Audit Keamanan Aplikasi E-Cash Menggunakan ISO 27001

Audit Security Application for E-Cash Using ISO 27001

Paradise[*1], Kusrini[2], Asro Nasiri[3]
[1,2,3]Program Pascasarjana Universitas Amikom Yogyakarta
E-mail: ***[1]emparadise.paradise@students.amikom.ac.id, [2]kusrini@amikom.ac.id, [3]asro@amikom.ac.id**

Abstrak

Mandiri e-cash adalah uang elektronik yang dikeluarkan oleh Bank Mandiri, berbasis server yang memanfaatkan teknologi aplikasi di handphone atau yang disebut sebagai uang tunai di handphone. Dalam pelaksanaannya, mandiri e-cash memberikan kemudahan kepada pengguna dalam proses transaksi keuangan, akan tetapi disamping itu banyak juga keluhan masyarakat akan maraknya tindak kejahatan dunia maya melalui mandiri e-cash. Keamanan adalah hal penting yang harus diperhatikan oleh pihak bank, mengingat pentingnya data-data yang ada pada aplikasi ini. Untuk mengukur keamanan informasi tersebut penulis akan melakukan audit menggunakan ISO 27001 untuk memastikan Bank Mandiri bekerja sesuai dengan procedure yang ada. ISO/IEC 27001:2005 adalah standar keamanan sistem informasi yang mempunyai 27 klausul untuk mengukur tingkat keamanan bank. Hasil audit didapatkan dari observasi, wawancara, dan pembagian kuisoner kepada responden yang telah dipilih. Hasil yang didapat dari penelitian ini adalah tingkat maturity level dari hasil perhitungan beberapa klausul yang dipilih. Dari hasil tersebut akan ditemukan rekomendasi dan saran untuk aplikasi Mandiri E-Cash.

***Kata Kunci** — Audit, E-Cash, ISO 27001*

Abstract

Mandirie-cash is an electronic money issued by Bank Mandiri, a server-based technology applications in mobile phones or called as cash in mobile. In practice, independent e-cash provides convenience to users in the process of financial transactions, but also many complaints besides communities will be rampant cyberspace crimes through mandiri e-cash. Security is important things that must be considered by the bank, given the importance of the existing data on this application. To measure the information security writers will use ISO 27001 audit to ensure Bank Mandiri working in accordance with the existing procedure. ISO/IEC 27001:2005 information systems security is a standard which has 27 clauses to measure the level of security of a company or organization. Audit results obtained from observation, interview, and Division kuisoner to selected respondents. The results obtained from this research is the level of maturity level of the results of the calculations of some of the selected clause. The results will be found from recommendations and suggestions for the standalone application E-Cash.

***Keyword** — Auditing, E-Cash, ISO 27001*

Dikirim: 12 Februari 2019; Direvisi: 20 Februari 2019; Diterima: 25 Februari 2019

1. PENDAHULUAN

Manusia menggunakan teknologi karena memiliki akal. Dengan akalnya manusia ingin keluar dari masalah, ingin hidup lebih baik, lebih aman, dan sebagainya. Perkembangan teknologi terjadi karena seseorang menggunakan akalnya untuk menyelesaikan setiap masalah yang dihadapinya. Kemajuan teknologi adalah sesuatu yang tidak bisa dihindari dalam kehidupan ini, karena kemajuan teknologi akan berjalan sesuai dengan kemajuan ilmu pengetahuan. Setiap inovasi diciptakan untuk memberikan manfaat positif bagi kehidupan manusia. Teknologi juga memberikan banyak kemudahan, serta sebagai cara baru dalam melakukan aktivitas manusia [1]. Perkembangan teknologi ini memiliki dampak besar pada banyak sektor tak terkecuali sektor perbankan Saat ini banyak kegiatan ekonomi yang memanfaatkan kecanggihan teknologi infromasi untuk memudahkan masyarakat seperti transaksi jual beli online, transfer mobile, atau juga pembayaran untuk pembelian dan tagihan melalui kartu kredit atau debit yang dikeluarkan oleh bank. Perkembangan teknologi telah membawa suatu perubahan kebutuhan masyarakat atas suatu alat pembayaran yang dapat memenuhi kecepatan, ketepatan, dan keamanan dalam setiap transaksi elektronik [2].

Mandiri *e-cash* adalah uang elektronik berbasis server yang memanfaatkan teknologi aplikasi di handphone dan USSD, atau yang disebut sebagai uang tunai di handphone, dimana memungkinkan pemegangnya untuk melakukan transaksi perbankan tanpa harus melakukan pembukaan rekening ke cabang Bank Mandiri. Keunggulan dari produk yaitu memberi pengalaman social banking bagi pemegangnya dan kemudahan dalam penggunaannya. Mandiri *e-cash* memiliki tiga karakter kemudahan yaitu: Gampang Dapat, Gampang Isi, dan Gampang Pakai. Dalam pelaksanaannya, mandiri *e-cash* memberikan kemudahan kepada pengguna dalam proses transaksi keuangan, akan tetapi disamping itu banyak juga keluhan masyarakat akan maraknya tindak kejahatan dunia maya melalui mandiri *e-cash*. Dari beberapa data yang didapat, kebanyakan faktor penipuan berawal dari jual beli online, yaitu pembeli diminta untuk mentransfer sejumlah uang ke nomor mandiri e-cash penipu. Sebelumnya perlu diketahui bahwa pengguna mandiri e-cash dibagi menjadi dua yaitu pengguna Registered dan Unregistered. *Registered* adalah pemegang mandiri *e-cash* yang telah melakukan *upgrade* layanan mandiri e-cash, yaitu dengan meng*upgrade* layanan melalui cabang dengan cara mengisi formulir *upgrade* layanan dan menyertakan *fotocopy* kartu identitas yang masih berlaku. Sedangkan pemegang *unregistered* adalah pemegang mandiri *e-cash* yang baru melakukan pendaftaran menggunakan data singkat berupa nama, tanggal lahir, dan email (*opsional*) [3].

Semakin besar dan berkembangnya suatu bank, maka akan semakin meningkat serta semakin kompleks pula kegiatan manajemennya. Kondisi ini membuat pihak bank harus mempunyai perencanaan, pengendalian serta pengawasan yang benarbenar baik. Manajemen juga dituntut untuk dapat menjaga keamanan harta bank serta mencegah kesalahan yang mungkin terjadi. Pihak manajemen memiliki tanggung jawab penuh mulai dari awal pembuatan rencana, memilih orang-orang yang tepat, memastikan bahwa orang-orang tersebut memang bekerja sesuai dengan rencana, serta memastikan bahwa segala sesuatunya berjalan sesuai dengan rencana. Di antara beberapa tanggung jawab manajemen tersebut, bagian yang paling penting adalah memastikan bahwa segala sesuatunya berjalan sesuai dengan rencana, dan hal ini juga dapat dilakukan dengan melakukan audit [4]. Audit sistem informasi adalah kegiatan melakukan evaluasi pada sistem dan mengumpulkan bukti-bukti serta temuan untuk menentukan apakah sistem yang digunakan telah dapat menjaga integritas data, melindungi asset bank dalam hal ini adalah aplikasi *e-cash*, memastikan apakah tujuan bank telah berjalan sesuai dengan visi misi, serta menggunakan sumber daya yang ada secara efektif dan efisien.

Audit keamanan sistem informasi dalam dilakukan dengan beberapa metode *framework*. Beberapa *framework* yang dapat di digunakan untuk melakukan audit kemanan adalah COBIT (*Control Objectives for Information and related Technology*), ISO *(International Organization for Standardization)*, ITIL (*Information Technology Infrastructure Library*), dan lain lain. Pada penelitian ini penulis akan melakukan audit menggunakan ISO 27001. ISO/IEC 27001 adalah standar information security yang memuat prinsip-prinsip dasar Information Security

Management Systems (Sistem Manajemen Keamanan Informasi – SMKI). Standar ini menggunakan pendekatan manajemen yang berbasis kontrol berdasarkan analisis risiko. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality, integrity dan availability*. Penelitian ini menggunakan 7 klausul, yaitu Prosedur Pengelolaan Aset, Organisasi Keamanan Informasi, Manajemen Aset, Keamanan Sumber Daya Manusia, Keamanan Fisik dan Lingkungan, Prosedur Pengendalian Akses, dan Manajemen Keamanan Informasi. Sebelum melakukan audit, terlebih dahulu melakukan observasi pada bank agar menyesuaikan dengan *framework* yang digunakan. Penelitian sebelumnya juga pernah melakukan audit menggunakan ISO 27001 dengan judul penelitian Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 dan COBIT 5 [5]. Penelitian ini dilakukan Wing Wahyu Winarno dan Armadyah Amborowati, dimana tujuan penelitian ini adalah untuk membuat tata kelola keamanan informasi sesuai dengan persyaratan SMKI ISO 27001:2013 dan kerangka kerja keamanan informasi COBIT 5. Kelebihan penelitian yang kami lakukan dibanding penelitian sebelumnya adalah penelitian ini memberikan saran dan rekomendasi yang tepat untuk objek penelitian, sedangkan penelitian sebelumnya tidak memberikan saran dan rekomendasi. Penelitian selanjutnya dilakukan oleh Agung Priambodo dan Ahmad Fauzan yang berjudul Audit Keamanan Sistem Informasi Manajemen Aset Pada PT. Puri Agung Management Services Menggunakan Metode ISO 27001:2005 [6]. Tujuan penelitian ini adalah untuk mengetahui tingkat maturity level dari hasil perhitungan beberapa klausul yang dipilih. Dari hasil tersebut akan ditemukan rekomendasi dan saran untuk aplikasi Mandiri E-Cash. Kelebihan penelitian kami adalah penelitian ini memiliki menggunakan 7 klausul sedangkan penelitian sebelumnya menggunakan 5 klausul. Selanjutnya penelitian dengan judul Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA Dan ISO 27001 Pada Organisasi XYZ [7]. Penelitian ini dilakukan oleh Raden Budiarto, dengan tujuan mengidentifikasi gangguan keamanan yang kemungkinan terjadi pada perusahaan XYZ, kemudian akan memberikan saran-saran dan rekomendasi yang sesuai untuk menjaga keamanan pada perusahaan tersebut. Kelebihan penelitian yang kami lakukan adalah penelitian ini menerapkan 7 konsul yang digunakan agar hasil audit dapat lebih spesifik, sedangkan yang penelitian sebelumnya tidak menyertakan berpaa jumlah klausul yang digunakan.

2. METODE PENELITIAN

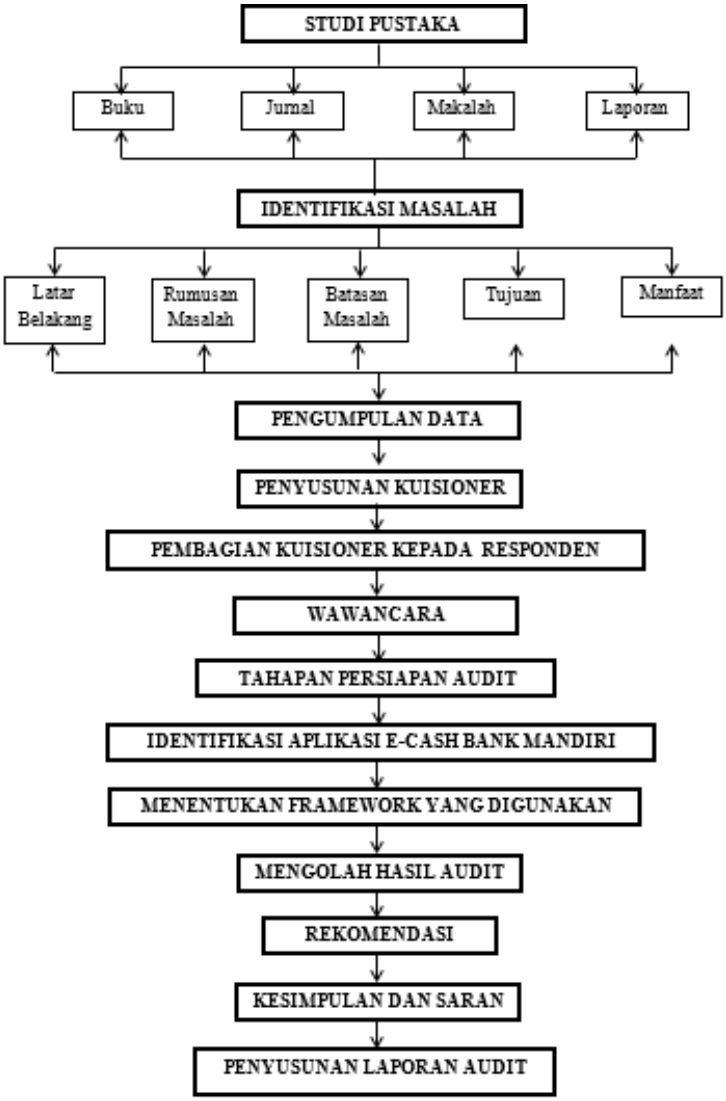
2.1. Metode Penelitian

Metode pelelitian yang digunakan pada penelitian ini adalah CISA (Certified Information Systems Auditor), dimana terdapat sepuluh (10) tahap yang dilakukan dalam proses audit [8], yaitu:

1. Membuat dan Mendapatkan Persetujuan Surat Kerjasama
2. Perencanaan Audit
3. Analisi Risiko.
4. Kemungkinan Audit
5. Pelaksanaan Audit
6. Pemeriksaan Data dan Bukti
7. Tes Audit
8. Pemeriksaan Hasil Audet
9. Pelaporan Audit
10. Penutup/ Exit Meting

Metode CISA memilik 10 tahapan dalam melakukan audit. Dari 10 tahapan tersebut, dapat dikelompkkan menjadi 4 bagian tahapan. Tahap pertama yaitu Perencanaan Audit dimana kegiatan yang dilakukan adalah membuat engamenet letter, identifikasi proses bisnis, penentuan ruang lingkup dan resiko, penentuan klausul. Tahap kedua, Persiapan Audit dimana dalam

tahapan ini akan menyusun kegiatan yang nantinya dilakukan saat mengaudit seperti, penyusunan jadwal kerja audit, menyampaian kebutuhan data, membuat pernyataan, membuat pembobotan, membuat pertanyaan. Tahap ketiga, Pelasanaan Audit yaitu melakukan wawancara atau observasi, pemeriksaan data, menyusun daftar temuan audit dan rekomendasi. Tahapan terakhir adalah tahap Pelaporan Audit yaitu permintaan tanggapan atas daftar temuan audit [9]. Gambar 1 merupakan gambaran metode penelitian yang digunakan.



Gambar 1. Alur Metode Penelitian

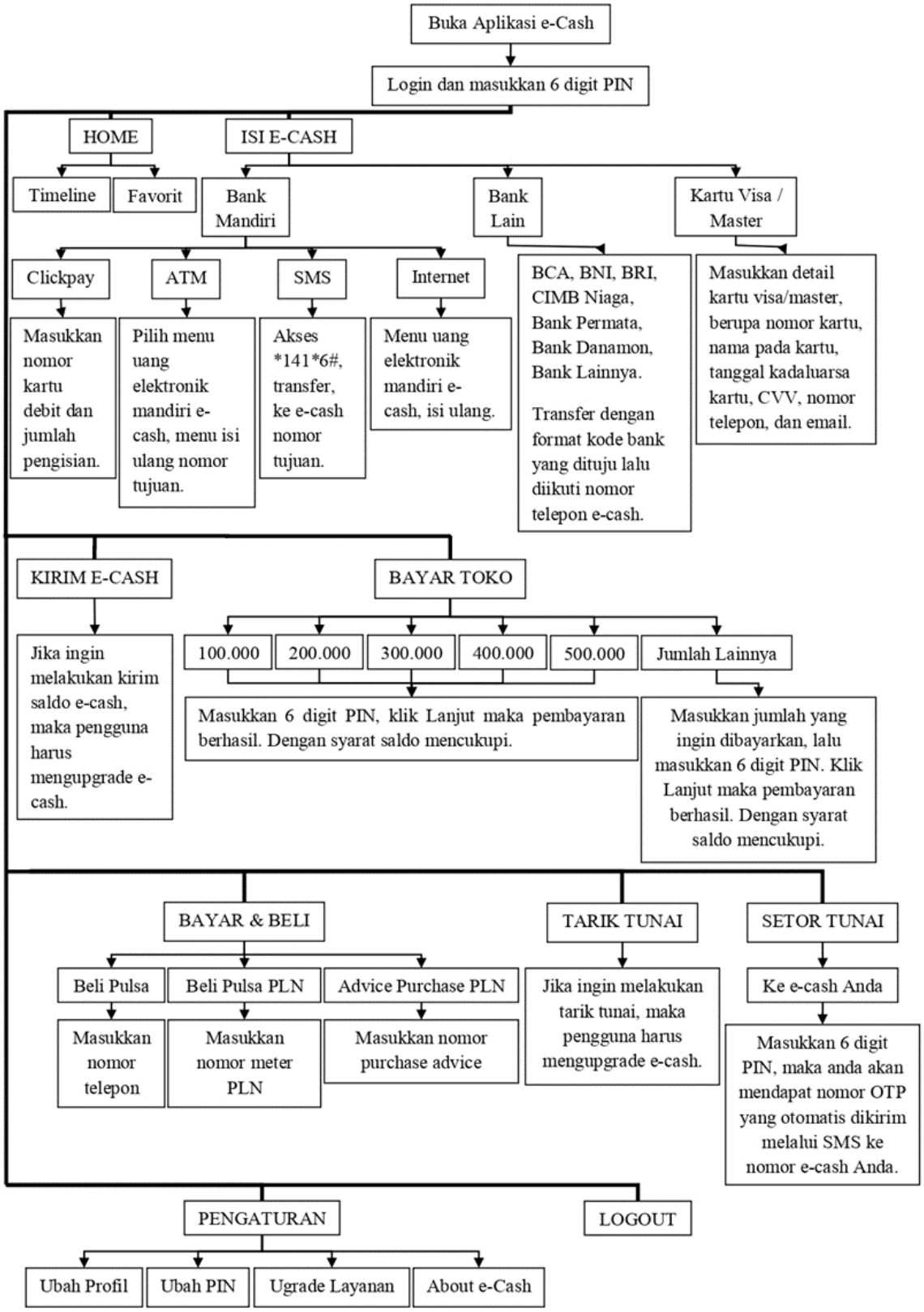
2.2. Framework yang Digunakan

Penelitian ini menggunakan ISO 27001:2005. ISO/IEC 27001 adalah standar information security yang memuat prinsip-prinsip dasar Information Security Management Systems (Sistem Manajemen Keamanan Informasi – SMKI). Standar ini menggunakan pendekatan manajemen yang berbasis kontrol berdasarkan analisis risiko. Dengan penerapan ISO/IEC 27001 dapat melindungi aspek-aspek dari keamanan informasi yaitu *confidentiality, integrity dan availability*. Penelitian ini menggunakan 7 klausul, yaitu Prosedur Pengelolaan Aset, Organisasi Keamanan Informasi, Manajemen Aset, Keamanan Sumber Daya Manusia, Keamanan Fisik dan Lingkungan, Prosedur Pengendalian Akses, dan Manajemen Keamanan Informasi.

3. HASIL DAN PEMBAHASAN

Sebelum dilakukan audit, maka perlu diketahui bagaimana proses alur penggunakan aplikasi e-cash ini. Pertama adalah silahkan download aplikasi e-cash Mandiri di playstore atau apsstore, jika pengunduhan telah selesai silahkan install sesuai dengan petunjuk yang ada. Setelah proses instalasi selesai maka tahap selanjutnya adalah membuka aplikasi tersebut dan registrasi agar dapat menggunakan aplikasi ini. Registrasi dengan menuliskan nama profil, nama nasabah, nomor identitas, alamat, email, tempat lahir, dan tanggal lahir. Tidak terdapat konfirmasi melalui email atau kebenaran atas nomor identitas yang dituliskan, sehingga rentan sekali terjadi penipuan data. Ketika sudah selesai melakukan registrasi, silahkan untuk membuka aplikasi dan login menggunakan 6-digit password yang sebelumnya sudah dibuat. Pada halaman pertama aplikasi kita dapat menemukan dua menu, yaitu HOME, ISI E-CASH, KIRIM E-CAS, BAYAR TOKO, BAYAR & BELI, TARIK TUNAI, SETOR TUNAI, PENGATURAN, dan LOGOUT. Pada home terdapat menu timeline dan favorit. Sedanglan pdaa menu isi e-cash terdapat tiga menu yaitu isi e-cash melalui bank mandiri, bank lain, dan kartu visa. Selanjutnya menu kirim e-cash, jika ingin melakukan transaksi transfer maka pengguna harus melakukan upgrade aplikasi terlebih dahulu. Lalu menuju ke menu bayar toko, menu ini menyediakan beberapa nominal untuk melakukan pembayaran di gerai toko. Pada menu bayar dan beli terdapat pilihan untuk membeli pulsa, membayar token PLN, dll. Sedangkan pada menu tarik tunai jika ingin melakukan transaksi tarik tunai maka pengguna harus melakukan upgrade aplikasi terlebih dahulu. Selanjutnya menu setor tunai yang digunakan untuk menabung uang yang semula dalam bentuk cash. Dan selanjutnya ada menu pengaturan untuk mengatur profil, mengubah pin, upgrade layanan, dan penjelasan mengenai e-cash. Menu terakhir adalah logout yang akan kita gunakan apabila telah selesai meggunakan aplikasi. Untuk mempermudah pemahaman mengenai alur digunakannya aplikasi e-cash dapat dilihat pada Gambar 2 yang menampilkan alur proses e-cash.

Dalam melakukan audit, hal yang utama harus diperhatikan adalah mengetahui bagaimana proses bisnis bank terebut berjalan. Memulai identifikasi dari hal dasar, seperti mengetahui visi misi bank, profil bank, struktrur organisasi bank, dan tujuan bank. Yang dimaksud bank dalam hal ini adalah Bank Mandiri yang mengeluarkan aplikasi mandiri *e-cash*. Memastikan sebelumnya apakah aplikasi ini sebelumnya sudah dilakukan audit ataukah belum. Jika sudah pernah dilakukan audit, maka perlu dicari informasi bagian apa saja yang sudah sesuai dengan tujuan organisasi dan apa yang belum sesuai. Apabila belum pernah dilakukan audit, maka pengumpulan data harus dilakukan dengan lebih baik dan sedetail mungkin.



Gambar 2. Alur Proses Penggunaan E-cash

Penentuan ruang lingkup didapatkan melakukan wawancara dengan costumer service Bank Mandiri dan pembagian kuisoner. Data merupakan hal yang penting untuk dijadikan acuan proses audit, sehingga data yang diperoleh harus ril dan sesuai fakta yang ada. Hasil yang didapat dari wawancara dan dengan pihak organisasi adalah kurangnya keamanan pada akses aplikasi. Penelitian tidak menggunakan seluruh klausul ISO 27001:2005, tetapi menggunakan 7 klausul. Pemilihan klausul didasarkan pada beberapa permasalahan yang ada pada aplikasi e-cash. Tabel 1 adalah klausul yang digunakan untuk melakukan audit keamanan menggunakan ISO 27001:2005, yaitu:

Tabel 1. Klausul yang Digunakan

KLAUSUL	DESKRIPSI
5	Prosedur Pengelolaan Aset
6	Organisasi Keamanan Informasi
7	Manajemen Aset
8	Keamanan Sumber Daya Manusia
9	Keamanan Fisik dan Lingkungan
11	Prosedur Pengendalian Akses
13	Manajemen Keamanan Informasi

Setelah menentukan klausul yang digunakan, tahap selanjutnya adalah melaksanakan proses audit dan menentukan maturity level. Tabel 2 menjelaskan kerangka kerja perhitungan maturity level pada klausul 13.2 mengenai keamanan fisik dan lingkungan di area yang aman. Sedangkan Tabel 5 mengenai hasil Maturity Level seluruh klausa yang digunakan untuk audit aplikasi e-cash. Tabel 4, Tabel 5, dan Tabel 6 didapatkan berdasarkan hasil wawancara dan pembagian kuisoner dengan customer service Bank Mandiri dan juga pengguna e-cash, dan non pengguna e-cash yang mengalami penipuan. Customer servise yang kami wawancarai ada 3 orang dari Bank Mandiri cabang yang berbeda. Sedangkan untuk pembagian kuisoner kepada pengguna e-cash dan non pengguna, terdapat 15 orang yang kami beri kuisoner untuk dinilai.

Tabel 2. Maturity Level Klausul 13.2 Area yang Aman

13.2	**Manajemen Akses Kontrol**								
No.	**Pernyataan**	**Bobot**	**0**	**1**	**2**	**3**	**4**	**5**	**Nilai**
1.	Tanggung jawab manajemen dan prosedur harus ditetapkan untuk memastikan tanggapan yang cepat, efektif dan sesuai terhadap insiden keamanan informasi.	1					√		4
2.	Harus tersedia mekanisme yang memungkinkan jenis, volume, dan biaya insiden keamanan informasi diukur dan dipantau	1					√		4
3.	Apabila tindak lanjut terhadap orang atau organisasi setelah insiden keamanan informasi melibatkan tindakan hukum (baik perdata atau pidana), bukti harus dikumpulkan, disimpan, dan disajikan sesuai aturan berkenaan dengan bukti yang ditetapkan dalam wilayah hukum yang relevan.	1						√	5
Total Bobot		**3**		**Tingkat Kemampuan**					**4,33**

Keterangan dari Tabel 2, apabila nilai Bobot 1 maka menunjukkan bahwa pernyataan tersebut terpenuhi. Sedangkan angka penilaian 0-5 adalah penilaian dari pernyataan, bagaimana pernyataan tersebut terimplementasi pada objek. Nilai 0 memiliki nilai paling rendah, sedangkan nilai 5 memiliki nilai paling tinggi atau sangat baik. Total bobot didapatkan dari jumlah pernyataan yang memiliki nilai 1. Tingkat kemampuan didapatkan dari seluruh nilai yang dijumlahkan dan dibagi berapa poin pernyataan yang ada.

Langkah selanjutnya adalah menentukan tingkat kematangan (*Maturity Level*). *IT Governance Institute* (ITGI, 2007:17) mendefinisikan model kedewasaan merupakan model yang digunakan untuk mengendalikan proses teknologi informasi yang terdiri dari pengembangan suatu metode penilaian sehingga suatu organisasi dapat mengukur dirinya sendiri. *Maturity Model* itu sendiri memiliki lima tingkat tingkat kematangan proses yang dapat dilihat pada Tabel 3 Maturity Model mengukur tingkat kematangan kedalam skala 0 - 5. Nilai kematangan dikatakan sudah memenuhi standar apabila nilai kematangan proses tersebut minimal 3 (*defined*) [9].

Tabel 3. Tingkat *Maturity Model*

Level	Keterangan
0	*non existence*
1	*initial*
2	*repeatable*
3	*defined*
4	*managed*
5	*optimised*

1. Skala 0 - *Not Existence*
   Perusahaan tidak menyadari pentingnya membuat perencanaan strategis di bidang teknologi informasi. Dalam skala ini penting untuk dilakukan evaluasi pengendalian dan dijadikan sebagai temuan yang penting.
2. Skala 1 - *Initial*
   Perusahaan telah menyadari akan pentingnya pembuatan perencanaan strategis di bidang teknologi informasi. Namun, tidak ada proses yang distandarisasi; perencanaan, perancangan dan manajemen masih belum terorganisir dengan baik. Dalam skala ini keperluan untuk dijadikan temuan tidak diutamakan, karena tingkat kemungkinan terjadinya resiko tidak sebesar skala nol.
3. Skala 2 - *Repeatable*
   Perusahaan telah menetapkan prosedur untuk dipatuhi oleh karyawan, namun belum dikomunikasikan dan belum adanya pemberian latihan formal kepada setiap karyawan mengenai prosedur; dan tanggung jawab diberikan sepenuhnya kepada individu sehingga pemberian kepercayaan sepenuhnya kemungkinan dapat terjadi penyalahgunaan.
4. Skala 3 - *Defined*
   Seluruh proses telah didokumentasikan dan telah dikomunikasikan, serta dilaksanakan berdasarkan metode pengembangan sistem komputerisasi yang baik, namun belum ada proses evaluasi terhadap sistem tersebut, sehingga masih ada kemungkinan terjadinya penyimpangan.
5. Skala 4 - *Managed*
   Proses komputerisasi telah dapat dimonitor dan dievaluasi dengan baik, manajemen proyek pengembangan sistem komputerisasi sudah dijalankan dengan lebih terorganisir.
6. Skala 5 - *Optimised*
   Best Practices (pedoman terbaik) telah diikuti dan diotomatisasi pada sistem berdasarkan proses yang terencana, terorganisir dan menggunakan metodologi yang tepat.

Tabel 4. Hasil Maturity Level Klausul 13

Klausul	Obyektif Kontrol	Kontrol Keamanan	Tingkat Kemampuan	Rata-Rata Obyektif Kontrol
13. Manajemen Keamanan Informasi	13.1 Pelaporan kejadian dan kelemahan keamanan informasi	13.1.1 Pelaporan kejadian keamanan informasi	3,30	3,15
		13.1.2 Pelaporan kelemahan keamanan	3,00	
	13.2 Manajemen insiden keamanan informasi dan perbaikan	13.2.1 Tanggung jawab dan prosedur	3,20	2,98
		13.2.2 Pembelajaran dari insiden keamanan informasi	2,75	
		13.2.3 Pengumpulan bukti	3,00	
***Maturity Level* Klausul 13**				**3,06**

Setelah melakukan perhitungan dan pengolahan data maturity level yang digunakan untuk audit, maka dapat dilihat hasil dari perhitungan seluruh klausul pada Tabel 4.

Tabel 5. Hasil Maturity Level Seluruh Klausul

KLAUSUL	NILAI MATURITY LEVEL
5	2,95
6	3,60
7	2,90
8	2,90
9	3,15
11	3,00
13	3,06
Nilai Seluruh Maturity Level	**3,08**

Dilihat dari Tabel 5 terlihat bahwa aplikasi e-cash memiliki nilai 3.08, sehingga harus ditemukan solusi untuk perbaikan bank kedepannya. Tahap selanjutnya adalah memetakan rekomendasi dan temuan. Temuan adalah fakta yang kami dapatkan selama melakukan audit. Temuan tersebut dapat berupa temuan yang bernilai positif ataupun temuan negative yang perlu diperbaiki. Sedangkan rekomendasi didapatkan dari temuan-temuan negative yang didpatkan selama proses audit. Temuan yang tidak sesuai dengan tujuan organisasi akan didiskusikan oleh pihak auditor dan pihak Bank Mandiri agar mendapatkan jalan keluar dari permasalahan tersebut. Selain itu masukan dari pengguna e-cash dan korban penipuan dari e-cash juga diperlukan untuk menentukan rekomendasi apa yang tepat untuk organisasi.

4. KESIMPULAN

Berikut adalah temuan yang didapatkan setelah melakukan audit aplikasi e-cash menggunakan ISO 27001.

1. Aplikasi e-cash ini sudah berjalan sesuai dengan visi, misi, dan tujuan organisasi, walaupun ada beberapa hal yang masih perlu diperbaiki.
2. Terdapat aturan tentang tanggung jawab atas kewenangan masing-masing pengguna.
3. Terdapat tata cara dan aturan penggunaan aplikasi.
4. Aplikasi e-cash ini tidak dapat di *screenshoot* sehingga lebih aman.
5. Aplikasi harus di upgrade agar dapat melakukan transaksi transfer dan tarik tunai.

Terdapat beberapa temuan yang nantinya harus diperbaiki agar bank tetap berjalan sesuai visi misi. Berikut adalah temuan yang perlu untuk diperbaiki yaitu:

1. Pegawai customer service tidak dapat menemukan data dari pengguna e-cash yang tidak melakukan upgrade aplikasi, sehingga hal ini menyulitkan para korban penipuan untuk mengetahui siapa pelaku penipuan tersebut.
2. Pendaftaran pengguna aplikasi e-cash tidak ada verifikasi melalui email maupun data pendukung lainnya, hanya verifikasi melalui nomor telepon saja.
3. Keamanan aplikasi atas tindak kejahatan dari luar belum dapat dikendalikan.
4. Pihak Bank Mandiri tidak boleh menutup mata akan banyaknya tindak kejahatan dengan menggunakan e-cash.
5. Tidak adanya focus khusus untuk mengembangkan aplikasi lebih mendalam.

5. SARAN

Berikut ini adalah rekomendasi yang disarankan untuk mengatasi temuan-temuan diatas, yaitu:

1. Seharusnya customer service Bank Mandiri sebagai pihak pertama yang ditemui korban penipuan memiliki informasi dan pengetahuan yang cukup mengenai aplikasi e-cash ini, tidak hanya membaca buku panduan yang ada.
2. Pendaftaran aplikasi e-cash ini seharusnya terverifikasi dengan data kependudukan, sehingga ketika kita memasukkan nomor KTP, semua data yang diperlukan sudah sesuai tanpa harus kita mengetikkan ulang nama dan alamat pendaftar.
3. Seharusnya terdapat verifikasi alamat email yang sudah dituliskan pada registrasi.
4. Pihak Bank Mandiri harus lebih banyak memberikan edukasi terhadap masyarakat mengenai penggunaan e-cash yang baik dan benar.
5. Masyarakat harus lebih berhati-hati dalam melakukan proses transaksi melalui uang elektronik.
6. Sebaiknya perlu dikaji ulang aplikasi yang telah dibuat.

DAFTAR PUSTAKA

[1] Ngafifi, M., 2014, Kemajuan Teknologi Dan Pola Hidup Manusia Dalam Perspektif Sosial Budaya, *Jurnal Pembangunan Pendidikan: Fondasi dan Aplikasi*, Vol. 2, No. 1, Hal. 33-47.

[2] Adiyanti, A. I., Pudjihardjo, M., 2015, Pengaruh Pendapatan, Manfaat, Kemudahan Penggunaan, Daya Tarik Promosi, dan Kepercayaan terhadap Minat menggunakan layanan E-money, *Jurnal Ilmu Ekonomi Univeristas Brawijaya*.

[3] Usman, R., 2017, Karakteristik Uang Elektronik Dalam Sistem Pembayaran, *Jurnal Yuridika*, No. 1, Vol. 32, Hal. 134-166

[4] Sihwahjoeni, 2011, Evaluasi Kualitas Fungsi Internal Auditor Dalam Meningkatkan Efektivitas Bank, J*urnal Keuangan dan Perbankan*, No.3, Vol.15, Hal. 466–478.

[5] Priambodo, A., Fauzan, A., 2017, Audit Keamanan Sistem Informasi Manajemen Aset Pada PT. Puri Agung Management Services Menggunakan Metode ISO 27001:2005. *Jurnal Ilmiah Fakultas Teknik LIMIT'S*, No 1, Vol.13

[6] Budiarto, R., 2017, Manajemen Risiko Keamanan Sistem Informasi Menggunakan Metode FMEA Dan ISO 27001 Pada Organisasi XYZ, *CESS (Journal of Computer Engineering System and Science)*, No. 2, Vol. 2, Hal. 48-58

[7] Lenawati, M., Winarno, W. W., Amborowati, A., 2017, Tata Kelola Keamanan Informasi Pada PDAM Menggunakan ISO/IEC 27001:2013 Dan Cobit 5, *Journal Speed – Sentra Penelitian Engineering dan Edukasi*, No. 1, Vol. 9, Hal. 44-49

[8] Afandi, H., Darmawan, A., 2015, Audit Keamanan Informasi Menggunakan ISO 27002 pada Data Center PT.Gigipatra Multimedia, *Jurnal TIM Darmajaya*, No. 02, Vol. 01, Hal. 175-191

[9] Yusup, D., Suyanto, M., Sudarmawan, 2014, Analisis Tata Kelola Teknologi Informasi pada Lembaga Kursus dan Pelatihan, *Citec Journal,* No. 2, Vol. 1. Hal. 102-115

[10] Widayanti, T, 2012, Audit Siskohat Menggunakan Framework Cobit Pada Domain Deliver And Support (DS) di Propinsi Daerah Istimewa Yogyakarta, *Jurnal Ilmiah SISFOTENIKA*, No. 2, Vol. 2, Hal. 31-40