Webtrust Sebagai Layanan Pemberian Jaminan Keamanan Yang Layak Dari Web

Nugroho Muhtarif – NIM: 13502054

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl Ganesha 10, Bandung
E-mail: if12054@students.if.itb.ac.id

Abstrak

Webtrust adalah stempel yang diberikan kepada situs web yang secara konsisten menjalankan standard-standard yang telah dibuat oleh Canadian Institute of Chartered Accountants (CICA) dan American Institute of Chartered Public Accountants (AICPA). Saat ini webtrust telah diakui secara internasional. Webtrust pada aplikasinya diberikan oleh Certificate Authority (CA) seperti Verisign. Standar ini dapat dikelompokkan menjadi beberapa bagian, yaitu: *privacy*, *security*, *business practices/transaction integrity*, *availability*, *confidentiality or non-repudiation*.

Webtrust dikembangkan karena kekhawatiran konsumen dan dunia bisnis akan privasi dan keamanan web. Webtrust terus mengalami evolusi sehingga ditujukan agar konsumen dapat menkonfirmasi legitimasi perusahaan yang menawarkan barang dan jasa melalui web. Pada dasarnya webtrust memberikan keyakinan yang wajar bagi user web bahwa web yang sedang diakses menjaga keprivasian dan keamanan data user. Yang membedakan webtrust dengan stempel lain adalah verfikasi web yang harus independen layaknya audit. Untuk bisa mendapatkan stempel ini, situs web yang bersangkutan akan diaudit 6 bulan sekali.

Agar suatu web bisa mendapatkan stempel atau sertifikasi *Webtrust* terdapat banyak kriteria yang harus dipenuhi berkaitan dengan prinsip security, availability, processing integrity, online privacy, confidentiality . Dalam makalah ini, penulis akan memaparkan secara mendetil kriteria-kriteria tersebut beserta contoh bentuk internal controlnya tetapi hanya yang berkaitan dengan prinsip ***security, online privacy, dan confidentiality*** yang masih erat kaitannya dengan kriptografi dalam kehidupan sehari-hari. Selain itu penulis juga akan memamparkan prosedur-prosedur yang harus dijalankan CA berkaitan dengan pemberian sertifikat Webtrust jika suatu web memohon untuk mendapatkan sertifikat.

Kata kunci: *Webtrust, kriteria, internal control, security, online privacy, confidentiality*

1. Pendahuluan

1.1 Certificate Authorities

Pada kriptografi, sebuah certficate authority (CA) adalah sebuah entitas yang menerbitkan sertifikat digital untuk digunakan oleh pihak lain. CA adalah sebuah contoh dari *trusted third party*. CA adalah karakteristik dari banyak skema *public key infrastructure (PKI)*. Saat ini banyak CA komersial yang meminta bayaran untuk layanan yang diberikan. Institusi-institusi dan pemerintah dapat memiliki CA tersendiri dan juga terdapat CA yang gratis. Menurut survey Netcraft pada tahun 2005, Verisign dengan afiliasi-afiliasi yang telah diakuisisinya seperti Thawte menguasi 53% pangsa pasar CA, disusul oleh GeoTrust (25%), Comodo (12%), Go Daddy (4%) dan Entrust (2%). Saat ini GeoTrust telah diakuisisi oleh VeriSign.

Penjelasan tentang cara kerja CA sendiri telah dijelaskan pada perkuliahan kriptografi (lihat bab Public Key Infrastructure).

1.2 Webtrust

Webtrust adalah stempel yang diberikan kepada situs web yang secara konsisten menjalankan standard-standard yang telah dibuat oleh Canadian Institute of Chartered Accountants (CICA) dan American Institute of Chartered Public Accountants (AICPA). Saat ini webtrust telah diakui secara internasional, standard-standard ini dapat berlaku pada area *privacy*, *security*, *business practices/transaction integrity*, *availability*, *confidentiality or non-repudiation*.

Webtrust dikembangkan karena kekhawatiran konsumen dan dunia bisnis akan privasi dan

keamanan web. Webtrust terus mengalami evolusi sehingga ditujukan agar konsumen dapat menkonfirmasi legitimasi perusahaan yang menawarkan barang dan jasa melalui web.

Tidak seperti stempel internet lainnya yang mengklaim telah melindungi privasi dari konsumen atau perusahaan, webtrust adalah satu-satunya stempel yang diadministrasi oleh pihek ketiga. Dengan kata lain, jika anda melihat stempel webtrust pada sebuah website, pemilik web tersebut tidak mendapatkan stempel dengan hanya membayar atas keistimewaan yang dimiliki (stempel webtrust). Untuk mendapatkan stempel webtrust, sebuah web haruslah memenuhi standar-standar yang telah ditentukan oleh badan akuntansi profesional yaitu AICPA dan CICA dan situs akan diaudit atas ketaatannya terhadap standar webtrust setidaknya 6 blan sekali.

Gambar 1
(Stempel Webtrust yang dikeluarkan oleh VeriSign dan Kantor Akuntan Publik Ernst & Young)

Pemilik dari website yang telah diberikan stempel webtrust percaya bahwa keamanan dan privasi sangatlah penting bagi klien dan rekanan bisnis mereka. Oleh karena itu mereka telah memperkerjakan auditor-auditor webtrust yang telah memiliki lisensi dan dilatih secara khusus untuk mereview *online procedure* yang mereka jalankan (khususnya pada area privasi). Mereka juga mempertahankan standar-standar bisnis terbaik yang ada di dunia internet. Stempel webtrust dapat diberikan kepada sebuah situs web jika pengelola web telah secara konsisten mempertahankan standar-standar tinggi yang telah ditentukan pada area keamanan, integritas praktik bisnis/transaksi, ketersediaan informasi, *confidentiality*, dan *non-repudiation*.

Terdapat 6 stempel webtrust yaitu:

1. Privacy
   Taat kepada aturan yang ketat mengenai pengumpulan, penyimpanan dan penggunaan informasi konsumen atau klien. Keuntungan bagi pemilik stempel adalah kepercayaan atas perusahaan.
2. Security
   Mengikuti prosedur dan teknologi terkini yang layak dan aman. Keuntungannya adalah memberikan rasa aman bagi konsumen saat menjalankan transaksi baik offline maupun online.
3. Business Practices/Transaction Integrity
   Mengurangi rasa kekhawatiran akan pencurian data saat transaksi online dan memastikan bahwa transaksi telah dijalankan secara menyeluruh Keuntungannya adalah mengurangi ketakutan konsumen akan melakukan praktik online.
4. Availability
   Secara konsisten meberikan tingkan pelayanan yang telah disepakati dengan konsumen. Keuntungannya adalah memperkuat daya tarik sebagai penyedia layanan aplikasi.
5. Confidentiality
   Memperlihatkan kemampuan untuk melindungi informasi business-to-business. Keuntungannya adalah memberikan konsumen rasa percaya atas pengelolan pertukaran informasi secara online.
6. Non-Repudiation
   Memastikan identitas dan kemampuan membayar konsumen atas transaksi online yang dilakukan. Keuntungannya adalah menjaga keuntungan perusahaan.

1.3 Webtrust for Certification Auhorities

Pertumbuhan transaksi internet dan layanan web yang sangat cepat tergantung pada proses otentikasi identitas yang kuat pada situs web, pemegang domain dan server online. Pengembang browser dan aplikasi lainnya serta banyak CA yang menerbitkan sertifikat TLS/SSL (Transport Layer Security/Secure Socket Layer), semunya mendukung sertifikat-sertifikat yang terstandarisasi lebih baik untuk memberikan kepastian yang lebih kuat mengenai identitas organisasi daripada sertifikat-sertifikat yang sering dipakai saat ini (awan tahun 2006).

CA dan pengembang-pengembang browser telah bekerja sama untuk mengembangkan tuntunan yang menjadi dasar untuk membedakan sertifikat yang memiliki otentikasi yang lebih kuat dari sertifikat lain. Sertifikat-sertifikat yang diterbitkan dalam naungan pengendalian, proses, dan prosedur otentikasi yang lebih kuat disebut Extended Validation (EV certificates).

Sebuah tim kerja yang terdiri dari banyak penerbit sertifikat digital telah mengembangkan sekumpulan panduan yang diharapkan dapat menjadi persyaratan dalam menerbitkan sertifikat EV. Tim kerja ini dikenal sebagai CA Browser Forum (CAB Forum). CA dan para pengembang browser telah menyadari pentingnya sebuah pemeriksaan pengendalian, proses, dan prosedur oleh pihak ketiga yang independen. Panduan EV yang disusun oleh CAB Forum akan berisikan persyaratan spesifik mengenai CA yang ingin menerbitkan sertifikat EV untuk menjalankan webtrust untuk pemeriksaan certification authorities atau setara yang melingkupi roots hirarki dan root subordinat yang terlibat dalam proses sertifikat EV. CA akan menjalani pemeriksaan tambahan oleh auditor WebTrust untuk memberikan opini apakah persyaratan tambahan untuk penerbitan sertifikat EV telah diikuti atau tidak. Oleh karena itu dibuatlah lampiran untuk program webtrust certification authorities yang berisikan rekomendasi tentang kriteria yang akan dijadikan dasar bagi auditor webtrust dalam memberikan keyakinan yang wajar yang diminta oleh CA, browser, dan user lainnya.

2. Kriteria Webtrust

Kriteria webtrust yang dimaksud adalah benchmark yang digunakan untuk mengukur materi permasalahan yang sedang diperiksa. Kriteria yang sesuai adalah objektif, terukur, komplet, dan relevan. Hal ini merupakan pandangan Assurance Services Development Board. Prinsip-prinsip digunakan untuk menjelaskan tujuan secara menyeluruh dan opini yang dibuat oleh auditor harus merujuk pada kriteria-kriteria tersebut.

Pada prisip dan kriteria layanan webtrust, kriteria-kriteria didukung oleh serangkaian contoh pengendalian-pengendalian. Ilustrasi pengendalian ini tidak dimaksudkan untuk menjadi sebuah kondisi yang harus dipenuhi melainkan hanya disajikan sebagai contoh saja. Pengendalian-pengendalian yang dilakukan oleh pengelola web mungkin saja tidak ada dalam ilustrasi pengendalian, dan beberapa pengendalian pada ilisustrasi tidak dapat diterapkan pada semua sistem dan keadaan klien. Para praktisi (auditor) harus mengidentifikasi dan menilai pengendalian-pengendalian relevan yang dilakukan klien untuk memenuhi kriteria. Pilihan dan jumlah pengendalian akan tergantung pada gaya manajemen klien, filosofi, dan ukuran perusahaan. Untuk mendapatkan opini unqualified pada penugasan layanan webtrust, semua kriteria harus dipenuhi kecuali jika kriteria tersebut sangat tidak bisa diterapkan. Pada konteks prinsip-prinsip dan kirteria layanan webtrust, kebijakan persyaratan yang digunakan merujuk pada pernyataan tertulis yang mengkomunikasikan maksud, tujuan, persyaratan, tanggung jawab, dan standar tentang permsalahan tertentu dari pihak manajemen. Komunikasi tersebut dapat secara eksplisit dibentuk sebagai kebijakan, dan bentuk komunikasi lainnya dapat bersifat implisit. Kebijakan-kebijakan dapat berbentuk banyak hal tetapi semuanya harus tertulis.
Beberapa prinsip dan kriteria merujuk pada kekonsistenan terhadap hukum dan peraturan yang berlaku, komitmen yang telah dibuat, kesepakatan tingkat pelayanan, dan kontrak lainnya.

Pada situasi normal, prinsip dan kriteria tersebut akan terdapat pada ruang lingkup penugasan auditor untuk melakukan identifikasi terhadap semua hukum dan peraturan yang berlaku, komitmen yang telah dibuat, kesepakatan tingkat pelayanan, dan kontrak lainnya yang relevan. Lagipula penugasan layanan webtrust tidak mengharuskan auditor untuk memberikan keyakinan akan ketaatan klien terhadap hukum dan peraturan yang berlaku, komitmen yang telah dibuat, kesepakatan tingkat pelayanan, dan kontrak lainnya, tetapi praktisi harus memberikan keyakinan tentang efektivitas pengendalian-pengendalian klien melalui pemantauan ketaatan terhadap hukum dan peraturan yang berlaku, komitmen yang telah dibuat, kesepakatan tingkat pelayanan, dan kontrak lainnya.

Prinsip-prinsip dan kriteria webtrust dapat dikelompokkan ke dalam 4 wilayah, yaitu:

1. Kebijakan
   Entitas klien telah mendefinisikan dan mendokumentasikan kebijakan-kebijakannya yang relevan terhadap prinsip tertentu.
2. Komunikasi
   Entitas klien telah mengkomunikasikan kebijakan-kebijakannya kepada pihak yang berwenang.
3. Prosedur
   Entitas klien menggunakan prosedur-prosedur untuk mencapai tujuannya yang berkaitan dengan kebijakan yang telah didefinisikan.
4. Pemantauan
   Entitas klien memantau sistem web dan melakukan sesuatu untuk mempertahankan

ketaatan terhadap kebijakan yang telah didefinisikan.

AICPA dan CICA sendiri telah membuat prinsip-prinsip dan kriteria dalam penugasan layanan webtrust, yaitu:

1. Keamanan
   Sistem web dilindungi dari akses yang tidak terotorisasi baik fisik maupun logika
2. Ketersediaan Informasi
   Sistem tersedia untuk operasi dan digunakan sebagaimana telah disepakati.
3. Integritas Pemrosesan
   Pemrosesan sistem lengkap, akurat, tepat waktu, dan terotorisasi.
4. Pivasi Online
   Informasi pribadi yang didapatkan dari hasil e-commerce dikumpulkan, digunakan, diungkapkan, dan dijaga sebagaimana telah disepakati.
5. Kerahasiaan
   Informasi didesain serahasia mungkin dan dilindungi sebagaimana telah disepakati.

Pada lingkungan e-commerce tertentu, persyaratan, kondisi, termasuk hak dan kewajiban, dan komitmen kedua belak pihak (pengelola situs dan konsumen) ditunjukkan secara implisit pada penyelesaian transaksi user pada situs web. Untuk memenuhi maksud kategori komunikasi kriteria pada situasi tersebut, kebijakan-kebijakan dan prosedur-prosedur yang diperlukan masing-masing oleh kriteria komunikasi harus diungkapkan pada situs web.

2.1 Kriteria dan Contoh Control untuk Prinsip Security

Prinsip keamanan merujuk pada perlindungan dari komponen sistem dari akses yang terotorisasi baik lgika maupun fisik. Pada e-commerce dan sistem lain, pihak yang berkepentingan ingin meyakinkan bahwa informasi yang diberikan hanya tersedia bagi individu-individu yang memerlukan aksen untuk menyelesaikan layanan atau transaksi tertentu, atau menindaklanjuti pertanyaan-pertanyaan yang mungkin muncul. Informasi yang diberikan melalui sistem rentan terhadap akses ilegal selama transmisi dan selama informasi tersebut disimpan pada sistem pihak lain. Membatasi akses akan membantu mencegah penyelewengan yang mungkin terjadi, pencurian sumberdaya atau informasi, penyalahgunaan perangkat lunak, dan akses ilegal untuk menggunakan, mengubah, merusak, atau membocorkan informasi. Elemen kunci dari perlindungan komponen sistem adalah mengizinkan akses yang telah diotorisasi dan mencegah akses ilegal terhadap kompenen sistem tersebut.

Berikut ini adala kriteria dan contoh kontrol untuk prinsip keamanan:

1 Wilayah Kebijakan: Entitas mendefinisikan dan mendokumentasikan kebijakan-kebijakan untuk keamananan sistemnya.

1.1 Kebijakan keamanan entitas dibuat dan secara berkala direview dan disetujui oleh individu atau grup yang ditunjuk. Contoh pengendalian: Petugas keamanan mengkaji kebijakan setahun sekali dan meyerahkan rekomendasi perubahan untuk disetujui oleh komite standar teknologi informasi.
1.2 Kebijakan keamanan entitas mencakupi (tetapi tidak membatasi) beberapa permasalahan yaitu:

a. Identifikasi dan dokumentasi persyaratan keamananan dari user yang sah
b. Mengizinkan akses, mendefinisikan sifat akses, dan siapa yang mengotorisasi akses tersebut.
c. Mencegah akses yang tidak diotorisasi
d. Prosedur untuk menambah user baru, memodifikasi tingkat akses dari user yang ada, dan menghapus user yang tidak lagi memerlukan akses.
e. Penugasan pertanggungjawaban dan akuntabilitas untuk keamanan sistem
f. Penugasan pertanggungjawaban dan akuntabilitas untuk perubahan dan pemeliharaan sistem.
g. Melakukan tes, evaluasi, dan mengotorisasi komponen sistem sebelum implementasi.
h. Menyediakan fasilitas untuk menangani komplain dan permintaan atas permasalahan yang berkaitan dengan kemananan.
i. Prosedur untuk menangani pembobolan keamanan dan kecelakaan lainnya
j. Menyediakan alokasi untuk pelatihan dan sumber daya lain untuk mendukung kebijakan keamanan.
k. Penanganan eksepsi dan situasi yang tidak secara spesifik diatur yang berhubungan dengan kebijakan keamanan.
l. Identifikasi dari kekonsistenan terhadap hukum dan peraturan yang berlaku, komitemn yang telah didefinisikan, kesepakatan layanan, dan kontrak lainnya.
m. Pemulihan dan kontinuitas layanan yang sesuai dengan kesepakatan dengan konsumen yang telah didokumentasikan atau kesepakatan lainnya.
n. Kapasitas pemantauan sistem untuk mencapai komitmen kepada pelanggan atau

kesepaktan lain yang berhubungan dengan keamanan.

1.3 Pertanggungjawaban dan akuntabilitas untuk kebijakan kemananan sistem entitas, serta perubahan dan update terhadap kebijakan yang ditetapkan. Contoh pengendaliannya adalah manajemen telah memberikan tanggung jawab untuk pemeliharaan dan pelaksanaan kebijakan kemananan kepada kepal bagian informasi (CIO). Pihak selain CIO dalam dewan eksekutif bertugas membantu review, update, dan persetujuan kebijakan sebagaimana tertulis pada buku panduan dewan eksekutif.

2. Wilayah Komunikasi: Entitas mengkomunikasikan kebijakan kemanan sistemnya yang telah didefinisikan kepada pihak yang berwenang.

2.1 Entitas telah mempersiapkan deskripsi tujuan dari sistem dan batasannya dan mengkomunikasikan deskripsi tersebut pada pihak yang berwenang. Contoh pengendaliannya adalah entitas menempatkan deskripsi sistem pada situs web.

2.2 Kewajiban dan komitmen terhadap konsumen dari entitas yang berhubungan dengan keamanan dikomunikasikan kepada pihak yang berwenang. Contoh pengendaliannya adalah Kewajiban dan komitmen terhadap konsumen dari entitas yang berhubungan dengan keamanan ditempatkan pada situs web atau merupakan bagian dari kesepakatan layanan.

2.3 Tanggung jawab dan akuntabilitas untuk kebijakan keamanan situs web beserta perubahan dan updatenya dikomunikasikan kepada pegawai pengelola situs web yang yang bertanggung jawab mengimplementasikannya. Conrohnya adalah petugas administrasi keamanan bertanggung jawab akan pemeliharan setiap hari dan memeberikan rekomendasi perbaikan kepada CIO dan komite IT.

2.4 Proses pemberitahuan pembobolan keamanan sistem situs web dan pelaporan komplain dikomunikasikan kepada user yang sah. Proses bagi konsumen atau pihak eksternal untuk memberitahu entitas akan kemungkinan pembobolan keamanan sistem dan kecelakaan lainnya ditempatkan pada situs web atau dijadikan sebagai bagian dari fitur penerimaan user baru.

2.5 Perubahan yang dapat mempengaruhi keamanan sistem dikomunikasikan kepada manajemen dan konsumen yang dipengaruhi. Contoh pengendaliannya adalah perubahan yang dapat mempengaruhi keamanan sistem dikaji dan disetujui oleh konsumen yang dipengaruhi dan sesuai kesepakatan pelayanan yang telah ditetapkan sebelum meengimplementasikan perubahan yang direncanakan.

3.0 Wilayah prosedur: entitas menggunakan prosedur-prosedur untuk mencapai tujuan keamanan sistem yang telah didokumentasikan sesuai dengan definisi kebijakannya.

3.1 Terdapat prosedur-prosedur untuk membatasi akses logik ke sistem meliputi hal (tidak bersifat membatasi):
a. Regsitrasi dan o0risasi user baru, contoh pengendalian: Kemampuan untuk membuat atau mengubah user dan kewenangan user hanya terbatas dimiliki oleh tim administrasi kemananan

b. Identifikasi dan otentikasi user. Contoh pengendalian: user harus log on ke jaringan sistem dengan user id dan password sebelum diberikan akses. User id unik, password minimal terdiri dari 6 karakater dan salah satunya adalah non alfanumerik. Password case sensitif dan harus diubah setiap 90 hari.

c. Proses pengubahan profil user, contoh pengendalian: pengubahan profil user oleh pihak entitas hanya terbatas oleh tim administrasi keamanan dan memerlukan persetujuan dari kepala dari bagian yang terkait misalkan manajer akun konsumen.

d. Proses pemberian izin dan kewenangan akses ke sistem. Contoh pengendalian: Sesi login akan dimatikan setelah tiga kali percobaan login. Sesi yang dimatikan ini akan dicatat untuk tindakan lebih lanjut.

e. Distribusi output, contoh pengendalian: akses terhadap output pemrosesan sistem hanya diberikan kepada individu-indvidu yang berhak sesuai tingkatan informasinya.

f. Pembatasan akses logik ke penyimpanan offline, backup data, contoh pengendalian: Akses ke penyimpanan offline, backup data hanya diberikan kepada staf operasi komputer.

g. Pembatasan akses terhadap konfigurasi sistem, master password, dan alat keamanan. Contoh pengendalian: tim keamanan informasi di bawah pengawasan CIO memelihara akses

ke firewall dan log seperti kepada media penyimpanan. Setiap akses dicatat dan dikaji minimal 4 kali dalam setahun.

3.2 Terdapat prosedur-prosedur untuk membatasi akses fisik ke fasilitas, media backup, dan komponen sistem lainnya seperti firewall, router, dan server (tetapi tidak terbatas hal tersebut). Contoh pengendaliannya adalah akses fisik kepada fasilitas dan sumber daya sistem seperi firewall, router, media penyimpanan dibatasi hanya kepada pihak yang berwenang dengan menggunakan sistem kunci kartu dan dimonitor oleh pemantauan video.

3.3. Terdapat prosedur untuk membatasi akses logik ilegal ke sistem. Contoh pengendalian: perangkat lunak virtual private networking (VPN) diguanakan untuk mengizinkan akses jarak jauh oleh user yang sah. User diotentikasi oleh server VPN melalui perangkat lunak user tertentu dan dengan user id dan password.

3.4 Terdapat prosedur-prosedur untuk melindungi sistem dari infeksi virus, kode-kode merusak, dan perangkat lunak yang tidak terotorisasi. Contoh pengendaliannya adalah adanya perangkat lunak anti virus termasuk pemeriksaan virus terhadap e-mail yang masuk. Tanda tangan virus diupdate minimal seminggu sekali.

3.5 Enkripsi atau teknik lain yang setara digunakan untuk melindungi informasi otentikasi user dan sesi terkait yang ditransmisikan melalui internet atau jaringan publik lainnya. Contoh pengendaliannya adalah penggunaan secure socket layer (SSL) 128 bit untuk transmisi informasi pribadi atau rahasia yang melalui jaringan publik, termasuk user id dan password. User diharuskan untuk mengupgrade browser ke versi terkini yang telah dites dan disetujui oleh tim administrasi keamananan untuk menghindari permasalahan keamanan yang mungkin muncul.

3.6 Terdapat prosedur untuk mengidentifikasi pembobolan keamanan beserta tindakan dan pelaporannya. Contoh pengendalian: log kecelakaan dimonitor dan dikaji oleh tim keamanan informasi setiah hari.

3.7 Terdapat prosedur untuk melaporkan ketidaktaatan terhadap kebijakan keamanan sistem dan terdapat perbaikan secara rutin. Contoh pengendaliannya adalah secara rutin kebijakan kemananm pengendalian, dan prosedur-prosedur diaudit oleh departemen internal audit atau komite audit. Hasil dari pemeriksaan tersebut dikaji oleh pihak manajemen, respon dipersiapkan, dan rencana perbaikan akan dilakukan.

3.8 Perencanaan, desain, implementasi, konfigurasi, modifikasi, pengaturan, sistem dan perangkat lunak yang berhubungan dengan keamanan harus konsisten dengan kebijakan keamanan untuk mengizinkan akses yang sah dan mencegah akses ilegal. Contoh pengendaliannya adalah: Tim administrasi keamanan mengkaji dan menyetujui arsitektur dan spesifikasi rancangan pengembanagan sistem baru untuk meyakinkan kekonsistenan terhadap kebijakan, tujuan, dan standar kemananan.

3.9 Terdapat prosedur untuk memastikan pribadi yang bertanggung jawab untuk desain, pengembangan, dan implementasi, dan operasi sistem yang mempengaruhi kemananan cukup memadai untuk memenuhi tanggung jawabnya. Contoh pengendaliannya adalah pelatihan dan pengembanagan dalam permasalahan dan konsep keamanan.

3.10 Terdapat prosedur untuk menjaga komponen sistem beserta konfigurasinya agar tetap konsisten dengan kebijakan keamanan sistem yang telah ditentukan. Contoh pengendaliannya adalah manajemen diberi opini oleh pihak ketiga mengenai kelayakan pengendalian keamananan dan secara rutin mengevaluasi tingkat kinerja yang diberikan sesuai dengan kesepakatan pelayanan.

3.11 Terdapat prosedur untuk memastikan bahwa hanya perubahan yang telah diotorisasi, diuji, dan didokumentasikan yang akan diimplementasikan. Contoh pengendaliannya adalah perubahan pada infrastruktur sistem dan perangkat lunak dilakukan dan diuji pada proses dan lingkungan yang berbeda sebelum implementasi perubahan.

3.12 Terdapat prosedur untuk memastikan bahwa perubahan darurat telah diotorisasi dan didokumentasikan. Contoh pengendaliannya adalah perubahan darurat yang menyimpang dari prosedur standar dicatat dan dikaji oelh manajemen setiap hari dan dilaporkan kepala bagian yang terkait. Perbaikan permanen dilakukan dengan persetujuan manajemen.

4.0 Wilayah pemantauan: Entitas memonitor sistem dan mengambil tindakan untuk menjaga ketaatan terhadap kebijakan keamananan sistem yang telah ditetapkan.

4.1 Keamanan sistem entitas secara rutin dikaji dan dibandingkan dengan kebijakan keamanan yang telah ditentukan. Contoh pengendaliannya adalah tim keamanan informasi memonitor sistem dan menilai kelemahan sistem menggunakan kakas yang layak. Risiko potensial dikaji dan dibandingkan dengan kesepakatan pelayananan dan kewajiban entitas lainnya. Rencana perbaikan disulkan dan implementasinya akan dimonitor.

4.2 Terdapat proses untuk mengidentifikasi melemahnya kemampuan entitas dalam mencapai tujuan yang berhubungan dengan kebijakan kemananan sistem yang telah ditentukan. Contoh pengendaliannya adalah log dianalisis untuk mengidentifikasi tren yang mungkin memliki dampak yang potensial terhadap melemahnya kemampuan manajemen dalam mencapai tujuan keamanan sistemnya.

4.3 Perubahan teknologi dan lingkungan dipantau dan dampaknya terhadap keamanan sistem dinilai secara periodik. Contoh pengendaliannya adalah kelompok keamanan IT nemantau dampak teknologi terbaru pada keamanan sistem.

2.2 Kriteria dan Contoh Control untuk Prinsip Online Privacy

Prinsip privasi online berfokus pada perlindungan informasi pribadi yang situs dapat kumpulkan dari konsumennya melalui sistem e-commerce. Walaupun pengendalian-pengendalian oleh pengelola situs sudah ada untuk melindungi informasi yang berada pada sistem situs web maupun penyedia layanan yang situs gunakan, bukanlah maksud dari prinsip ini mengalamatkan perlindungan kepada semua informasi pribadi yang sistem mungkin dapatkan dari semua sumber. AICPA dan CICA telah membuat tim kerja yang terpisah untuk mempertimbangkan prinsip-prinsip dan kriteria yang relevan untuk privasi perusahaan.

E-commerce memfasilitasi pengumpulan informasi dari dan tentang individu-individu. Beberapa konsumen menyukai hal ini karena memungkinkan mereka untuk menerima materi pemasaran dari e-commerce yang sesuai dengan pilihan dan kebutuhan mereka. Pada sisi lain banyak konsumen yang menilai bahwa penggunaan informasi tersebut merupakan invasi terhadap privasi mereka. Untuk itu sangatlah penting bagi situs untuk menjelaskan konsumen-konsumen mereka tentang informasi apa saja yang dikumpulkan tentang konsumen, penggunaan informasi tersebut, opsi konsumen, dan hal lain yang berkaitan. Sebagai tambahan, banyak negara yang telah mengimplementasikan hukum dan peraturan mengenai keprivasian informasi yang diperoleh melalui e-commerce.

Privasi bisa memiliki banyak aspek dan kriteria yang berhubungan. Privasi didefinisikan sebagai perlindungan terhadap pengumpulan, penyimpanan, penghapusan dan pengumuman informasi pribadi. Informasi pribadi didefinisikan sebagai semua informasi yang berhubungan individu yang diidentifikasi atau teridentifikasi. Informasi tersebut termasuk nama, alamat, no kependudukan, no telepon, catatan pembelian barang, catatan kredit dan informasi lainnya. Sedangkan informasi yang bersifat sensitif dapat berupa informasi medis, agama, opini politik, kepercayaan filosofis, orientasi seksual, etnik, catatan kriminal, dan informasi lainnya yang sejenis.

Sangatlah penting bagi konsumen-konsumen untuk memiliki kerpercayaan terhadap pihak yang mengambil langkah yang sesuai untuk melindungi informasi pribadi. Walaupun secara relatif mudah untuk membangun sebuah sistem e-commerce, teknologi yang mendasari bisa jadi sangat rumit dan dapat memerlukan banyak perlindumgan informasi dan permasalahan keamanan lainnya. Keprivasian informasi yang ditransmisikan pada internet atau jaringan publik lainnya secara relatif dapat dengan mudah diatasi. Tanpa menggunakan teknik dasar enkripsi, sebagai contoh nomer kartu kredit konsumen dapat dilacak dan dicuri saat transmisi. Tanpa firewall yang layak dan praktik keamanan lainnya, informasi pribadi yang berada pada sistem komputer e-commerce dapat secara sengaja dan tidak sengaja diberikan kepada pihak ketiga yang tidak berkaitan.

Kerangka kerja privasi AICPA dan CICA terdiri dari 9 praktik privasi yang merupakan kunci dari manajemen informasi pribadi yang layak dan didasarkan praktik-praktik yang secara internasioanal telah dikenal baik. Hukum dan peraturan privasi dari berbagai wilayah yuridiksi di seluruh dunia memerlukan banyak praktik-praktik privasi tersebut. Walapun praktik-praktik tersebut tidak dikenal luas, kesembilan prakti privasi ini hampir muncul di seluruh humum privasi di seluruh dunia. Praktik-praktik tersebut adalah:

1. Notice
   Pengelola situs web memberikan penjelasan tentang kebijakan-kebijakan

privasinya dan praktik-praktik terhadap invidu-individu baiik sebelum informasi dikumpulkan atau sesaat setelah praktik dijalankan. Penjelasan ini bersikan tujuan pengumpulan informasi pribadi dan bagaiamana informasi tersebut akan digunakan.

2. Choice and Concent
   Entitas pengelola situs web menjelaskan pilihan yang ada kepada individu dan memperoleh izin atau persetujuan dari individu terkait permasalahan pengumpulan, penggunaan, pengungkapan, dan menyimpan informasi pribadi.
3. Collection
   Entitas pengelola situs web membatasi pengumpulan informasi pribadi yang diperlukan untuk tujuan yang telah dijelaskan pada poin notice.
4. Use and Retention
   Entitas pengelola situs web membatasi pengumpulan informasi pribadi yang diperlukan untuk tujuan yang telah dijelaskan pada poin notice dan membatasi informasi pribadi kepada hanya yang telah diberikan izin oleh konsumen baik secara eksplisit maupun implisit. Entitas pengelola situs web menyimpan informasi pribadi selama hanya diperlukan untuk pemenuhan tujuan yang telah dijelaskan atau yang disyaratkan oleh hukum dan peraturan yang berlaku
5. Access
   Entitas pengelola situs web memberikan akses kepada individu untuk melakukan review, update, menggunakan, atau menghapus informasi pribadinya
6. Onward Transfer and Disclosure
   Entitas pengelola situs web mengungkapkan informasi pribadi pada pihak ketiga hanya dengan tujuan yang dijelaskan pada notice dan jika individual telah memberikan izin secara eksplisti atau implisit atau karena hukum dan peraturan yang berlaku. Entitas pengelola situs web hanya mengungkapkan informasi pribadi pada pihak ketiga yang memberikan perlindungan terhadap informasi pribadi yang setara dengan yang entitas pengelola situs web lakukan.
7. Security
   Entitas pengelola situs web mengambil tindakan pencegahan untuk melindungi informasi pribadi dari kehilangan, penyalahgunaan, akses ilegal, pembocoran, perubahan, dan penghapusan berdasarkan nilai dan sensitivitas informasi.
8. Integrity
   Entitas pengelola situs web mempertahankan informasi pribadi secara akurat, lengkap, relevan, dan handal agar informasi tersebut dapat digunakan.
9. Management and Enforcement
   Entitas pengelola situs web menandai satu atau lebih individu yang akuntabel untuk ketaatan perusahaan terhadap kebijakan-kebijakan privasi yang dibuatnya. Entitas pengelola situs web memiliki proses periodik untuk menilai dan memverifikasi ketaatan terhadap kebijakan-kebijakan privasinya. Entitas pengelola situs web juga memiliki prosedur-prosedur untuk menangani pertanyaan-pertanyaan dan perselisihan mengenai privasi.

Kriteria privasi yang ditentukan telah memberikan dampak di dunia ini. E-commerce yang bersifat global. Saat perusahaan-perusahaan melewati batas internasional, maka perusahaan akan menghadapi tantangan untuk memenuhi standar-standar dan menaati aturan yang berkaitan dengan privasi. Organisasi yang ingin melangkap ke pasar global tanpa standar privasi dan pengungkapan yang memadai maka bisnis organisasi tersebut terancam dibatasi atau bahkan dilarang.

Di era global ini, para konsumen di selurh dunia khawatir akan penggunaan informasi pribadi mereka, perlindungan terhadap informasi, proses-proses apa saja yang dapat dilakukan untuk mengkoreksi kesalahan informasi, dan siapa yang dapat mengakses informasi tersebut. Tanpa pengendalian yang memadai dan tanpa pengungkapan hal terkait yang memadai, para konsumen akan memilih situs web lain yang memiliki pengendalian yang cukup untuk berbisnis.

Karena karakteristik e-commerce yang unik, para konsumen khawatir dengan bagaiaman mereka akan mengalamatkan komplain. Jika sebuah situs web enggan atau tidak bisa menanggapi kekhawatiran para konsumen, apakah ada jalan lain yang dapat ditempuh oleh konsumen? Jika seorang konsumen di suatu negara dan perusahaan berada pada negara lain, bagaiamana hak konsumen akan dilindungi? Beberapa negara telah mensyaratkan prosedur alternatif untuk memastikan perlindungan konsumen. Penyelesaian perselisihan tradisional melalui sistem persidangan dapat memakan waktu dan biaya yang tinggi. Mekanisme penyelesaian perselishan pihak ketiga (seperti yang ditawarkan oleh National Arbitration Forum) dapat memberikan cara yang efektif sebagai jalur alternatif bagi konsumen.

Kriteria privasi onlne mengharuskan entitas pengelola situs web untuk:

- Komitmen terhadap penggunaan mekanisme penyelesaian pihak ketiga yang sesuai dengan prinsip arbitrasi. Penyelesaian perseilishan tersebut dapat diberikan oleh organisasi apapun atau institusi pemerintahan.
- Mengungkapkan prosedur-prosedur yang dijalankan untuk jalur alternatif bagi kunsumen untuk permasalahan yang tidak ditetapkan oleh entitas pengelola situs web.

Berikut ini adala kriteria dan contoh control untuk prinsip privasi online:

1.1 Wilayah kebijakan: entitas mendefinisikan dan mendokumentasikan kebijakannya yang berhubungan dengan perlindungan informasi pribadi sebagai hasil e-commerce. Contoh pengendaliannya adalah persyaratan user didokumentasikan pada kesepakatan pelayanan atau dokumen lain.

1.2 Kebijakan keamanan entitas mencakupi (tetapi tidak membatasi) beberapa permasalahan yaitu:

a. Identifikasi dan dokumentasi persyaratan prvasi online dari user yang sah

b. Mengizinkan akses, mendefinisikan sifat akses, dan siapa yang mengotorisasi akses tersebut.

c. Mencegah akses yang tidak diotorisasi

d. Prosedur untuk menambah user baru, memodifikasi tingkat akses dari user yang ada, dan menghapus user yang tidak lagi memerlukan akses.

e. Penugasan pertanggungjawaban dan akuntabilitas untuk privasi online sistem

f. Penugasan pertanggungjawaban dan akuntabilitas untuk perubahan dan pemeliharaan sistem.

g. Melakukan tes, evaluasi, dan mengotorisasi komponen sistem sebelum implementasi.

h. Menyediakan fasilitas untuk menangani komplain dan permintaan atas permasalahan yang berkaitan dengan privasi online.

i. Prosedur untuk menangani pembobolan keamanan dan kecelakaan lainnya

j. Menyediakan alokasi untuk pelatihan dan sumber daya lain untuk mendukung kebijakan privasi online.

k. Penanganan eksepsi dan situasi yang tidak secara spesifik diatur yang berhubungan dengan kebijakan keamanan.

l. Identifikasi dari kekonsistenan terhadap hukum dan peraturan yang berlaku, komitemn yang telah didefinisikan, kesepakatan layanan, dan kontrak lainnya.

m. Memberikan pemberitahuan tentang informasi pribadi yang dikumpulkan.

n. Memberikan pilihan pada konsumen berkaitan dengan tipe dan opsi yang berhubungan dengan informasi yang dikumpulkan.

o. Memberikan akses kepada konsumen untuk mengubah atau atau memperbaiki informasi pribadinya.

p. Mencatat penyimpanan dan penghapusan informasi pribadi.

1.3 Pertanggungjawaban dan akuntabilitas untuk kebijakan privasi online sistem entitas, serta perubahan dan update terhadap kebijakan yang ditetapkan. Contoh pengendalianya adalah penyimpanan dan perlindungan terhadap informasi pribadi dan tanggung jawab untuk menjaga keamanan informasi tersebut telah ditetapkan.

2.0 Wilayah komunikasi: Entitas mengkomunikasikan kebijakan mengenai perlindungan terhadap informasi pribadi kepada pihak internar dan eksternal.

2.1 Entitas telah mempersiapkan deskripsi tujuan dari sistem dan batasannya dan mengkomunikasikan deskripsi tersebut pada pihak yang berwenang. Contoh pengendaliannya adalah entitas menempatkan deskripsi sistem pada situs web.

2.2 Kewajiban dan komitmen terhadap konsumen dari entitas yang berhubungan dengan privasi online dikomunikasikan kepada pihak yang berwenang dan diungkapkan pada situs web. Hal-hal yang diungkapkan adalah (tetapi tidak bersifat memabatasi):

a. Jenis informasi tertentu yang dikumpulan dan disimpan, penggunaan informasi tersebut dan kemungkinan distribusi informasi tersebut ke pihak ketiga. Contoh pengendaliannya adalah entitas mempublikasikan kebijakan privasi onlinenya pada intranet perusahaan.

b. Pilihan yang berkaitan dengan cara pengumpulan informasi yang dapat digunakan dari individu yang sedang online. Individu-individu diberi kesempatan untuk memilih opsi yang diberikan, baik dengan tidak memberikan informasi tersebut dan atau menolak distribusi informasi yang tidak terlibat dalam transaksi.

c. Informasi sensitif yang diperlukan dalam transaksi e-commerce. Konsumen harus memilih terlebih dahulu sebelum informasi tersebut dikumpulkan dan distransmisikan.

d. Konsekuensi yang mungkin terjadi jika konsumen menolak memberikan informasi atau menolak penggunaan informasi tersebut.
e. Cara informasi pribadi dikumpulkan dapat dikaji dan jika perlu diperbaiki atau ditiadakan.

2.3 Jika situs web entitas menggunakan cookies atau metode tracking lainnya (seperti webbugs atau middleware), entitas harus mengungkapkan bagaimana metode tersebut digunakan. Jika konsumen menolak penggunaan cookies, konsekuensi yang mungkin terjadi karena penolakan tersebut harus diungkapkan. Contoh penggunaannya adalah entitas mengungkapkan penggunaan cookies pada situs web dan bagaimana cara kerjanya.

2.4 Proses untuk mendapatkan bantuan dan memberitahu entitas tentang pembobolan atau pelanggaran privasi online dikomunikasikan kepada user yang sah. Contoh pengendaliannya adalah terdapat prosedur untuk identifiikasi dan eskalasi pembobolan kemanan dan pelanggaran privasi online dan kecelakaan lainnya.

2.5 Entitas mengungkapkan prosedur untuk jalur alternatif konsumen untuk hal yang berhubungan dengan privasi online yang tidak ditetapkan oleh entitas. Komplain dapat berhubungan dengan pengumpulan, penggunaan, dan distribusi informasi pribadi, dan konsekuensi kegagalan menyelesaikan komplain tersebut. Proses penyelesaian harus memiliki atribut:

a. Komitemen manajemen untuk menggunakan layanan penyelesaian perselisihan pihak ketiga atau proses lainnya yang diamanatkan oleh badan yang mengatur pada kasus konsumen tidak puas dengan penyelesaian yang ditawarkan oleh entitas, tentunya disertai dengan komitmen pihak ketiga untuk untuk menyesaikan permasalahan tersebut. Penyelesaian oleh pihak ketiga baru dilakukan setelah penyelesaian yang diwarkan entitas ditolak.

b. Penggunaan dan tindakan apa saja yang dikenakan pada informasi pribadi yang menjadi subjek komplain sampai penyelesaian yang memuaskan tercapai.

2.6 Entitas mengungkapakan prakti privasi tambahan yang diperlukan untuk mentaati hukum dan peraturan yang berlaku. Cara pengendaliannya misalkan dengan memberitahukan praktik-praktik tersebut pada situs web.

2.7 Pada kejadian kebijakan privasi online tidak lagi dijalankan atau diperlonggar, entitas harus memberikan pemberitahuan yang jelas kepada konsumen tentang kebijakan tersebut. Contoh pengendaliannya adalah pengiriman e-mail kepada pelanggan perihal kebijakan tersebut.

2.8 Entitas memberitahu user jika user tersebut telah keluar dari situs yang dilingkupi oleh kebijakan privasi online entitas. Entitas menggunakan pop-up window untuk memberitahukan user bahwa mereka telah meninggalkan situs yang dilingkupi oleh kebijakan privasi online entitas.

2.9 Tanggung jawab dan akuntabilitas untuk kebijakan privasi online sistem entitas beserta perubahan dan updatenya dikomunikasikan kepada pegawai yang bertanggung jawab mengimplementasikan kebijakan tersebut. Contoh pengendaliannya adalah manajemen telah memberikan tanggung jawab dan akuntabilitas mengenai kebijakan privasi online kepada CPO. Sedangkan untuk kebiijakan keamanan diberikan pada CIO. CPO bertanggungjawab akan pemeliharaan kebijakan privasi online setiap hari dan merekomendasikan perbaikan pada komite.

2.10 Perubahan yang dapat mempengaruhi privasi online dikomunikasikan kepada pihak manajemen dan user yang terpengaruhi oleh perubahan tersebut. Contoh pengendaliannya adalah perubahan yang dapat mempengaruhi user dan privasi onlinenya atau kewajiban yang terkait dihighlight pada situs web entitas.

3.0 Wilayah prosedur: Entitas menggunakan prosedur-prosedur untuk mencapai tujuan privasi yang telah didokumentasikan yang berhubungan dengan kebijakan privasi yang telah ditetapkan.

3.1 Prosedur entitas yang memerlukan pengungkapan informasi pribadi hanya dilakukan kepada pihak yang penting dalam transaksi, kecuali jika pelanggan secara jelas mengizinkan sebelum informasi tersebut diungkapkan. Jika pelanggan tidak mengizinkan secara jelas, maka entitas harus mendapatkan izin terlebih dahulu dari pelanggan sebelum informasi tersebut diberikan pada pihak ketiga. Contoh pengendaliannya adalah prosedur entitas mensyaratkan pelanggan diberikan opsi yang jelas tentang distribusi informasi pribadi tersebut dengan pihak lain yang tidak berhubungan dengan transaksi dan terdapat

pengendalian entitas untuk menelusuri opsi tersebut pada database.

3.2 Prosedur yang memberikan informasi pribadi sebagai hasil e-commerce hanya dijalankan oleh pegawai hanya untuk hal-hal yang berhubungan dengan bisnis entitas. Contoh pengendaliannya adalah pegendalian yang memadai untuk membatasi akses ke informasi pribadi berdasarkan keperluan dan fungsi pekerjaan pegawai.

3.3 Entitas memiliki prosedur untuk untuk mengedit dan menvalidasi informasi pribadi yang dikumpulkan, dibuat, atau disimpan. Contoh pengendaliannya adalah sebelum menyelesaikan transaksi, pelanggan disarankan oleh sistem untuk memeriksa data pribadi yang mereka telah masukkan.

3.4 Entitas memiliki prosedur untuk mendapatkan keyakinan tentang perlindungan informasi dan kebijakan privasi pihak ketiga berhubungan dengan kemana saja informasi tersebut didistribusikan dan kepada siapa (pihak ketiga) entitas mempercayakan sesuai dengan kebijakan privasi yang telah diungkapkan. Contoh pengendaliannya adalah jika entitas mendapatkan dukungan atau layanan teknologi pihak luar dan melakukan transfer data ke pihak ketiga. Entitas harus mengetahui dan mengkaji pengendalian yang dilakukan oleh pihak luar dan laporan mengenai efektivitas pengendalian dari auditor independen.

3.5 Izin pelanggan harus didaptkan sebelum mendownload file dan informasi untuk disimpan, diubah dan, digandakan pada komputer pelanggan. Jika pelanggan telah mengindikasikan kepada entitas bahwa ia tidak mau menggunakan cookies, maka entitas harus memiliki pengendalian untuk meyakinkan bahwa cookies tidak tersimpan pada komputer pelanggan. Entitas harus meminta izin pelanggan untuk menyimpan, mengubah, atau menggandakan informasi selain cookies pada komputer pelanggan. Contoh pengendaliannya adalah halaman registrasi pelanggan memberitahu dan meminta izin kepada konsumen untuk menggunakan cookies dengan tujuan mempercepat proses rgeistrasi dan login. Pelanggan akan diberitahu saat file akan didownload ke komputer mereka sebagai bagian dari layanan.

3.6 Pada kejadian praktik kebijakan privasi tidak lagi dijalankan atau diperlonggar, entitas memiliki prosedur untuk melindungi informasi pribadi saat informasi tersebut dikumpulkan atau mendapatkan izin pelanggan untuk menggunakan praktik privasi baru berkaitan dengan informasi pribadi pelanggan. Contoh pengendaliannya adalah penulusuran data yang dikumpulkan sebelum dan sesudah pemberlakuan praktik privasi yang baru.

3.7 Kriteria prinsip privasi online yang berkaitan dengan keamanan sejenis dengan kriteria untuk prinsip keamanan dari poin 3.1 sampai dengan 3.12.

4.0 Wilayah pemantauan: Entitas melakukan pemantauan terhadap sistem dan mengambil tindakan untuk mentaati kebijakan-kebijakan yang telah ditetapkan yang berhubungan dengan perlindungan informasi pribadi.

4.1 Kinerja privasi entitas secara rutin dikaji dan dibadningkan dengan kebijakan privasi online. Contoh pengendaliannya adalah entitas mengkontrak pihak ketiga untuk secara rutin melakukan review dan penilaian kelemahan sistem. Sedangakan internal audit berfungsi melakukan penilaian sebagai bagian dari rencana audit tahunan. Hasil dan rekomendasi untuk perbaikan dilaporkan kepada pihak manajemen.

4.2 Terdapat proses untuk mengidentifikasi melemahnya kemampuan entitas dalam mencapai tujuan yang berhubungan dengan kebijakan privasi online sistem yang telah ditentukan. Contoh pengendaliannya adalah pertemuan staf IT dilakukan untuk membahas permasalahan privasi, penemuan masalah baru didiskusikan dalam pertemuan yang berlangsung minimal 4 kali dalam setahun.

4.3 Perubahan teknologi dan lingkungan dipantau dan dampaknya terhadap keamanan sistem dinilai secara periodik. Contoh pengendaliannya adalah CPO memantau persyaratan privasi dan mengubah praktik privasi pada pasar yang entitas lakukan.

2.3 Kriteria dan Contoh Control untuk Prinsip Confidentiality

Prinsip kerahasiaan berfokus pada informasi yang dinilai rahasia. Tidak seperti informasi pribadi yang teridentifikasi, yaitu yang telah didefinisikan oleh aturan di berbagai negara di dunia, saat ini tidak ada definisi yang diakui secara luas dari informasi yang bersifat rahasia. Pada sesi komunikasi dan transaksi bisnis, konsumen seringkali bertukar informasi yang mereka perlukan untuk dijaga kerahasiannya. Pada banyak kejadian, pihak-pihak yang berkepentingan ingin untuk meyakinkan

bahwa informasi yang merika berikan hanya tersedia bagi individu-individu yang perlu mengakses untuk menyelesaikan transaksi atau menjawab pertanyaan-pertanyaan yang mungkin ada. Untuk meningkatkan kepercayaan rekanan bisnis, sangatlah penting bahwa rekanan bisnis dijelaskan tentang praktik-praktik dari entitas pengelola situs web mengenai kerahasiaan. Entitas pengelola situs web perlu untuk mengungkapkan praktik-praktik berkaitan dengan bagaiamana mereka memberikan akses yang diotorisasi untuk menggunakan dan berbagi informasi yang bersifat rahasia.

Contoh informasi yang mungkin dapat dikategorikan sebagai rahasia adalah:

- Gambar atau desain teknik
- Rencana Bisnis
- Informasi perbankan suatu perusahaan
- Ketersediaan inventori
- Harga penawaran atau permintaan
- Daftar harga
- Dokumen hukum
- Daftar pelanggan dan klien
- Penghasilan suatu perusahaan

Tidak seperti informasi pribadi, pada informasi rahasia tidak terdapat hak akses terhadap informasi yang didefinisikan untuk memberi keyakinan mengenai kelengkapan dan ketepatan informasi. Sehingga interpretasi tentang apa yang dimaksud sebagai informasi rahasia dapat beragam dari setiap usaha dan kebanyakan kasus interpretasi diperngaruhi oleh kontrak kesepakatan. Sehingga penting bagi pihak yang menjalani bisnis dengan memanfaatkan situs web atau akan memanfaatkan situs web untuk memahami dan menerima informasi apa yang dinilai rahasia dan hak akses atau harapan-harapan lain dari klien untuk mengupdate informasi untuk memberi keyakinan akan ketepatan dan kelengkapan.

Informasi yang diberikan kepada pihka lain rentan terhadap akses ilegal selama transmisi dan selama informasi disimpan pada sistem komputer pihak lain. Sebagai contoh, pihak ilegal dapat menangkap informasi, instruksi-instruksi perjanjian, dan transaksi saat sedang ditransmisikan. Pengendalian-pengendailan seperti enkripsi dapat digunakan untuk melindungi kerahasiaan informasi selamam transmisi, sedangkan firewall dan pengendalian akses ilegal dapat membantu melindungi informasi saat sedang disimpan pada sistem komputer.

Berikut ini adala kriteria dan contoh control untuk prinsip privasi kerahasiaan:

1.0 Wilayah kebijakan: Entitas mendefinisikan dan mendokumentasikan kebijakan yang berhubungan dengan perlindungan informasi rahasia.

1.1 Kebijakan entitas yang berhubungan dengan perlindungan informasi rahasia dibuat, dikaji, dan disetujui oleh pihak yang ditunjuk.Contoh pengendaliannya adalah Petugas keamanan mengkaji kebijakan yang berhubungan dengan kerahasiaan setahun sekali dan meyerahkan rekomendasi perubahan untuk disetujui oleh komite standar teknologi informasi.

1.2 Kebijakan entitas yang berhubungan dengan perlindungan informasi rahasia meliputi hal-hal (tetap tidak membatasi):

a. Identifikasi dan dokumentasi persyaratan kerahasiaan dari user yang sah

b. Mengizinkan akses, mendefinisikan sifat akses, dan siapa yang mengotorisasi akses tersebut.

c. Mencegah akses yang tidak diotorisasi

d. Prosedur untuk menambah user baru, memodifikasi tingkat akses dari user yang ada, dan menghapus user yang tidak lagi memerlukan akses.

e. Penugasan pertanggungjawaban dan akuntabilitas untuk kerahasiaan sistem

f. Penugasan pertanggungjawaban dan akuntabilitas untuk perubahan dan pemeliharaan sistem.

g. Melakukan tes, evaluasi, dan mengotorisasi komponen sistem sebelum implementasi.

h. Menyediakan fasilitas untuk menangani komplain dan permintaan atas permasalahan yang berkaitan dengan kerhasiaan.

i. Prosedur untuk menangani pembobolan keamanan dan kecelakaan lainnya

j. Menyediakan alokasi untuk pelatihan dan sumber daya lain untuk mendukung kebijakan kerahasiaan.

k. Penanganan eksepsi dan situasi yang tidak secara spesifik diatur yang berhubungan dengan kebijakan kerahasiaan.

l. Identifikasi dari kekonsistenan terhadap hukum dan peraturan yang berlaku, komitemn yang telah didefinisikan, kesepakatan layanan, dan kontrak lainnya.

1.3 Pertanggungjawaban dan akuntabilitas untuk kebijakan kerahasiaan sistem entitas, serta perubahan dan update terhadap kebijakan yang ditetapkan. Contoh pengendalianya adalah manajemen telah memberikan tanggung jawab kepada wakil

presiden tentang kebijakan kerahasiaan entitas, dan tim sumber daya manusia. Sedangkan tanggung jawab implementasi kebijakan diberikan kepada CIO. Pihak lain dalam dewan eksekutif membantu dalam melakukan review, update, dan persetujuan kebijakan sebagaiamana tercantum dalam buku panduan dewan eksekutif.

2.0 Wilayah komunikasi: Entitas mengkomunikasikan kebijakan mengenai perlindungan terhadap informasi pribadi kepada pihak internar dan eksternal.

2.1 Entitas telah mempersiapkan deskripsi tujuan dari sistem dan batasannya dan mengkomunikasikan deskripsi tersebut pada pihak yang berwenang. Contoh pengendaliannya adalah entitas menempatkan deskripsi sistem pada situs web.

2.2 Kewajiban kerahasiaan dan komitmen kerhasiaan kepada pelanggan dikomunikasikan kepada user yang sah sebelum informasi rahasia diberikan. Komunikasi termasuk hal-hal berikut tetapi tidak terbatas pada:

a. Bagaimana suatu informasi dinilai rahasia dan kapan tidak lagi bersifat rahasia.
b. Bagaimana akses ke informasi rahasia diotorisasi.
c. Bagaimana informasi rahasia diguanakan
d. Bagaimana informasi rahasia didistribusikan.
e. Jika informasi diberikan kepada pihak ketiga, pemberitahuaan termasuk pembatasan keprecayaan pada pengendalian kerahasiaan pihak ketiga. Pemberitahuan yang tidak cukup mengindikasikan bahwa entitas mempercayai pengendalian dan praktik kerahasiaan pihak ketiga yang memenuhi atau melebihi standar entitas.
f. Praktik kerahasiaan harus taat pada hukum dan peraturan yang berlaku.

Contoh pengendaliannya adalah kesepakatan penutupan informasi yang disetujui diperlukan sebelum mendistribusikan informasi rahasia kepada pihak ketiga. Kontrak pelanggan, kesepakatan layanan dinegosiasikan sebelum pelaksanaan atau penerimaan layanan. Perubahan terhadap standar kerahasiaan pada kontrak memerlukan perstujuan dewan eksekutif.

2.3 Tanggung jawab dan akuntabilitas untuk kebijakan kerahasiaan situs web beserta perubahan dan updatenya dikomunikasikan kepada pegawai pengelola situs web yang yang bertanggung jawab mengimplementasikannya. Conrohnya adalah petugas administrasi keamanan bertanggung jawab akan pemeliharan setiap hari dan memeberikan rekomendasi perbaikan kepada CIO dan komite IT.

2.4 Proses pemberitahuan pembobolan kerahasiaan sistem situs web dan pelaporan komplain dikomunikasikan kepada user yang sah. Proses bagi konsumen atau pihak eksternal untuk memberitahu entitas akan kemungkinan pembobolan kerrahasiaan sistem dan kecelakaan lainnya ditempatkan pada situs web atau dijadikan sebagai bagian dari fitur penerimaan user baru.

2.5 Perubahan yang dapat mempengaruhi kerahasiaan sistem dikomunikasikan kepada manajemen dan konsumen yang dipengaruhi. Contoh pengendaliannya adalah perubahan yang dapat mempengaruhi kerahasiaan sistem dikaji dan disetujui oleh konsumen yang dipengaruhi dan sesuai kesepakatan pelayanan yang telah ditetapkan sebelum meengimplementasikan perubahan yang direncanakan.

3.0 Wilayah prosedur: entitas menggunakan prosedur-prosedur untuk mencapai tujuan kerahasiaan sistem yang telah didokumentasikan sesuai dengan definisi kebijakannya.

3.1 Prosedur entitas yang memerlukan pengungkapan informasi rahasia kepada pihka lain hanya jika sesuai dengan kebijakan kerhasiaannya. Contoh pengendaliannya adalah paryawan karyawan diharuskan menandatangani perjanjian kerahasiaan sebagai bagian dari pekerjaan mereka. Perjanjian ini melarang segala bentuk pengungkapan informasi dan data yang karyawan telah akses.

3.2 Entitas memiliki prosedur untuk mendapatkan keyakinan bahwa kebijakan kerahasiaan pada pihak ketiga yang menerima transfer informasi dan dipercayai oleh entitas sesuai dengan kebijakan kerahasiaan entitas, dan pihak ketiga taat terhadap hukum dan kebijkan tersebut. Contoh pengendaliaannya adalah Entitas mengetahui pengendalian yang dilakukan oleh pihak ketiga dan mendapatkan laporan mengenai efektivitas pengendalian dari auditor independe.

3.3 Pada kejadian kebijakan kerahasiaan tidak lagi dijalani atau diperlonggar, entitas memilii prosedur untuk melindungi informasi rahasia dengan melakksanakan praktik kerahasiaan saat informasi tersebut diterima entitas, atau

dengan mendapatkan izin dari pelanggan untuk mengikuti praktik kerahasiaan yang baru berhubungan dengan informasi pelanggan yang rahasia. Contoh pengendaliannya adalah perubahan pada permasalahan kerahasiaan dinegosiasi kembali dengan rekanan bisni.

3.4 Kriteria prinsip kerahasiaan yang berkaitan dengan keamanan sejenis dengan kriteria untuk prinsip keamanan dari poin 3.1 sampai dengan 3.12.

4.0 Wilayah pemantauan: Entitas memantau sistem dan mengambil tindakan untuk menjaga ketaatan kepada kebijakan kerahasiaan yang telah ditetapkan.

4.1 Kinerja kerahasiaan entitas secara rutin dikaji dan dibadningkan dengan kebijakan kerahasiaan. Contoh pengendaliannya adalah entitas mengkontrak pihak ketiga untuk secara rutin melakukan review dan penilaian kelemahan sistem. Sedangkan internal audit berfungsi melakukan penilaian sebagai bagian dari rencana audit tahunan. Hasil dan rekomendasi untuk perbaikan dilaporkan kepada pihak manajemen.

4.2 Terdapat proses untuk mengidentifikasi melemahnya kemampuan entitas dalam mencapai tujuan yang berhubungan dengan kebijakan kerahasiaan sistem yang telah ditentukan. Contoh pengendaliannya adalah pertemuan staf IT dilakukan untuk membahas permasalahan privasi, penemuan masalah baru didiskusikan dalam pertemuan yang berlangsung minimal 4 kali dalam setahun.

4.3 Perubahan teknologi dan lingkungan dipantau dan dampaknya terhadap kerahasiaan sistem dinilai secara periodik. Contoh pengendaliannya adalah CPO memantau persyaratan kerahasiaan dan mengubah praktik kerhasiaan pada pasar yang entitas lakukan.

3. Kriteria dalam Pemberian Sertifikat Webtrust oleh CA

Dalam menerbitkan suatu sertifkat webtrust, banyak kriteria yang CA harus penuhi. Pada makalah ini penulis akan memaparkan kriteria EV dalam penerbitan sertifikat dari sisi CA dan kriteria tambahan selain kriteria yang telah dipaparkan sebelumnya yang harus dipenuhi suatu entitas untuk mendapatkan sertfikat EV webtrust.

3.1 Kriteria dalam Penerbitan Sertifikat EV Webtrust

Semua CA yang akan menerbitkan sertifikat EV sebelum menerbitkan sertifikat EV, baik CA dan root CA harus memenuhi beberapa kriteria yaitu:

a. Ketaatan, CA dan Root CA setiap waktu harus:

1. Taat kepada semua hukum yang berlaku dan sertifikat yang diterbitkan pada setiap wilayah yuridiksi di mana pemegang sertfikat beroperasi.
2. Taat dengan semua persyaratan yang ada pada panduan EV.
3. Taat dengan semua persyaratan program webtrust saat ini dan mendatang dan program webtrust EV sekarang dan mendatang yang disetujui oleh CAB Forum
4. Terlisensi sebagai CA disetiap wilayah yurisdiksi di mana CA beroperasi untuk menerbitkan setifikat EV.

b. Kebijakan EV

1. Implementasi, CA dan root CA harus mengembangkan, mengimplementasikan, menjalankan, menampilan dengan jelas pada situs web, dan secara rutin mengupdate praktik-praktik setifikasi EV auditabel yang diperlukan, seperti certification practice statement (CPS) dan certificate policy (CP) yang:
   - Mengimplementasikan persyaratan dari panduan-panduan EV yang direvisi dari waktu ke waktu.
   - Mengimplementasikan persyaratan program webtrust untuk CA sekarang dan mendatang dan program webtrust EV atau program yang lainnya CAB forum.
   - Menspesifikasikan hirarki CA dan root CA termasuk semua root yang CA perluakan untuk menerbitkan sertifikat EV untuk otentikasi sertifikat-sertifikat EV tersebut.
2. Pengungkapan, CA dan root CA harus secara publik mengungkapan kebijakan EV denagn cara online yang siap diakses dan layak yang tersedia selama 7 x 24 jam seminggu. CA juga disyaratkan untuk secara publik untuk mengungkapkan CPSnya. CPS harus dibentuk sesuai standar RFC 2527 atau RFC 3647.
3. Komitmen untuk taat dengan panduan. CA dan CA root harus secara publik mentaati panduan EV dengan memasukkannya ke dalam kebijakan EV. Sebagai tambahan CA harus memasukkan secara langsung atau dengan rujukan persyaratan dari panduan pada semua kontrak denagn subordinat CA, RA, RA perushaan, dan

subkontraktor yang terlibat atau berhubungan dengan penerbitan atau pemeliharaan sertifikat EV.

c. Asuransi

1. CA dan root CA harus memelihara beberapa asuransi yang berhubungan dengan kinerja dan kewajibannya dalam panduan EV, yitu:
   a. Asuransi kewajiban umum komersial dengan batas kebijakan minimal 2 juta dollar amerika
   b. Asuransi kehilangan dan kewajiban atas kesalahan profesional dengan batas kebijakan minimal sebesar 5 juta dollar amerika dan mencakupi klaim atas kerusakan yang terjadi akibat kesalahan, kehilangan, atau pelanggaran kontrak yang tidak disengaja, atau lalai dalam menerbitkan atau memelihara sertifikat EV, dan klaim atas kerusakan yang diakibatkan pelanggaran hak kepemilikan dari pihak ketiga manapun (termasuk copyright, trademark), dan pelanggaran privasi dan kecacatan iklan.
2. Asuransi tersebut harus berada pada perusahaan asuransi dengan predikat minimum A- dalam panduan asuransi terbaik atau dalam asosiasi perusahaan asuransi dengan penilaian predikat yang setara.
3. CA dan atau root CA boleh mengasuransikan sendiri kewajiban yang mungkin muncul akibat kinerja CA, dalam panduan EV diperluakan setidaknya 500 juta dollar amerika pada aset likuid pada laporan keuangan yang telah diaudit selama 12 balun lalu, dan dengan quick ratio (perbandingan antara aset likuid dengan kewajiban likuid) tidak kurang dengan 1.0.

d. Persyaratan Audit

CA dan root CA harus memenuhi persyaratan audit dalam rangka ketaatan yang ada dalam panduan EV.

3.2 Kriteria Untuk Mendapatkan Sertifikat EV Webtrust

CA hanya menerbitkan sertifikat kepada pihak yang memenuhi berbagai persyaratan, yaitu:

a. Kriteria untuk organisasi swasta, CA dapat memberikan sertfikat EV kepada organisasi swasta yang memenuhi persyaratan tertentu yaitu:

1. Organisasi swasta harus diakui sebagai entitas yang legal yang keberadaannya diakui karena terdaftar pada departmen perindustrian atau institusi lainnya yang disyaratkan hukum pada wilayah yurisdikis tertentu.
2. Organisasi swasta harus tidak ditandai oleh departmen perindustrian atau institusi lainnya yang disyaratkan oleh hukum pada wilayah yurisdiksi tertentu sebagai ”tidak aktif”, ”tidak valid” atau status lainnya yang sejenis.
3. Wilayah yurisdiksi dari organisasi swasta bukanlah wilayah yang dilarang bagi CA untuk menerbitkan sertifikat oelh hukum.
4. Organisasi swasta tidak berada pada negara yang terdapat pada daftar pelarangan seperti embargo perdagangan dalam hukum yursidiksi CA.

b. Kriteria untuk institusi pemerintahan, CA dapat memberikan sertfikat EV kepada institusi pemerintahan yang memenuhi persyaratan tertentu yaitu:

1. Keberadaan institusi pemerintahan berada pada wilayah yurisdiksi CA.
2. Institusi ridak boleh berada pada negara yang di mana CA dilarang untuk menerbitkan sertfikat oleh hukum pada yurisdiksi CA.
3. Institusi pemerintahan tidak berada pada negara yang terdapat pada daftar larangan seperti embargo ekonomi dalam hukum yurisdiksi CA.

c. Kriteria untuk badan lainnya, sebelum kriteria tambahan didefinisikan pada panduan EV, CA tidak boleh menerbitkan sertifikat EV kepada siapapun atau organisasi apapun yang tidak memenuhi persyaratan sebagai organisasi swasta dan pemerintahan yang telah dipaparkan di atas.

3.3 Prosedur Pengecekan Status dan Pencabutan sertifikat

3.3.1 Pemeriksaan status sertfikat EV

a. Repository, CA harus menjaga mekanisme repository online selama 24 jam x 7 dalam seminggu di mana browser dapat dapat secara otomastis memeriksa dengan online status terkini dari semua sertifikat.

1. Untuk setiap sertfikat EV atau sertifikat subordinat CA yang diterbitkan kepada suatu entitas yang tidak diatur oleh entitas lain yang mengatur root CA:

- CRL harus diupdate dan diterbitkan ulang setidaknya setiap 7 hari dan dengan waktu kadaluarsa maximum 10 hari, atau
- OCSP, jika CA menggunakan Online Certificate Status Protocol (OCSP), CA harus menjaga kapabilitas OCSP yang diupdate setiap 7 hari sekali dengan waktu kadaluarsa maksimum 10 hari

2. Untuk sertifikat subordinat CA yang dikendalikan root CA:
   - CRL harus diupdate dan diterbitkan ulang setidaknya setiap 12 bulan dan dengan waktu kadaluarsa maximum 12 bulan, atau
   - OCSP, jika CA menggunakan Online Certificate Status Protocol (OCSP), CA harus menjaga kapabilitas OCSP yang diupdate setiap 12 bulan sekali dengan waktu kadaluarsa maksimum 12 bulan

b. Pengalaman user yang wajar, pada kejadian di mana CA memilih untuk mengoperasikan kalpabilitas CRL, CA harus memastikan bahwa semua CRL untuk sebuah rantai sertifikat EV dapat didownload tidak lebih dari 3 detik melalui jalur telepon analog pada kondisi normal.

c. Waktu respon, CA harus beroperasi dan mempertahankan kapabilitas CRL dan atau OCSP dengan sumber daya yang cukup untuk memberikan waktu respon yang wajar secara komersial untuk beberapa query yang dibangkitkan oleh semua sertfikat yang diterbitkan oleh CA.

d. Penghapusan masukan, masukan pencabutan dari CRL dan atau OCSP tidak boleh dihapus sebelum waktu kadaluarsa sertifikat EV yang dicabut.

3.3.2 Pencabutan Sertifikat EV

a. Kapabilitas dan panduan pencabutan, CA harus mempublikasikan panduan yang jelas untuk mencabut sertifikat CA sebagai bagian dari kebijakannya untuk EV dan menjaga 24 jam x 7 dalam seminggu untuk menerima dan merespon permintaan pencabutan dan pertanyaan lainnya.

b. Kejadian Pencabutan, CA harus mencabut sertifikat EV yang telah diterbitkannya jika terjadi salah satu kejadian di bawah ini:

1. Pemegang sertifikat memohion pencabutan sertifikat EV.
2. Pemegang sertifikat mengindikasikan bahwa permintaan sertifikat EV yang asli tidak diotorisasi yang berarti tidak mendapatkan otorisasi.
3. CA memeperoleh bukti yang cukup kuat bahwa kunci privat pemegang sertfikat telah disalahgunakan atau tidak dilindungi dengan layak.
4. CA menerima pemberitahuan atau menyadari bahwa pengadilan atau badan arbitrase telah mencabut hak pemegang sertifikat untuk menggunakan nama domain yang terdaftar pada sertifikat EV.
5. CA menerima pemberitahuan atau menyadari bahwa pemegang sertifikat melanggar kewajiban dalam kesepakatan sertifkat EV.
6. CA menerima pemberitahuan atau menyadari perubahan materi informasi yang terkandung pada sertifikat EV.
7. Keyakinan pada kebijaksanaan CA bahwa sertifikat EV tidak diterbitkan berdasarkan persyaratan dan kondisi panduan EV atau kebijakan EV.
8. Jika CA tidak yakin sepenuh hati bahwa informasi apa saja yang muncul pada sertifikat EV tidak akurat.
9. CA menghentikan operasi dengan alasan apapun dan tidak direncanakan untuk EV CA dalam melakukan pencabutan sertifikat.
10. Hak CA untuk menerbitkan sertifikat berakhir berdasarkan panduan EV atau dicabut kecuali jika CA mmbuat perjanjian untuk menjaga repositori CRL/OCSP.
11. Kunci privat CA untuk sertfikat EV telah diketahui.
12. Kejadian pencabutan tambahan yang dipublikasikan pada kebijakan EV.
13. CA menerima pemberitahuan atau menyadari bahwa pemegang sertfikat menjadi pihak yang dilarang atau termasuk ke dalam daftar hitam atau kegiatan bisnisnya dilarang oleh hukum dalam wilayah yurisdiksi CA

3.3.3 Kapabilitas respon dan pelaporan masalah sertifikat EV

a. Pelaporan, sebagai tambahan kepada pencabutan sertifikat EV, CA harus memberikan pemegang sertifikat, pihak yang menaruh kepercayaan, vendor aplikasi perangkat lunak, dan pihak ketiga lainnya instruksi-instruksi jelas untuk pelaporan komplain atau kecurigaan akan kebocoran kunci privat, penyalahgunaan sertfikat EV, atau kecurangan, penyalahgunaan,

penyelewengan lainnya yang berhubungan dengan sertifikat EV, serta kemampuan untuk menerima dan menjawab laporan tersebut.

b. Penyidikan, CA harus memulai penyidikan terhadap semua laporan masalah sertifikat EV kurang dari 24 jam dan menentukan apakah pencabutan atau tindakan pantas lainnya berdasarkan setidaknya satu kriteria berikut:

1. Sifat permasalahan yang diduga tanpa bukti
2. Jumlah laporan masalah sertfikat yang diteriam tentang situs web atau sertifikat EV tertentu.
3. Identitas pihak yang melakukan komplain (contoh: komplain dari penegak hukum bahwa suatu situs web melakukan kegiatan ilegal memiliki bobot lebih dari pada komplain dari pelanggan yang bersikeras bahwa dirinya trdak pernah menerima barang yang ia pesan)
4. Perwakilan yang relevan pada aparat penegak hukum.

c. Respon, CA harus menjaga kemampuan terus menerus selama 24jam x 7 dalam seminggu untuk secara internal merespon terhadap laporan masalah sertfikat yang memiliki prioritas tinggi, dan jika laoran tersebut layak, CA meneruskan komplain tersebut kepada pihak penegak hukum dan atau mencabut sertifikat EV yang menjadi subjek komplain.

4. Kesimpulan dan Saran

4.1 Kesimpulan

Webtrust adalah salah satu bentuk assurance services yang memberikan keyakinan yang wajar atas efektivitas kinerja suatu situs web dan ketaatannya terhada standar, hukum, dan aturan yang berlaku. Untuk mendapatkannya, situs web harus memenuhi kriteria-kriteria yang banyak dari kriteria tersebut sangat erat kaitannya dengan kriptografi.

Setelah memaparkan dengan cukup detil kriteria-kriteria tersebut, penulis berasumsi bahwa situs web yang memiliki stempel webtrust dapat dikatakan aman dengan tingkat keyakinan yang wajar.

4.2 Saran

Karena situs web yang telah memiliki stempel webtrust dapat dikatakan aman dengan tingkat keyakinan yang wajar, maka penulis sarankan bagi para konsumen untuk melakukan transaksi hanya dengan situs web dengan stempel webtrust agar menjaga informasi pribadi dan rahasia konsumen tetap terjaga. Keuntungan lainnya dari menggunakan situs web berstempel webtrust adalah adanya perlindungan konsumen dari segi kerahasiaan dan keprivasian.

Saat ini stempel webtrust belum terlalu dikenal di Indonesia. Penulis sarankan bagi para pengelola web di Indonesia untuk menggunakan jasa webtrust untuk meningkatkan kepercayaan pada situs web karena sebagaimana kita ketahui, Indonesia dikenal tidak aman dalam masalah dunia cyber. Tetapi tentunya jasa webtrust tidaklah murah yaitu seharga $295 sehingga banyak pengelola web yang enggan menggunakannya. Oleh karena itu penulis menyarankan agar pihak-pihak yang terkait dalam penerbitan sertfikat webtrust untuk berusaha agar biaya jasa webtrust terjangkau di seluruh dunia.

Daftar Pustaka

[1] A. Arens, Alvin and J. Elder, Randal and S. Beasley, Mark (2006) “Auditing and Assurance Services”, Prentice Hall
[2] http://www.aicpa.org
[3] http://www.wikipedia.org