinggi perusahaan ataupun secara non formal dari *technical support* dan pengguna akhir. Assessor perlu memiliki kejelian dimana dan bagaimana peraturan tersebut diterapkan.

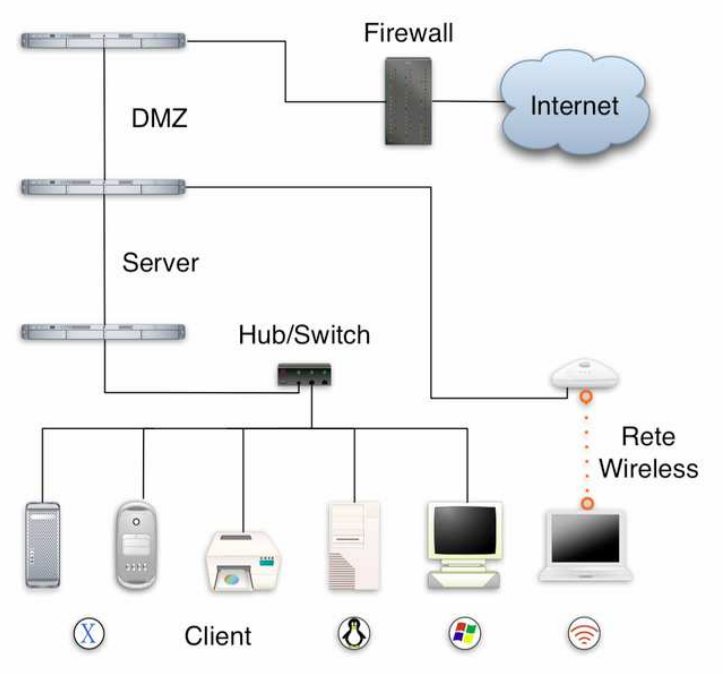
Saat melakukan evaluasi peraturan dan kebijakan assessor perlu melakukan wawancara dengan pengguna akhir ataupun *system administrator* secara langsung. Hal ini didasari bahwa ada banyak ketidaksesuaian antara peraturan yang ada dan pelaksanaan dilapangan. Assessor tidak bisa semata-mata bersandar pada bukti tertulis yang didapatkan tapi juga dari wawancara langsung.

Selain wawancara juga diperlukan survey terhadap lokasi VA sehingga gambaran mengenai kondisi pengelolaan TI bisa didapatkan secara menyeluruh.

Tingkat II: Evaluasi Jaringan

Evaluasi jaringan dan keamanannya merupakan tahapan paling penting dalam proses VA, dalam proses ini assessor akan menggunakan alat bantu VA *scanning*. Alat bantu ini bisa berupa alat bantu komersil seperti Retina, GFI Languard, Symantec Vulnerability ataupun alat bantu non komersial seperti Nessus.

Alat bantu ini biasanya dijalankan oleh sistem administrator yang bersangkutan, ataupun oleh assessor atas sepengetahuan penanggung jawab pada sistem tersebut. Hal ini berlaku secara professional dimana assessor tidak diperkenankan memasuki sistem, melakukan instalasi ataupun mendapatkan *network access* dalam sistem tersebut.



Gambar 2. Topologi Jaringan
(sumber gambar: wikipedia.org)

Dalam contoh diatas, kita bisa melihat komponen-komponen mana saja yang memiliki resiko tinggi atas kerusakan atau kehilangan data seperti Server ERP, email dan database. Bila perusahaan tersebut belum memiliki aplikasi terintegrasi (ERP) maka perlu dilakukan inventarisir terhadap aplikasi-aplikasi yang ada, misalnya menyangkut aplikasi keuangan, tenaga kerja, penjualan dan pembelian.

Dari aplikasi-aplikasi yang ada kemudian dibuat matrix yang menunjukkan bagaimana posisi aplikasi tersebut dibandingkan dengan sistem yang lain, sebagai contoh :

Tabel 1. Contoh tabel perbandingan aplikasi

No	Aplikasi	Basis data	Jenis aplikasi	Penggunaan	Tingkat resiko
1	Sistem Penjualan	SQL Server	Inhouse dev.	Client Server	Tinggi
2	Sistem Pembelian	mySQL	Outsource	Client Server	Tinggi
3	Sistem Perencanaan Pemasaran	Access	Custom	Standalone	Sedang

Selain dari komponen yang memiliki resiko tinggi atas kerusakan, assessor juga perlu mengklasifikasikan berdasarkan komponen yang merupakan titik rawan terjadinya perusakan sistem. Semisal dari firewall, sebagai gerbang awal menuju internet, ataupun dari *client* dan jaringan nirkabel.

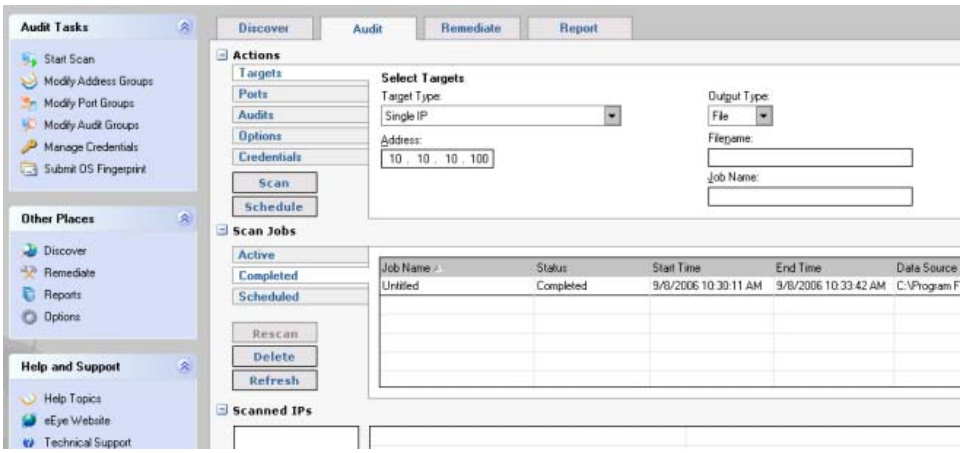
Tabel 2. Inventarisir Sistem

No	Network node	Operating System	IP Address	Fungsi	Tingkat resiko
1	Client computer site A	Windows 98	192.168.1.1-9	Dept. Keuangan	Rendah
2	Client computer site B	Windows 2000	192.168.2.1-254	Dept. Produksi	Rendah
3	Switch: Cisco Catalyst	IOS	192.168.1.10	Switch site A	Sedang
4	Firewall: Cisco PIX	PIX 5.01	202.10.31.3	Firewall Site B	Tinggi

Inventarisir sistem ini memerlukan konfirmasi dari berbagai pihak baik internal audit, *security* atau pengguna akhir itu sendiri.

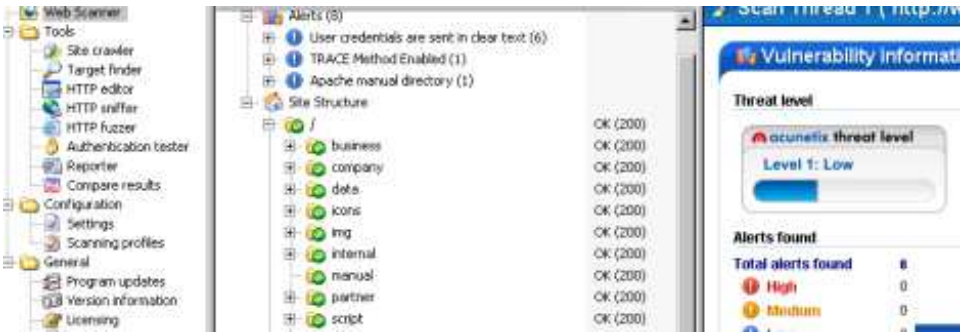
Pada sistem yang sangat kompleks maka bisa dilakukan pengambilan sampel secara acak ataupun dalam jumlah tertentu yang bisa merepresentasikan kondisi sebenarnya dilapangan.

Berikut adalah contoh tampilan dari aplikasi scanning menggunakan Retina dari eEye.



Gambar 3. Hasil scanning menggunakan Retina dari eEye

Dan berikut adalah tampilan dari Acunetix *vulnerability assessment*



Gambar 4. Tampilan Acunetix vulnerability assessment

Dari hasil scanning inilah yang kemudian dikombinasikan dengan daftar invetaris diawal sebelumnya yang assessor akan membuatnya menjadi sebuah laporan VA.

3.3 Laporan akhir

Hasil temuan dilapangan dengan alat bantu VA *scanning* tidak serta merta ditindaklanjuti oleh *client*, tentunya diperlukan evaluasi dan pemeriksaan kembali dari sisi penggunanya. Evaluasi ini perlu melihat sejauh mana kebutuhan penggunanya terhadap sistem yang dinilai rawan, adakah kontrol pengganti (*compensating control*) bila sistem tersebut mengalami gangguan.

Assesor pun harus melakukan kategorisasi terhadap hasil temuannya. Paling tidak perlu ada tiga kategori seperti resiko tinggi, sedang dan rendah yang penentuan tingkat kerawanan ini merupakan hasil diskusi antara assesor dan *client* sebelumnya. Matriks tingkat kerawanan inilah yang akan diajukan

Laporan dibuat dalam dua versi, yang pertama adalah versi lengkap yang akan diberikan pada *security officer* ataupun *system administrator* di perusahaan tersebut. Sedangkan yang kedua dalam versi yang lebih ringkas diberikan pada pimpinan di perusahaan yang berisi masukan dalam tingkat kebijaksanaan dan strategi.

Berikut adalah contoh laporan dari sisi teknikal keamanan informasi.

Tabel 3. Laporan sisi teknikal keamanan informasi

No	Kerawanan	Node	Saran	Resiko
1	Blank password	Client Site A, B	Set password	Sedang
2	FTP Service	Application Server	Matikan service yang tidak perlu	Sedang
3	Security Patch	DB Server	Patch security terbaru	Tinggi
4	Remote Execution	DB, Apps Server	Matikan service yang tidak perlu	Tinggi
5	Log reporting	Apps Server	Nyalakan fungsi log	Sedang

Sedangkan laporan untuk kebijaksanaan dan strategi dapat berupa:

1. Standar access pengguna sistem
2. Standar pemeliharaan sistem

3.4 Penyampaian laporan akhir

Tugas dari assessor yang paling akhir adalah menyampaikan hasil VA dan memberikan rekomendasi terhadap perusahaan bagaimana seharusnya pemeliharaan sistem dan kesadaran akan keamanan informasi dilakukan. Assesor haruslah orang yang memiliki kapabilitas untuk menentukan bagaimana solusi yang terbaik bagi perusahaan tersebut.

Pada contoh diatas kerawanan nomor lima, mengenai Log pada sistem terhadap aktivitas pengguna. Fitur log merupakan fitur yang sangat penting mengingat dapat digunakan sebagai bukti atau jejak (audit trail) bila terjadi pengrusakan suatu sistem. Namun pada prakteknya dilapangan lebih banyak perusahaan yang memilih untuk tidak mengaktifkan fitur ini pada berbagai sistem aplikasi.

Mengingat kondisi perusahaan yang tidak memungkinkan bila harus menambah sebuah server dan harddisk baru untuk keperluan logging misalnya, maka assessor harus mengajukan solusi lain sebagai kontrol pengganti seperti menggunakan buku log aktivitas pada sistem atau memperketat prosedur keamanan dalam sistem.

Selain log, adanya *network device* pada ruangan yang tidak terkunci misalnya, dapat digunakan kontrol pengganti dengan meletakkan piranti tersebut pada rak yang terkunci dan begitu seterusnya.

Kesimpulan

Seperti sudah dijelaskan dimuka bahwa VA adalah suatu bentuk kontrol preventif sebagaimana antivirus yang mencegah terjadi insiden terhadap sistem, maka tujuan VA sebenarnya adalah untuk meningkatkan kesadaran akan pentingnya keamanan informasi, yang seringkali menjadi prioritas kesekian dalam sebuah institusi. Dengan hasil pengukuran ini diharapkan

perusahaan dapat berbenah dan melaksanakan proses keamanan informasi dengan lebih baik.

VA sebaiknya juga dilaksanakan secara kontinu tanpa memandang kompleksitas perusahaan tersebut. Perusahaan besar tentunya akan melaksanakan VA lebih kompleks dibandingkan perusahaan menengah, namun tidak berarti perusahaan menengah memilih tidak melaksanakan VA. Sehingga resiko-resiko terhadap keamanan sistem informasi bisa dimitigasi sejak awal.

Hasil dari VA sebaiknya segera ditindaklanjuti oleh manajemen sesuai dengan tingkat urgensi dari tiap-tiap temuan. Hasil dari VA ini dapat digunakan untuk menentukan bagaimana strategi keamanan informasi kedepan.

Pada prakteknya di industri, VA biasanya dikerjakan dikerjakan oleh pihak ketiga diluar perusahaan. Hal ini didasari atas segregasi tugas, dimana pembuat sistem keamanan haruslah orang yang berbeda dengan orang yang mereviewnya. Selain alasan teknis seperti kemampuan sumberdaya dan efisiensi perusahaan. Kedepannya seiring sistem yang menjadi semakin kompleks tentunya metode VA pun akan semakin kompleks dengan peralatan yang lebih baik.

Akhirnya VA tidak lebih dari sekedar alat bantu untuk meningkatkan keamanan informasi. Metode VA secanggih apapun tidak akan berarti apa-apa bila tidak diikuti dengan kesadaran dan kesediaan dari internal perusahaan akan pentingnya keamanan informasi

Daftar Pustaka

Chirillo, J. (2003). *Hack attack testing: How to conduct your own security audit*. Wiley Publishing Inc.

Greg, M., & Kim, D. (2005). *Inside Inside Network Security Assessment: Guarding your IT Infrastructure*. Sams Publishing.

Whitaker, A., & Newman D. (2005). *Penetration Testing and Network Defense*. Cisco Press.