Syntax Literate: Jurnal Ilmiah Indonesia p–ISSN: 2541-0849 e-ISSN: 2548-1398
Vol. 7, No. 12, Desember 2022

DESAIN KERANGKA KERJA KEAMANAN INFRASTRUKTUR DOMPET DIGITAL MENGGUNAKAN PCI DSS 4.0 DAN COBIT 2019 BERBASIS ANALISIS MANAJEMEN RISIKO

Mangampu Silaban, Kalamullah Ramli
Department of Electrical Engineering, Faculty of Engineering, Universitas Indonesia, Depok, Indonesia
E-mail: mangampu.silaban@ui.ac.id, kalamullah.ramli@ui.ac.id

Abstrak

Dompet digital adalah salah satu bentuk transaksi elektronik yang semakin diminati oleh setiap orang. Selain penggunaan yang praktis karena tidak perlu memegang duit sebagai alat pembayaran secara langsung, proses untuk pendaftarannya juga dinilai tidak cukup sulit untuk dilakukan. Akan tetapi dibalik semua kemudahan yang terdapat dalam dompet digital, sebagai suatu aplikasi yang di dalamnya terdapat dana yang berasal dari pengguna, aplikasi dompet digital ini menjadi salah satu aplikasi yang sedang gencar diincar oleh para pelaku serangan siber. Pada makalah ini akan dibahas terkait proses desain suatu kerangka kerja keamanan pada lingkup infrastruktur dompet digital yang menggunakan standarisasi kombinasi PCI DSS 4.0 dan COBIT 2019 menggunakan pendekatan analisis berbasis manajemen risiko. Kerangka kerja ini berisikan point-point terkait manajemen risiko yang berupa identifikasi ruang lingkup, aset dan celah keamanan, asesmen risiko, evaluasi risiko, pengendalian risiko dalam bentuk validitas dan penerapan kendali terhadap risiko dan monitoring serta umpan balik dari penerapan kontrol terhadap risiko yang timbul. Dengan adanya kerangka kerja keamanan infrastruktur ini diharapkan dapat menjadi acuan bagi setiap perusahaan dompet digital khususnya perusahaan yang beroperasional dalam wilayah negara Kesatuan Republik Indonesia untuk dapat mengendalikan risiko di lingkungan transaksi elektronik sehingga operasional dapat berjalan sesuai dengan tujuan yang diharapkan dengan meminimalisir setiap serangan-serangan siber yang timbul pada setiap aset infrastruktur dompet digital.

Kata kunci: cobit, e-wallet, pci-dss, manajemen risiko.

Abstract

Digital wallets are one form of electronic transactions that are increasingly in demand by everyone. In addition to practical use because there is no need to hold

How to cite:	Mangampu Silaban, Kalamullah Ramli (2022) Desain Kerangka Kerja Keamanan Infrastruktur Dompet Digital Menggunakan PCI DSS 4.0 dan COBIT 2019 Berbasis Analisis Manajemen Risiko, (7) 12, http://dx.doi.org/10.36418/syntax-literate.v7i12.11645
E-ISSN:	2548-1398
Published by:	Ridwan Institute

money as a means of payment directly, the process for registration is also considered not difficult enough to do. However, behind all the conveniences contained in a digital wallet, as an application in which there are funds derived from users, this digital wallet application is one of the applications that are being intensively targeted by cyber attack actors. This paper will discuss the design process of a security framework within the scope of digital wallet infrastructure that uses standardization of a combination of PCI DSS 4.0 and COBIT 2019 using a risk management-based analysis approach. This framework contains points related to risk management in the form of identification of scope, assets and security gaps, risk assessment, risk evaluation, risk control in the form of validity and application of control over risk and monitoring and feedback from the application of control against risks that arise. With this infrastructure security framework, it is expected to be a reference for every digital wallet company, especially companies operating within the territory of the Unitary State of the Republic of Indonesia to be able to control risks in the electronic transaction environment so that operations can run according to the expected goals by minimizing any cyber attacks that arise on each digital wallet infrastructure asset.

Keywords: *cobit, e-wallet, pci-dss, risk management.*

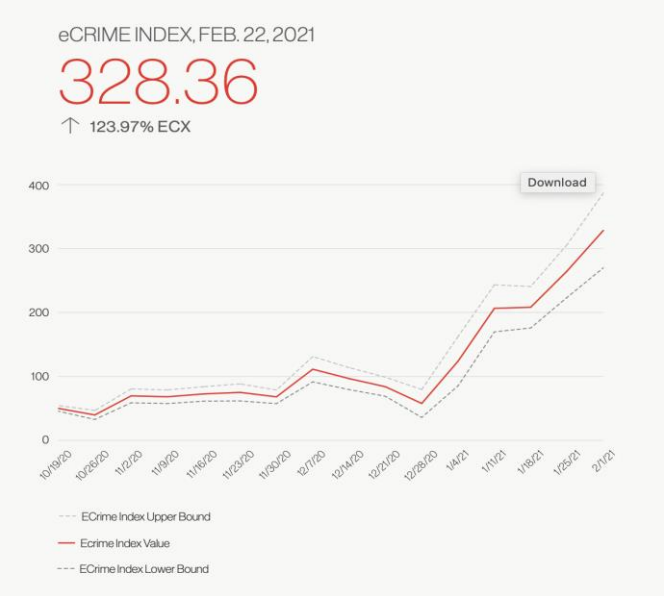
Pendahuluan

Teknologi digital pada saat ini memegang peranan yang sangat penting dalam setiap sendi kehidupan masyarakat. Salah satu sektor yang mengalami penyesuaian teknologi digital adalah terkait pembayaran elektronik dimana perubahan pola pembayaran ini mengalami evolusi pada setiap masa mulai dari sistem barter, uang tunai, transfer hingga pada saat ini dikenal dengan sebutan dompet digital (Suleman et al., 2021).

Pada saat ini sudah banyak perusahaan yang mengembangkan sistem dompet digital mulai dari konglomerasi multi nasional hingga perusahaan domestik. Tidak hanya dari segi jumlah perusahaan saja, jumlah dana yang mengalir dan transaksi yang terjadi juga menggambarkan bahwa metode pembayaran dompet digital ini perlahan tapi pasti sudah mulai menggantikan segala jenis metode pembayaran konvensional (Lawaceng & Rahayu, 2020).

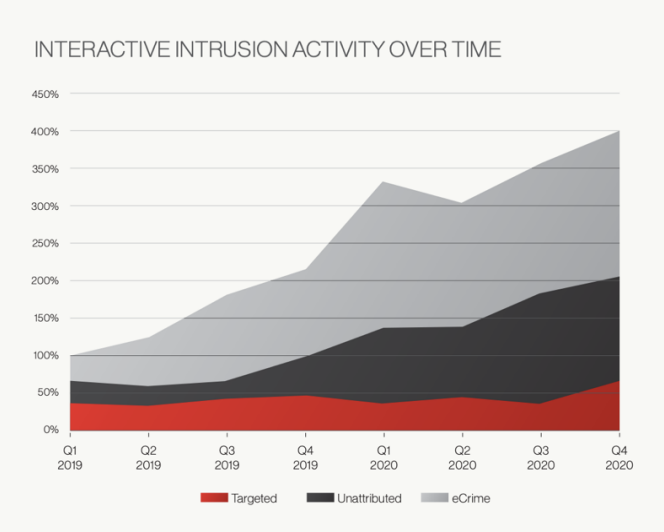
Hal ini tentu menjadi sesuatu kabar yang menggairahkan khususnya kepada setiap insan yang bekerja dalam bidang Informasi Teknologi. Akan tetapi di balik euforia besar terhadap penggunaan teknologi digital ini untuk melakukan pembayaran, terdapat suatu fakta yang patut diwaspadai oleh setiap stakeholder yang berada di dalamnya. Dalam data yang dibagikan oleh Crowdstrike di Global Report Threat tahun 2022 (Jasper, 2017), menunjukkan adanya kenaikan e-crime index per periode yang artinya kriminal siber setiap periode semakin meningkat.

Gambar 1
e-crime Index Crowdstrike



Dengan fakta grafik ini, setiap pemangku kepentingan dalam dompet digital seharusnya semakin waspada dan meningkatkan daya tahan sistem aplikasi dompet digital untuk berbenah dalam menangkal serangan siber.

Gambar 2
Interactive Instrution Activity



Dari gambar 2 di atas juga terlihat bahwa grafik instrution activity e-crime yang semakin meningkat hampir 2 kali lipat yang dihitung dari periode quarter keempat 2019 ke quarter keempat 2020. Dengan kondisi ini dapat diperkirakan, apabila perlindungan keamanan terhadap suatu sistem tidak diperkuat, faktor e-crime suatu saat akan memperoleh celah kerentanan terhadap sistem tersebut.

Hal berikutnya yang menjadi bahan pertimbangan untuk perusahaan memikirkan sistem keamanan infrastruktur pada layanan dompet digital ini adalah penguatan sistem yang mengacu kepada CIA Triad yaitu suatu sistem acuan keamanan siber yang mensyaratkan data informasi yang berada dalam sistem bersifat rahasia, integritas dan selalu tersedia setiap saat (Siwiendrayanti et al., 2015). Faktor CIA Triad ini menjadi salah satu jaminan yang juga dipersyaratkan oleh lembaga pengawas keuangan pemerintah Indonesia seperti Bank Indonesia (BI) dan Otoritas Jasa Keuangan (OJK).

Dalam POJK No. 13/POJK.02/2018 pasal 28 ayat (2) tentang Inovasi Keuangan Digital di Sektor Keuangan mensyaratkan bahwa setiap penyelenggara kegiatan dompet digital wajib untuk menyusun kebijakan, prosedur dan standar dari beberapa aspek diantaranya adalah aspek risiko keamanan informasi (Clarissa et al., 2020). Kebijakan ini semakin dikuatkan oleh Peraturan Bank Indonesia Nomor 20/6/PBI/2018 terkait Transaksi Elektronik Pasal 13 ayat 4 mewajibkan penyelenggara untuk memiliki kebijakan Manajemen risiko dan penerapan keamanan informasi (Salsabila & Sulistiyono, 2019).

Pada makalah ini, penulis melakukan langkah-langkah untuk penyusunan suatu desain kerangka kerja keamanan pada layanan dompet digital menggunakan kombinasi PCI DSS 4.0 dan COBIT 2019 dengan menggunakan analisis manajemen risiko sehingga diharapkan kerangka kerja ini akan menjadi panduan bagi setiap pemangku kepentingan di layanan dompet digital untuk membentuk sistem keamanan yang handal dengan tindakan pengendalian berbasis kepada analisis risiko.

Literature Review

Pada bagian ini, peneliti menjelaskan terkait setiap literatur yang digunakan dalam mendukung penelitian desain kerangka kerja ini. Literatur yang digunakan dijelaskan pada setiap sub bagian berikut:

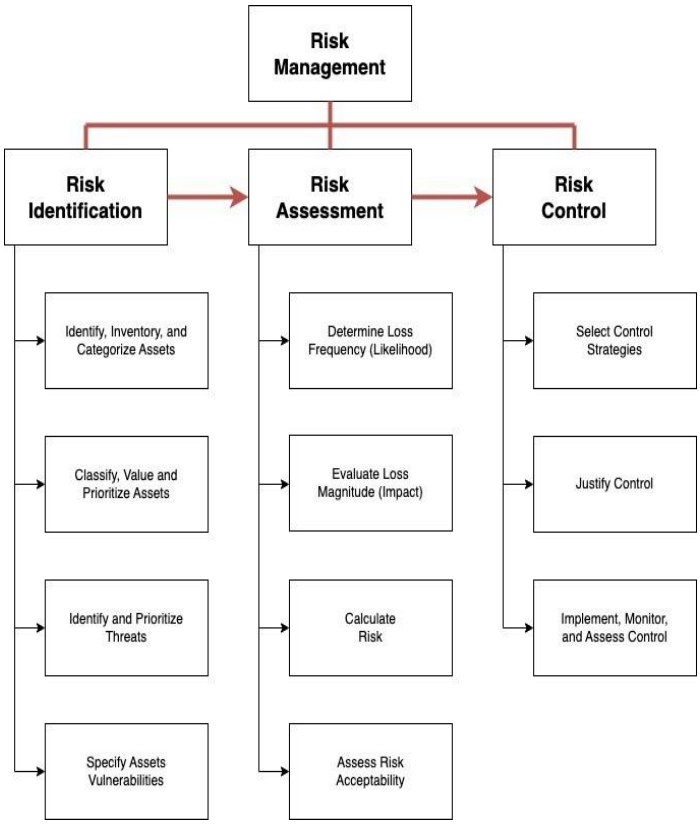
1. Dompet Digital

   Menurut Bank Indonesia dalam Peraturan Bank Indonesia Nomor 20/6/PBI/2018 terkait Transaksi Elektronik menyatakan bahwa dompet digital yaitu suatu transaksi elektronik yang menggunakan aplikasi digital sebagai tempat penyimpanan dana yang dapat dipergunakan untuk melakukan pembayaran yang dilakukan melalui dalam jaringan. Dompet digital ini adalah suatu perkembangan metode dari cara pembayaran yang mengikuti trend revolusi industri digital 4.0 (Mulyana et al., 2021).

   Dalam kegiatan operasionalnya, menurut Bank Indonesia juga dalam Peraturan Bank Indonesia Nomor 18/40/PBI/2016 menyatakan bahwa ada 2 (dua) hal yang paling utama yang diwajibkan oleh Bank Indonesia untuk dilengkapi oleh pihak penyelenggara jasa sistem pembayaran yaitu menerapkan manajemen risiko secara efektif dan konsisten serta menerapkan standar keamanan sistem informasi (Fidhayanti, 2020).
2. Manajemen Risiko Perusahaan

Menurut Whitman (2021), risiko merupakan suatu kemungkinan dari timbulnya suatu peristiwa yang tidak diinginkan yang menyebabkan timbulnya suatu kehilangan terhadap tujuan suatu organisasi atau kegiatan. Dalam suatu aktivitas kegiatan pasti memiliki suatu risiko dan manajemen risiko hadir sebagai reaksi organisasi atau perusahaan terhadap risiko yang timbul untuk mencegah dampak yang melenceng jauh dari tujuan utama organisasi atau perusahaan.

Gambar 3
Komponen dalam Manajemen Risiko



Berdasarkan gambar diatas, manajemen risiko memiliki 3 (tiga) komponen utama yaitu identifikasi risiko, asesmen risiko dan kontrol risiko. Identifikasi risiko terdiri dari bagian untuk melakukan identifikasi, inventory dan kategorisasi aset. Kemudian aktivitas kegiatan dilanjutkan dengan melakukan klasifikasi, penilaian dan prioritas aset (Syahindra et al., 2022). Lalu proses selanjutnya adalah dengan melakukan identifikasi dan prioritas ancaman serta melakukan spesifikasi celah keamanan pada aset secara spesifik. Faktor ancaman dan celah keamanan pada aset ini akan memunculkan risiko yang dapat berakibat aset terkompromise dan tidak akan memiliki kemampuan maksimal sesuai dengan tujuan organisasi (Hamzah et al., 2020).

Pada bagian asesmen risiko terdapat penentuan frekuensi dari serangan terjadi dalam periode tertentu. Kemudian dalam asesmen risiko ini juga akan dilakukan evaluasi terhadap dampak terjadinya risiko, lalu dilanjutkan dengan pengukuran

risiko dengan melihat faktor-faktor ancaman, celah keamanan dan frekuensi terjadinya serangan (Indarta et al., 2022). Pengukuran kalkulasi risiko ini akan memetakan risiko-risiko yang terdeteksi ke dalam suatu level pengukuran risiko dan pada bagian akhir dari asesmen risiko ini akan ditentukan dari hasil setiap tingkat risiko tersebut, perlakuan apa saja yang akan dilakukan, apakah diterima, dimitgasi, dihindari atau ditransfer ke pihak ketiga (Putri et al., 2023).

Lalu langkah selanjutnya adalah pemberian kendali risiko. Pada bagian ini terjadi langkah untuk pemilihan kontrol yang strategis, kemudian melakukan justifikasi kontrol apakah sudah sesuai diterapkan untuk risiko-risiko yang dihadapi dan langkah terakhir adalah melakukan implementasi, monitor dan melakukan asesmen terhadap kontrol yang diterapkan (Kholmi, 2011).

3. Payment Card Industry Data Security Standard 4.0 (PCI DSS 4.0)

Payment Card Industry Data Security Standard (PCI DSS) pada mulanya hadir sebagai suatu standar jawaban untuk mengakomodir terhadap kebutuhan industri kartu kredit. Hal yang menjadi fokus dalam standard kerangka kerja ini adalah bagaimana dapat meakukan perlindungan terhadap data pemegang kartu dan bagaimana dapat melakukan perlindungan terhadap akun-akun terotorisasi yang masuk untuk mengelola sistem kartu keredit tersebut (Zulaeha, 2017).

Seiring dengan perkembangan teknologi, PCI DSS juga dapat digunakan untuk pengguna transaksi pembayaran elektronik seperti dompet digital dengan menitikberatkan kepada data akun pengelola dan data pengguna aplikasi dompet digital. Secara khusus, PCI DSS dikembangkan untuk melakukan review atas setiap aktivitas kegiatan yang berhubungan dengan keamanan data rekening pembayaran dan memfasilitasi adopsi luas langkah-langkah keamanan data yang konsisten secara global (Ardiyanto, 2015). Secara global ada 6 tujuan utama dari standar kerangka kerja PCI DSS ini dan dibagi ke dalam 12 persyaratan khusus yang dapat dilihat dalam tabel 2.1 di bawah (Santoso, 2016).

Tabel 1
Tujuan dan Persyaratan Khusus PCI DSS

Goals	PCI DSS Requirement
Build and Maintain Secure Network and Systems	1. Install and maintain network security controls
	2. Apply secure configurations to all system components
Protect Account Data	3. Protect stored account data
	4. Protect cardholder data with strong cryptography during transmission over open, public networks
Maintain a Vulnerability Management Program	5. Protect all systems and networks from malicious software
	6. Develop and maintain secure systems and software
Implement Strong Access Control Measures	7. Restrict access to system components and cardholder data by business need to know
	8. Identify users and authenticate access to system components
	9. Restrict physical access to cardholder data
Reguraly Monitor and Test Networks	10. Log and monitor all access to system components and cardholder data
	11. Test security of system and network regularly
Maintain an Information Security Policy	12. Support information security with organizational policies and programs

Dari tabel terlihat adanya tujuan untuk membangun dan memelihara jaringan dan sistem yang aman. Dari tujuan tersebut ada 3 persyaratan khusus yang harus dipenuhi yaitu instalasi dan pemeliharaan terhadap kendali keamanan jaringan dan penerapan konfigurasi yang aman ke seluruh komponen sistem.

Sementara itu untuk tujuan perlindungan terhadap data akun, persyaratan khusus yang harus dipenuhi adalah serta perlindungan data akun yang disimpan dan perlindungan data pemegang kartu/pengguna dengan penggunaan kriptografi yang kuat selama pengiriman melalu jaringan publik yang terbuka. Hal ini dilakukan agar data akun yang merupakan inti dari proses bisnis dompet digital ini aman dari segala bentuk serangan siber baik itu dalam penyimpanan maupun ketika dalam pengiriman data.

Kemudian untuk tujuan berikutnya adalah pemeliharan kepada program manajemen celah keamanan. Pada tujuan ini, persyaratan yang harus dipenuhi adalah perlindungan seluruh sistem dan jaringan dari perangkat lunak yang berbahaya dan pengembangan dan pemeliharaan sistem dan perangkat lunak yang aman. Sering sekali ketika sistem dan jaringan sudah terlindungi, serangan keamanan informasi tersebut memanfaatkan celah keamanan dari perangkat lunak yang dipergunakan dengan cara para staf pengelola sistem secara tidak sengaja melakukan instalasi terhadap suatu perangkat lunak tanpa melakukan pengetesan ataupun pencobaan perangkat lunak tersebut kepada suatu sistem Non-Live yang terpisah dengan sistem produksi. Alhasil karena kecerobohan personil yang melakukan pengelolaan dan pemeliharaan, celah keamanan menjadi tercipta melalui perangkat lunak yang berbahaya.

Selanjutnya, tujuan dari PCI DSS adalah melakukan implementasi pengukuran kendali terhadap akses yang kuat. Untuk tujuan ini, persyaratan khusus yang dilakukan sesuai dengan PCI DSS adalah membatasi akses ke komponen sistem dan data pengguna kartu berdasarkan kebutuhan bisnis untuk diketahui, melakukan identifikasi pengguna dan otentikasi akses ke komponen sistem serta pembatasan akses fisik ke pengguna data. Pada bagian ini diatur terkait akses fisik untuk masuk ke lokasi perangkat dompet data digital berada serta akses virtual yang berupa VPN ataupun metode lain agar pengelola dapat melakukan operasional terhadap sistem dompet digital tersebut.

Kemudian ada tujuan untuk melakukan monitoring dan pengetesan jaringan secara reguler. Tujuan ini dilakukan dengan persyaratan khusus melakukan pengumpulan log dan pemantauan seluruah akses ke komponen sistem dan data pemegang kartu dan melakukan pengetesan keamanan sistem dan jaringan secara reguler. Pengetesan dapat dilakukan dengan cara penerapan penetration test secara berkala untuk melihat setiap celah keamanan yang ada dalam jaringan dan sistem dompet digital yang ada.

Dan untuk tujuan terakhir dari PCI DSS ini adalah untuk melakukan pemeliharaan terhadap kebijakan keamanan informasi. Untuk tujuan ini, persyaratan

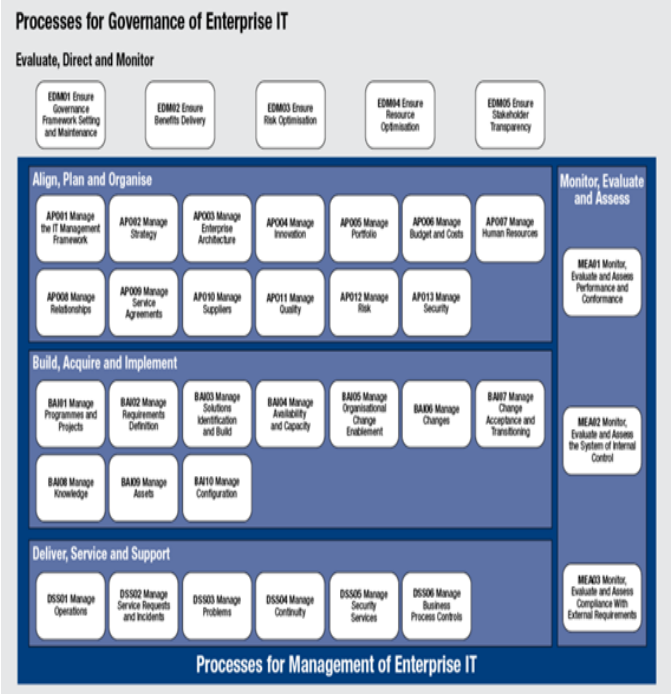
khusus yang diperlukan adalah mendukung keamanan informasi dengan program-program dan kebijakan-kebijakan terorganisir.

Untuk saat ini, versi standar PCI DSS sudah berubah dari PCI DSS v3.2.1 menjadi PCI DSS 4.0. Hal ini dilakukan untuk mengakomodir point-point baru yang berhubungan dengan perkembangan teknologi digital khususnya di bidang pembayaran elektronik (Purnama, 2018).

4. Control Objectives for Information Technologies (COBIT) 2019

Control Objectives for Information Technologies (COBIT) 2019 adalah suatu standar yang banyak digunakan oleh organisasi yang memiliki basis dalam pengelolaan Informasi dan Teknologi (I&T). Standar kerangka kerja ini mengedepankan 2 bagian besar dalam pelaksanaannya yaitu tata kelola manajemen yang diperbarui dan pengelolaan yang sesuai dengan kebutuhan bisnis dalam dunia I&T (Soesanto, 2022).

Gambar 4
Proses Domain Kerangka Kerja COBIT 2019[11]



Dari gambar 4 terlihat 5 proses domain kerangka kerja COBIT 2019 yaitu:

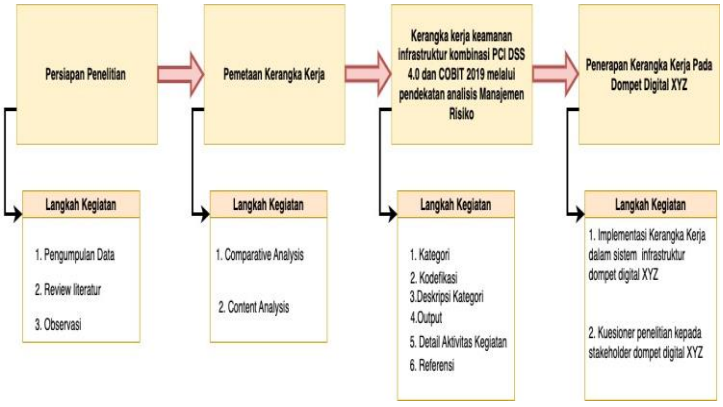
a. Evaluate, Direct and Monitoring (EDM) yaitu merupakan domain tata kelola yang melakukan penilaian terkait setiap opsi strategis yang dipilih dan pemantauan pencapaian strategis.
b. Align, Plan and Organize (APO) merupakan domain manajemen untuk menjelaskan terkait keseluruhan organisasi, strategi dan kegiatan pendukung untuk IT.

c. Build, Acquire and Implement (BAI) merupakan domain manajemen yang menjelaskan definisi, akuisisi dan implementasi solusi I&T serta integrasi dalam proses bisnis.
d. Deliver, Service and Support (DSS) merupakan domain manajemen yang menjelaskan terkait operasional pengiriman, pelayanan dan dukungan dari setiap aktivitas kegiatan operasional.
e. Monitor, Evaluarte and Assess (MEA) yaitu domain manajemen yang menangani pemantauan, evaluasi dan penilaian dari kinerja sistem I&T.

5. Terkait Penelitian

Penelitian ini dilakukan dengan langkah-langkah yang sesuai dengan gambar 5 berikut:

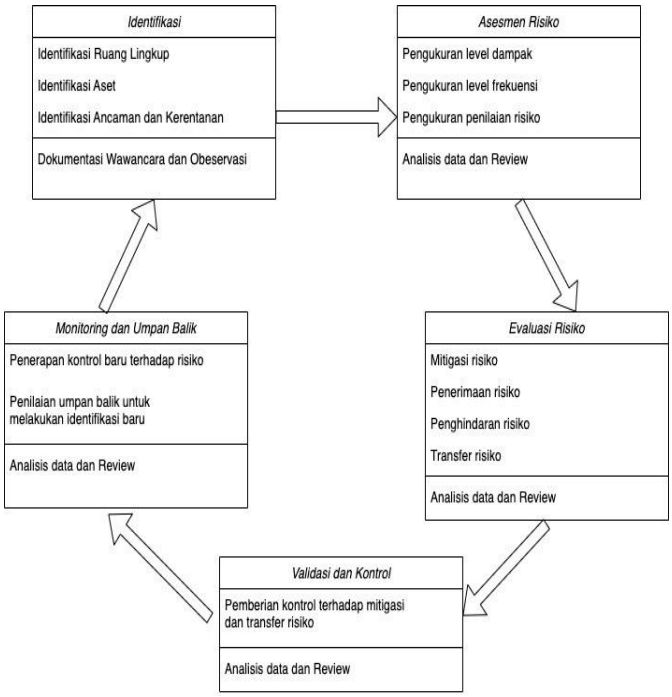
Gambar 5
Langkah-Langkah Penelitian



a. Persiapan Penelitian

Pada tahap Langkah ini, kegiatan yang dilakukan adalah pengumpulan data-data yang menjadi target penelitian yaitu perusahaan yang memiliki layanan dompet digital dengan segala dokumentasi yang dibutuhkan dalam penelitian ini. Kemudian dilakukan review literatur terhadap analisis manajemen risiko, PCI DSS, COBIT 2019 dan makalah-makalah lain yang berkaitan dengan keamanan jaringan dan informasi. Dari persiapan penelitan ini didapat diagram alir dari siklus kerangka kerja keamanan berbasis manajemen risiko seperti gambar 6.

Gambar 6
Diagram Alir Manajemen Risiko



Pada gambar 6 di atas, terdapat 5 (lima) bagian besar yaitu identifikasi, asesmen risiko, evaluasi risiko, validasi dan kontrol serta monitoring dan umpan balik. Kelima kategori ini merupakan pengembangan dari 3 (tiga) bagian dari manajemen risiko yaitu identifikasi risiko, asesmen risiko dan kendali risiko. Dengan adanya pengembangan diagram alir ini, akan lebih mudah untuk melakukan detail aktivitas kegiatan dari kelima kategori dan lebih mudah untuk dipahami dan diaplikasikan dalam suatu sistem infrastruktur aplikasi.

Identifikasi merupakan tahapan pertama dari kerangka kerja ini, dimana identifikasi sendiri terdiri dari identifikasi ruang lingkup, identifikasi aset dan identifikasi ancaman dan kerentanan. Tujuan dari identifikasi ini adalah untuk dapat menggali, mendalami setiap ruang lingkup, aset, ancaman dan kerentanan yang terdapat dalam sistem yang ada. Hal ini juga termasuk kontrol yang sudah diterapkan sebelum kerangka kerja ini dilakukan. Tahapan ini dapat dilakukan dengan cara wawancara, dokumentasi dan observasi terhadap lingkungan dalam sistem tersebut.

Kemudian asesmen risiko merupakan tahapan kedua dari kerangka kerja ini. Tujuan dilakukan asesmen risiko ini adalah untuk membuat suatu tolok ukur tingkatan dari dampak, frekuensi maupun penilaian risiko dari setiap aset yang terdapat dalam sistem. Untuk tahapan ini dilakukan dengan analisis data dan review dari aset, level ancaman dan data dari personel yang mengelola sistem tersebut.

Tahapan ketiga adalah melakukan evaluasi risiko. Pada tahapan ini, adalah langkah selanjutnya setelah diperoleh tolok ukur pelevelan dari setiap dampak, frekuensi dan risiko yang dapat timbul dari setiap aset. Setelah diperoleh tingkatan risiko yang timbul, maka perlu dilakukan evaluasi dan perlakuan organisasi terhadap risiko tersebut disesuaikan dengan sumber daya tersedia, apakah risiko tersebut akan dimitigasi, diterima, dihindari atau ditransfer ke pihak ketiga. Hal ini dilakukan dengan cara analisis dan diskusi terutama kepada pihak manajemen untuk level apa yang akan dilakukan terhadap risiko yang telah dinilai.

Langkah selanjutnya adalah pemberian validasi dan kontol. Langkah ini dilakukan setelah dilakukan evaluasi risiko dan risiko dalam tahapan untuk dilakukan mitigasi dan transfer. Sesuai dengan keputusan manajemen dan pemangku kepentingan, akan dibuat suatu kontrol dari setiap risiko apabila diperlukan berdasarkan diskusi dengan pihak manajemen. Langkah ini sangat erat kaitannya dengan sumber daya yang mampu untuk disediakan organisasi.

Kemudian di langkah terakhir terdapat proses monitoring dan umpan balik. Langkah ini dilakukan dengan cara penerapan dan pemantauan terhadap setiap kontrol yang sudah diambil sesuai dengan keputusan manajemen. Kemudian secara berkala, setiap kontrol yang ada akan dilakukan penilaian dan menjadi umpan balik sebagai masukan untuk tahapan identifikasi selanjutnya. Dengan demikian pengendalian risiko dalam sistem organisasi teresbut dilakukan dengan cara berkesinambungan dalam suatu bagan diagram alir yang tersiklus.

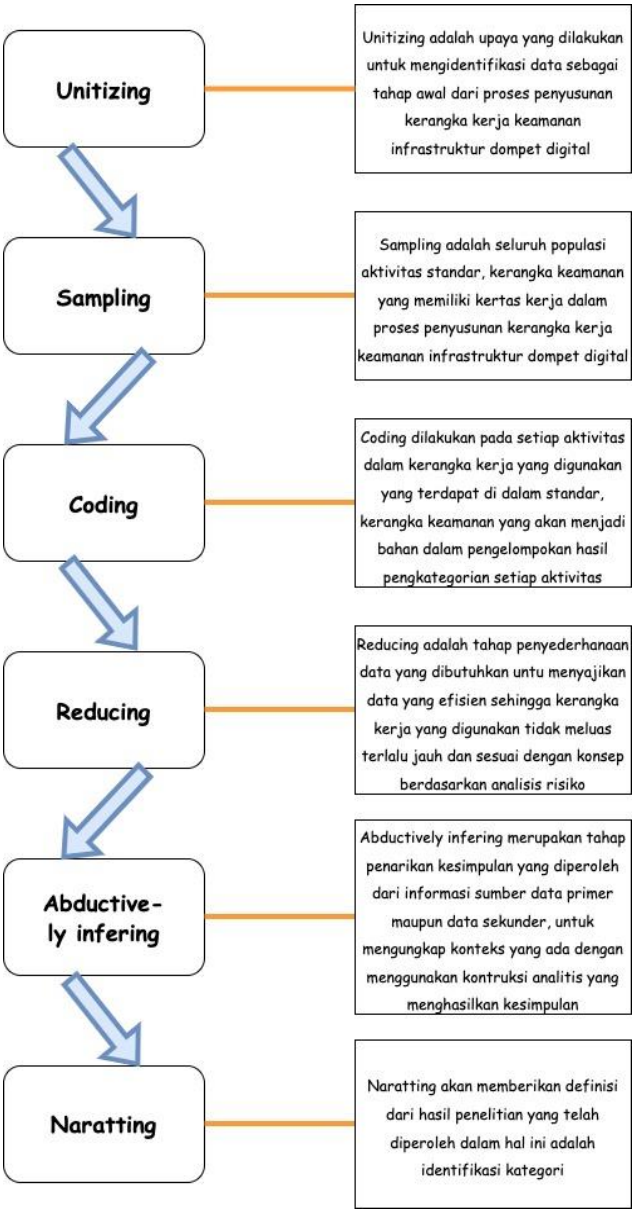
b. Pemetaan Kerangka Kerja Standarisasi PCI DSS 4.0 dan COBIT 2019 Pada Diagram Alir Manajemen Risiko

Langkah kedua yang dilakukan dalam penelitian ini adalah melakukan pemetaan standarisasi PCI DSS 4.0 dan COBIT 2019 pada diagram alir manajemen risiko. Dalam melakukan pemetaan ini, metode yang digunakan adalah metode analisis perbandingan dan analisis konten.

Pada metode analisis perbandingan, penelitian dilakukan dengan cara perbandingan setiap point dari aktivitas masing-masing standarisasi ke dalam setiap kategori yang terdapat dalam diagram alir manajemen risiko. Perbandingan-perbandingan ini akan dituangkan dalam detail aktivitas dari masing-masing standarisasi.

Sementara itu metode analisis konten menurut Sulistyowati, merupakan tahap analisis yang bertujuan mendalami dan menggali makna tersembunyi dari informasi yang telah diperoleh dari tahap sebelumnya. Metode ini dilakukan dengan melakukan review dan pemahaman dari setiap konten detail aktivitas yang terdapat dalam setiap standarisasi. Hal ini dilakukan mulai dari unitizing, sampling, coding, reducing, deductively infering, narrating (Oktavia & Karlimah, 2018). Penjelasan dari setiap tahapan dapat terlihat dari gambar di bawah ini.

Gambar 7
Tahapan Analisis Konten



c. Kerangka Kerja Keamanan Infrastruktur Kombinasi PCI DSS 4.0 dan COBIT 2019 Melalui Pendekatan Analisis Manajemen Risiko

Hasil dari pemetaan kerangka kerja kemudian dikembangkan dalam tabel kerangka kerja yang setiap kolom berisikan :

1) Category

Kategori merupakan bagian yang terdapat dalam manajemen risiko yang terdiri dari identifikasi, asesmen risiko, evaluasi risiko, validasi dan kontrol serta monitoring dan umpan balik.

2) Coding

Kodefikasi atau pengkodean adalah suatu penomoran dalam bentuk kode dalam kerangka kerja yang berfungsi untuk memberikan kode khusus dalam setiap kategori dan detail aktivitas kegiatan dalam kerangka kerja.

3) Category Description
Deskripsi kategori merupakan suatu penjabaran detail dari setiap komponen yang terdapat dalam setiap kategori untuk memudahkan dalam melakukan analisa dan review dalam suatu sistem.
4) Output
Output merupakan langkah kongkrit yang dilakukan dalam setiap kategori. Output ini merupakan gambaran keluaran dari suatu sistem yang diharapkan
5) Activity Details
Kolom ini merupakan poin-poin spesifik yang dibuat berdasarkan hasil analisis perbandingan dan analisis konten dari tahap pemetaan dari kedua standarisasi PCI DSS 4.0 dan COBIT 2019.
6) References
Referensi merupakan kode-kode sumber detail aktivasi diambil yang berasal dari PCI DSS 4.0 dan COBIT 2019.

d. Implementasi Kerangka Kerja Pada Sistem Infrastruktur Dompet Digital

Proses penerapan kerangka kerja pada sistem infrastruktur dompet digital dilakukan dengan melihat setiap detail aktivitas kegiatan yang terdapat dalam kerangka kerja dan disesuaikan dengan sistem infrastruktur dan kebijakan manajemen yang terdapat dalam perusahaan dompet digital yang menerapkan.

Untuk setiap rekomendasi implementasi dari kerangka kerja ini dapat ditemukan dalam Apendix 1.

e. Validasi Indikator Penerapan Kerangka Kerja

Ketika kerangka kerja sudah diimplementasikan ke dalam suatu sistem infrastruktur yang dalam penelitian ini dilakukan dalam sistem dompet digital, maka perlu dilakukan pengujian untuk melihat sejauh mana penerapan kerangka kerja ini sudah berjalan. Indikator-indikator dalam penelitian ini dilakukan dengan cara menyebarkan suatu kuesioner penilaian terhadap implementasi kerangka kerja ini ke lingkungan dompet digital.

Menurut Roscoe dalam buku Research Method for Business, dalam point (a) menyatakan bahwa ukuran sampel yang layak dalam penelitan adalah 30 sampai dengan 500, dimana jumah 30 orang dianggap sudah mewakili dari jumlah populasi yang ada khususnya untuk populasi yang berjumlah 40 sampai dengan 500 orang (Surahman, 2017).

Kuesioner penelitian disebar secara online melalui media google form. Ada 7 (tujuh) pertanyaan detail yang diajukan dalam kuesioner tersebut dan ada 30 orang responden yang terlibat dalam pengisian dengan latar belakang jabatan dari Head sampai kepada staf pelaksana yang berkecimpung dalam bidang I&T dan layanan dompet digital.

Untuk pertanyaan pertama terkait apakah kerangka kerja keamanan jaringan yang dibentuk mudah untuk dipahami untuk produk layanan dompet digital. Dalam hasil kuesioner, sebanyak 80% responden menyatakan mudah dan sangat mudah dipahami.

Kemudian untuk pertanyaan kedua terkait kerangka kerja keamanan merupakan kerangka kerja yang mudah diterapkan, hasil dari kuesioner adalah 66,7% menyatakan responden mudah untuk dipahami.

Selanjutnya untuk pertanyaan apakah kerangka kerja keamanan tersebut sudah memiliki langkah-langkah lengkap dan mencakup seluruh kegiatan operasional, sebanyak 86,7% menyatakan bahwa kerangka kerja keamanan dalam penelitian ini sudah memiliki langkah-langkah yang lengkap.

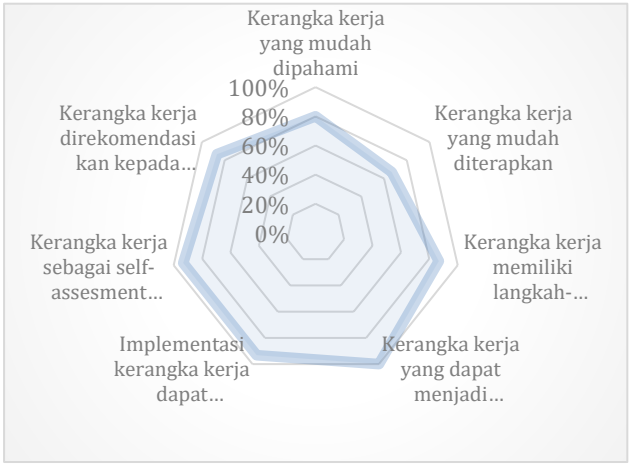
Kemudian untuk pertanyaan selanjutnya terkait apakah kerangka kerja keamanan ini bisa menjadi tolok ukur, sebanyak 100% responden setuju menyatakan bahwa kerangka kerja ini dapat dijadikan tolok ukur standar untuk layanan transaksi elektronik khususnya dompet digital.

Untuk pertanyaan selanjutnya apakah kerangka kerja ini bisa meminimalisir terjadinya risiko serangan siber dengan penerapan kontrol yang tepat, sebanyak 93,3% responden setuju bahwa kerangka kerja ini dapat digunakan untuk meminimalisir terjadinya risiko serangan siber dengan penerapan kontrol yang tepat.

Dan untuk pertanyaan apakah kerangka kerja keamanan ini dapat menjadi acuan untuk melakukan self-assesment kembali sebanyak 93,3% responden merasa bahwa kerangka kerja ini bisa digunakan sebagai acuan dari setiap pelaksana layanan dompet digital.

Untuk pertanyaan terakhir yang menyatakan apakah responden akan merekomendasikan kerangka kerja keamanan ini kepada rekan atau pelaku layanan dompet digital, sebanyak 86,6% responden mengaku akan merekomendasikan kerangka keamanan kerja ini.

Gambar 8
Hasil Kuesioner dalam Penerapan Kerangka Kerja Keamanan



Kesimpulan

Sehingga dari kesimpulan terkait penerapan kerangka kerja keamanan infrastruktur ini, dari hasil kuesioner kepada 30 orang responden menyatakan bahwa kerangka kerja ini mudah untuk dipahami, mudah untuk diterapkan, telah memiliki langkah-langkah yang lengkap terkait kegiatan operasional dompet digital, dapat menjadi tolok ukur untuk standar layanan dompet digital dapat meminimalisir terjadinya risiko serangan siber, dapat dipergunakan sebagai self-assesment dan akan merekomendasikan kerangka kerja keamanan infrastruktur ini kepada kolega ataupun pelaku yang terlibat dalam layanan dompet digital.

BIBLIOGRAFI

Ardiyanto, I. (2015). *Pelaksanaan Sistem Pengendalian Intern Pemerintah (Kasus Pada Suatu Satuan Kerja Di Jawa Timur)*. Universitas Brawijaya.

Clarissa, N. B., Njatrijani, R., & Triyono, T. (2020). Praktik Asuransi Kesehatan Digital Pada PT. Asuransi Allianz Life Cabang Semarang. *Diponegoro Law Journal*, *9*(2), 500–516.

Fidhayanti, D. (2020). Pengawasan Bank Indonesia Atas Kerahasiaan Dan Keamanan Data/Informasi Konsumen Financial Technology Pada Sektor Mobile Payment. *Jurisdictie*, *11*(1), 16.

Hamzah, R. A. F., Jaya, I. D., & Putri, U. M. (2020). Analisis Risiko Keamanan Sistem Informasi E-LKP Dengan Metode Octave Pada Perguruan Tinggi Negeri X. *JUSIFO (Jurnal Sistem Informasi)*, *6*(1), 55–65.

Indarta, Y., Ranuharja, F., Ashari, I. F., Sihotang, J. I., Simarmata, J., Harmayani, H., Algifari, M. H., Muslihi, M. T., Mahmudi, A. A., & Fatkhudin, A. (2022). *Keamanan Siber: Tantangan di Era Revolusi Industri 4.0*. Yayasan Kita Menulis.

Jasper, S. E. (2017). US cyber threat intelligence sharing frameworks. *International Journal of Intelligence and CounterIntelligence*, *30*(1), 53–65.

Kholmi, M. (2011). Akuntabilitas dalam perspektif teori agensi. *Journal of Innovation in Business and Economics*, *2*(02).

Lawaceng, C., & Rahayu, A. Y. S. (2020). Tantangan pencegahan stunting pada era adaptasi baru "New Normal" melalui pemberdayaan masyarakat di Kabupaten Pandeglang. *Jurnal Kebijakan Kesehatan Indonesia: JKKI*, *9*(3), 136–146. https://doi.org/10.22146/jkki.57781

Mulyana, M., Roup, A., & Sulastri, S. (2021). Pelatihan Penerapan Potongan Harga Pada Layanan Dompet Digital OVO. *Jurnal Abdimas Dedikasi Kesatuan*, *2*(2), 169–176.

Oktavia, R. N., & Karlimah, K. (2018). Analisis Kemampuan Komunikasi Matematis Siswa Kelas IV Sekolah Dasar Pada Materi Penjumlahan dan Pengurangan Bilangan Bulat. *PEDADIDAKTIKA: Jurnal Ilmiah Pendidikan Guru Sekolah Dasar*, *5*(3), 35–44.

Purnama, S. (2018). *Sistem Pendukung Keputusan Perceraian Menurut Hukum Islam Menggunakan Metode Naive Bayes*. UIN RADEN FATAH PALEMBANG.

Putri, H. D. Z., Mulyatno, I. P., & Manik, P. (2023). Studi Manajamen Risiko dengan Metode FTA dan FMEA akibat Keterlambatan Proyek Pembangunan Kapal Perintis KM. Sabuk Nusantara 72. *Jurnal Teknik Perkapalan*, *11*(2), 1–12.

Salsabila, S. S., & Sulistiyono, A. (2019). Urgensi Dikeluarkannya Peraturan Bank

Indonesia Nomor 20/6/Pbi/2018 Tentang Uang Elektronik (E-Money) Sebagai Alat Pembayaran. *Jurnal Privat Law*, *7*(2), 289–294.

Santoso, B. P. (2016). *Penyusunan Panduan Pengelolaan Keamanan Informasi Untuk Firewall Configuration Berdasarkan Kerangka Kerja PCI DSS v. 3.1 dan COBIT 5*. UNIVERSITAS AIRLANGGA.

Siwiendrayanti, A., Pawenang, E. T., & Endroyo, B. (2015). Iptek bagi Masyarakat (IbM) Dusun Lebari dan Dusun Krajan untuk Pengelolaan Air Buangan Rumah Tangga. *Rekayasa: Jurnal Penerapan Teknologi Dan Pembelajaran*, *13*(1).

Soesanto, S. (2022). Akuntansi Lingkungan Menuju Ekonomi Hijau Perspektif Relasi Natural Suistanibility Dengan Keberlanjutan Bisnis. *Account: Jurnal Akuntansi, Keuangan Dan Perbankan*, *9*(1).

Suleman, D., Zuniarti, I., & Rusiyati, S. (2021). Sosialisasi Strategi Menarik Minat Konsumen Untuk Membeli Produk Hasil UMKM. *PaKMas: Jurnal Pengabdian Kepada Masyarakat*, *1*(2), 134–141.

Surahman, I. (2017). Keefektifan Game Petualangan Baseta untuk Meningkatkan Pemahaman Materi Uji Teori Calon Pemohon SIM C di Wilayah Hukum Polres Jepara. *Advances in Police Science Research Journal*, *1*(1), 1–46.

Syahindra, I. P. S., Primasari, C. H., & Iriantor, A. B. P. (2022). Evaluasi Risiko Keamanan Informasi Diskominfo Provinsi XYZ Menggunakan Indeks Kami dan ISO 27005: 2011. *Jurnal Teknoinfo*, *16*(2), 165–182.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security*. Cengage learning.

Zulaeha, M. (2017). Hukum Transaksi Elektronik sebagai Panduan dalam menghadapi Era Digital Bisnis E-Commerce di Indonesia. *Hukum Transaksi Elektronik Sebagai Panduan Dalam Menghadapi Era Digital Bisnis E-Commerce Di Indonesia*.