

# ANALISIS RISIKO KUANTITATIF ASET TI PADA BLC E-GOV DINKOMINFO SURABAYA

Mutia Annisa Dewi<sup>1</sup>, Awalludiyah Ambarwati<sup>2</sup>, Cahyo Darujati<sup>3</sup>

<sup>1,2</sup>Program Studi Sistem Informasi, Fakultas Ilmu Komputer, Universitas Narotama

<sup>3</sup>Program Sistem Komputer, Fakultas Ilmu Komputer, Universitas Narotama

E-mail: <sup>1</sup>mannisadewi93@gmail, <sup>2</sup>ambarwati1578@yahoo.com, <sup>3</sup>cahyo.darujati@narotama.ac.id

**Abstrak** – Pemerintahan Kota Surabaya merupakan pemerintahan kota yang kerap menjadi percontohan untuk kota lainnya. Peranan teknologi informasi (TI) memiliki andil besar dalam semakin baiknya layanan pemerintahan kota Surabaya. Beberapa fitur layanan berbasis TI terbaik dari pemerintah kota Surabaya di antaranya adalah sapawarga, Surabaya Single Window (SSW), Broadband Learning Center (BLC) dan e-health. BLC berada di bawah pengelolaan e-Gov Dinas Komunikasi dan Informatika (DINKOMINFO) Surabaya. Salah satu tugas BLC adalah memberikan layanan kepada masyarakat Surabaya berupa fasilitas pembelajaran TI yang dapat dimanfaatkan secara gratis sehingga warga kota Surabaya tidak gagap teknologi. BLC memiliki aset TI yang cukup beragam yang digunakan dalam menjalankan tugasnya. TI selain memberi manfaat juga menghadirkan risiko yang mengancam keberlangsungan layanan BLC. Penelitian ini bertujuan untuk melakukan pengukuran terhadap risiko aset TI pada BLC E-Gov DINKOMINFO Surabaya dengan menggunakan metode Quantitative Risk Analysis (QRA). Aset TI yang digunakan berupa Monitor, CPU, Projector dan Stavolt. Hasil penelitian menunjukkan bahwa aset TI berupa CPU merupakan aset yang memiliki risiko tertinggi dan perlu tindakan pengendalian oleh BLC, berupa maintenance secara periodik untuk meminimalkan risiko yang dapat terjadi.

**Kata Kunci** — aset TI, BLC, QRA

**Abstract** – Surabaya City Government is a city government that often become a model for other cities. Information technology (IT) has a significant role for better service in Surabaya city government. Some of the best features of IT-based services from Surabaya city government include Sapawarga, Surabaya Single Window (SSW), Broadband Learning Center (BLC) and e-health. BLC is managed by e-Gov Dinas Komunikasi dan Informatika (DINKOMINFO) Surabaya. One of BLC tasks is to provide services to Surabaya citizens in the form of IT learning facilities that can be used for free so that Surabaya citizens become technology literate. BLC has various IT assets used in performing its tasks. IT in addition to providing benefits also presents risks that threaten the continuity of BLC services. This study aims to measure the risk of IT assets in BLC E-Gov DINKOMINFO Surabaya by using Quantitative Risk Analysis (QRA) method. IT assets include are Monitor, CPU, Projector and Stabilizer voltage. The results showed that CPU is IT assets that has the highest risk and need control measures by BLC by maintenance periodically to minimize the risk.

**Keywords** — BLC, IT assets, QRA

## 1. PENDAHULUAN

Pemerintah Kota Surabaya berusaha mengelola dan memaksimalkan sumber daya dari setiap bidang yang ada di Surabaya. Salah satunya adalah penggunaan Teknologi Informasi (TI) dalam setiap layanan yang dimiliki oleh Pemerintah Kota Surabaya. Penerapan sistem yang terintegrasi membuat pengambilan keputusan yang dilakukan pemerintah kota Surabaya ataupun lembaga terkait menjadi lebih cepat. Pemanfaatan TI yang dikelola dengan baik dilaksanakan guna menyiapkan Kota Surabaya sebagai *smart city* dan *smart citizen*.

Pemerintahan Kota Surabaya kerap menjadi percontohan untuk kota lainnya. Peranan TI memiliki andil besar dalam semakin baiknya layanan pemerintahan kota Surabaya. Beberapa fitur layanan berbasis TI terbaik dari pemerintah kota Surabaya di antaranya adalah Sapawarga, Surabaya Single Window (SSW), Broadband Learning Center (BLC) dan e-health. BLC merupakan salah satu program yang mendukung tujuan Kota Surabaya untuk menjadi *smart citizen* dan *smart city*. BLC berada di bawah pengelolaan e-Gov Dinas Komunikasi dan Informatika (DINKOMINFO) Surabaya.

DINKOMINFO adalah Dinas yang mempunyai tugas melaksanakan kewenangan

daerah di bidang pengelolaan Teknologi Informasi dan Komunikasi serta melaksanakan tugas pembantuan yang diberikan oleh Pemerintah dan atau Pemerintah Provinsi dimana dalam setiap kegiatannya selalu berhubungan dengan Pembangunan dan Pengembangan Sistem Informasi, Pengembangan dan Pemeliharaan Jaringan Komputer Antar Bidang, Pengelolaan Produksi Informasi dan Publikasi, Pengelolaan dan Pengembangan Komunikasi Publik. BLC merupakan salah satu layanan bagi masyarakat yang memberikan fasilitas pembelajaran TI yang dapat dimanfaatkan masyarakat Surabaya secara gratis, sehingga warga kota Surabaya tidak gagap teknologi. Saat ini BLC tersebar di 44 lokasi dan jumlahnya masih akan terus bertambah. Semakin banyaknya jumlah BLC maka komponen penunjang layanan BLC juga akan semakin banyak. Komponen sebuah BLC terdiri dari ruangan, PC (*Personal Computer*), AC (*Air Conditioner*), proyektor, furnitur dan komponen pendukung lainnya yang didata dalam inventaris BLC.

Inventaris BLC merupakan barang milik Daerah (BMD) yang diperoleh dengan Anggaran Pendapatan dan Belanja Daerah/Negara (APBD/APBN) yang merupakan aset negara dimana pengelolaannya tidak hanya terhadap proses administrasi yang baik, namun juga efektifitas, efisiensi dan menciptakan nilai tambah dalam pengelolaan aset tersebut. Pengelolaan aset yang baik akan memberi informasi yang berkualitas bagi pejabat pemerintah sebagai penentu dan pengambil keputusan [1].

Aset TI yang merupakan inventaris BLC perlu dikelola dengan baik untuk meminimal risiko. Dimana risiko menggambarkan kemungkinan terjadinya insiden yang merusak (bila ada ancaman karena adanya kerentanan), serta kemungkinan kerusakan jika insiden tersebut terjadi [2]. Beberapa risiko yang dihadapi BLC antara lain hilangnya data, rusaknya perangkat keras dan perangkat lunak. Risiko tersebut menimbulkan kerugian baik finansial maupun non finansial bagi BLC.

Penelitian ini bertujuan untuk melakukan analisis risiko kuantitatif aset TI pada BLC E-Gov DINKOMINFO Surabaya. Aset TI yang digunakan berupa Monitor, CPU, proyektor dan Stavolt. Metode analisis risiko yang digunakan adalah *Quantitative*

*Risk Analysis* (QRA) yang menggunakan angka numerik untuk menyatakan dampak dan probabilitas, mengenali pengendalian pengamanan apa dan bagaimana yang seharusnya diterapkan serta besaran biaya untuk menerapkannya [3].

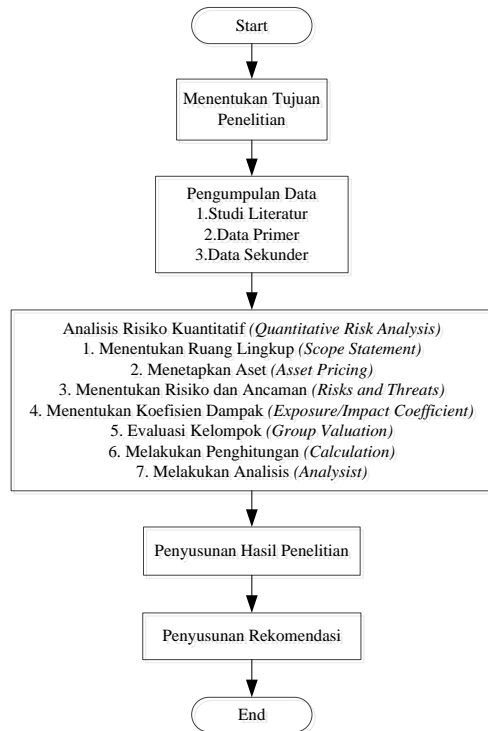
*Risk analysis* merupakan teknik untuk mengidentifikasi dan menilai faktor-faktor yang dapat membahayakan keberhasilan sebuah proyek atau pencapaian suatu tujuan. Teknik ini juga membantu mendefinisikan langkah-langkah preventif untuk mengurangi kemungkinan faktor-faktor tersebut terjadi dan melakukan identifikasi tindakan penanggulangannya [4]. Metode QRA digunakan pada penelitian sebelumnya pada suatu perusahaan dengan empat lokasi gudang. Aset TI yang dikelola perusahaan tersebut mencapai lebih dari 18 milyar rupiah. QRA aset TI pada suatu perusahaan dapat mengidentifikasi faktor risiko yang perlu mendapat skala prioritas dan memberikan rekomendasi pengendalian. Dalam penelitian tersebut kesalahan tidak disengaja (*Accidental Errors*) merupakan potensi nilai kerugian tertinggi secara finansial [5]. Beberapa perbedaan penelitian ini dengan penelitian sebelumnya di antaranya adalah dilakukan pada instansi pemerintahan yang tersebar di 44 lokasi, jumlah aset TI yang dikelola dan jenis aset TI yang digunakan.

## 2. METODE PENELITIAN

Gambar 1 merupakan diagram alur tahapan penelitian yang digunakan pada penelitian ini. Pengumpulan data diperoleh dari studi literatur, data primer dan data sekunder dari BLC e-Gov DINKOMINFO Surabaya. Studi literatur berupa referensi terkait topik penelitian. Data primer diperoleh dari berupa observasi dan wawancara kepada Koordinator BLC. Data sekunder berasal dari BLC e-Gov DINKOMINFO berupa laporan, catatan dan arsip yang telah ada baik yang dipublikasikan maupun yang tidak dipublikasikan secara umum.

Metode QRA meliputi tujuh tahapan [3], [5]. Tahap pertama adalah menentukan ruang lingkup (*scope statement*). Lokasi keberadaan aset TI berupa 44 BLC di seluruh kota Surabaya. Jumlah aset TI yang dianalisa adalah aset TI BLC hingga periode bulan Desember 2017 yang difokuskan pada

aset TI penunjang layanan BLC yang dianalisis. Berdasarkan proses *responsibility of asset*, terdapat empat jenis aset TI pada BLC yang digunakan dengan berbagai merk dan tipe yaitu Monitor, CPU, proyektor dan Stavolt.



Gambar 1. Diagram Alur Tahapan Penelitian

Tahap berikutnya adalah penetapan aset (*asset pricing*). Penetapan aset dilakukan dengan menentukan harga (*price*) sesuai dengan tipe dan model aset TI BLC yang dianalisis. Data *asset pricing* diperoleh dari dokumen aset TI BLC dan wawancara dengan Koordinator BLC.

Selanjutnya, menentukan Risiko (*Risk*) dan Ancaman (*Threats*). Tahap ini bertujuan untuk mengidentifikasi potensi dari sumber ancaman dan melakukan penyusunan suatu daftar yang memaparkan potensi sumber ancaman sehingga dapat diterapkan pada sistem pemeliharaan aset TI yang sedang dievaluasi. Suatu sumber ancaman digambarkan sebagai suatu keadaan atau peristiwa yang memiliki potensi dapat menyebabkan kerusakan pada suatu sistem pemeliharaan aset TI. Kategorisasi *threats* yang digunakan mengadaptasi pada kategori

*threats* yang telah ada pada referensi dan penelitian sebelumnya [3], [4].

Tahap keempat berupa penentuan Koefisien Dampak (*Exposure/Impact coefficient*). Melakukan identifikasi kerentanan aset TI terhadap risiko tertentu atau yang tidak rentan sama sekali terhadap suatu risiko. Hal ini dilakukan dengan membuat klasifikasi dampak pada aset TI berdasarkan tingkat *vulnerability* (kerentanan atau kelemahan) aset TI tersebut. *Vulnerability Analysis/Analisa Kerentanan* aset TI dilakukan untuk mengetahui potensi kehilangan aset, yang disebut *Exposure Factor* (EF), yang merupakan presentase kehilangan akibat ancaman yang terjadi terhadap aset.

Evaluasi Kelompok (*Group Evaluation*) dilakukan untuk mengulas ancaman (*threat*) dan koefisiensi dampak EF (*Exposure Factor*) pada aset TI. Evaluasi Kelompok terdiri dari Koordinator BLC, Koordinator Wilayah dan staf BLC.

Tahap *Calculation Impact Analysis* merupakan perhitungan terhadap dampak dari kejadian gangguan keamanan berupa *Single Loss Expectancy* (SLE) dan *Annualized Loss Expectancy* (ALE). SLE adalah nilai moneter yang akan hilang pada satu kali kejadian gangguan keamanan informasi. Sedangkan ALE merupakan nilai moneter yang akan hilang karena gangguan keamanan terhadap aset, pada jangka waktu satu tahun. Berikut adalah persamaan yang dipergunakan untuk mendapatkan SLE dan ALE [3], [5], [6]:

$$SLE = Asset Value \times EF \dots\dots\dots (1)$$

$$ALE = SLE \times ARO \dots\dots\dots (2)$$

Dimana:

- a. *Asset Value*, merupakan nilai finansial masing-masing aset TI yang telah ditetapkan nilainya dalam tahap *Asset Pricing*.
- b. *EF* (*Exposure Factor*), merupakan presentase kehilangan akibat ancaman yang terjadi terhadap aset. EF memiliki rentang nilai antara 0 hingga 1.
- c. *SLE* (*Single Loss Expectancy*), merupakan nilai kerugian secara finansial pada setiap aset TI yang diakibatkan oleh setiap *threat*.
- d. *ARO* (*Annualized Rate Occurrence*), merupakan nilai prosentase potensi setiap *threat* untuk setiap aset TI dalam 1 tahun.

Tahap terakhir berupa analisis yang dapat menghasilkan dan menentukan aspek mana yang patut mendapatkan pengendalian. Terdapat dua metode analisis yaitu *Analysis Across Asset* dan *Analysis Across Risk* [3], [5]. *Analysis Across Asset* dilakukan dengan cara menjumlahkan nilai dampak masing-masing aset TI dari semua *threat* dari *spreadsheet* pada tahap *Calculation* dan menentukan skala prioritas jenis aset TI yang perlu mendapatkan pengendalian. Sedangkan *Analysis Across Risk* dilakukan dengan cara menjumlahkan nilai dampak masing-masing *threat* untuk semua aset TI dari *spreadsheet* pada tahap *Calculation* dan menentukan skala prioritas jenis *threat*/risiko yang perlu mendapatkan pengendalian.

### 3. HASIL DAN PEMBAHASAN

Penelitian dilakukan pada 44 lokasi BLC di Surabaya yang memiliki aset TI penunjang layanan BLC. Jumlah aset TI yang dianalisa adalah aset TI di BLC hingga periode bulan Desember 2017, terdiri dari empat jenis aset TI dengan berbagai merk dan tipe berupa Monitor, CPU, proyektor dan Stavolt. Adanya perbedaan tipe, merk maupun harga tiap aset TI dipengaruhi oleh tahun pengadaan dan spesifikasi aset tersebut.

Tabel 1 merupakan jenis dan penetapan harga aset TI di BLC. Nilai aset TI secara keseluruhan mencapai Rp 1.883.400.000. Aset TI terbanyak adalah CPU berjumlah 412 unit juga merupakan aset dengan nilai tertinggi yaitu Rp 1.277.200.000. Proyektor merupakan jenis aset dengan jumlah terendah yaitu 43 unit. Sedangkan nilai aset terendah adalah Stavolt sebesar Rp 71.500.000.

Tabel 1. Jenis dan Penetapan harga Aset TI

Jenis Aset TI	Jumlah Aset TI (Unit)	Total Harga
CPU	412	Rp 1.277.200.000
Monitor	409	Rp 347.650.000
Proyektor	43	Rp 187.050.000
Stavolt	220	Rp 71.500.000
Jumlah		Rp 1.883.400.000

Tabel 2. Ancaman dalam satu tahun

No	Ancaman	ARO
1	Kehilangan Daya	2.00
2	Kehilangan komunikasi	2.00
3	<i>Data Integrity Loss</i>	0.00
4	<i>Accidental Errors</i>	0.72
5	Virus Komputer	0.68
6	Penyalahgunaan hak akses oleh pegawai	0.40
7	Bencana Alam	0.29
8	Percobaan pengaksesan system oleh pengguna tidak dikenal	0.27
9	Pencurian / Hilangnya aset TI	0.24
10	<i>Destruction of data</i> / Kerusakan data	0.17
11	Pihak luar yang berhasil dalam mengakses perangkat PC	0.08
12	Penghentian proses kerja suatu perangkat tanpa sebab bencana	0.06
13	Kebakaran	0.01

Tabel 3. Koefisien Dampak Aset TI

EF	Deskripsi
0	Aset tersebut tahan dan tidak ada kerusakan yang dihasilkan oleh ancaman terhadap aset tersebut.
0.3	Saat terjadi ancaman biasanya tidak terjadi kerusakan terhadap aset namun ada kemungkinan kerusakan tersebut menghasilkan penggantian total.
0.5	Saat terjadi ancaman tidak ada kerusakan atau tidak membutuhkan penggantian total
0.7	Setelah ancaman dieksekusi, aset terdampak biasanya akan membutuhkan penggantian, dalam beberapa kasus mungkin bisa menghindari kerusakan total ataupun secara keseluruhan.
1	Ketika ancaman ini diketahui, penggantian total adalah satu-satunya hal bisa dilakukan.

Tabel 2 adalah nilai ARO pada aset TI yang diperoleh dari prosentase potensi risiko pada aset TI di BLC dan merupakan ancaman yang dapat menyebabkan kerugian, baik kerugian ekonomis maupun kerugian non ekonomis dalam kurun waktu 1 tahun. Tabel 3 merupakan standar yang menjadi acuan nilai koefisien dampak pada aset TI dengan nilai 0 hingga 1 [3]. Tabel 4 menyajikan nilai EF untuk empat jenis aset TI di BLC yang diperoleh dari *Group Evaluation*, dimana

Tabel 4. Koefisien dampak jenis aset TI

No	Ancaman	EF		
		CPU	Monitor & Proyektor	Stavolt
1	Kehilangan Daya	0.3	0.3	0.3
2	Kehilangan komunikasi	0.3	0.0	0.0
3	<i>Data Integrity Loss</i>	0.0	0.0	0.0
4	<i>Accidental Errors</i>	0.5	0.5	0.5
5	Virus Komputer	0.5	0.0	0.0
6	Penyalahgunaan hak akses oleh pegawai	0.0	0.0	0.0
7	Bencana Alam	0.3	0.5	0.3
8	Percobaan pengaksesan sistem oleh pengguna tidak dikenal	0.3	0.0	0.0
9	Pencurian / Hilangnya aset TI	1.0	1.0	0.5
10	<i>Destruction of data/Kerusakan data</i>	0.0	0.0	0.0
11	Pihak luar yang berhasil dalam mengakses perangkat PC	0.7	0.0	0.0
12	Penghentian proses kerja suatu perangkat tanpa sebab bencana	0.3	0.3	0.00
13	Kebakaran	0.3	0.3	1.00

*Calculation Impact Analysis* dilakukan untuk mengetahui nilai SLE dan ALE. Data pada Tabel 1 dan Tabel 4 digunakan untuk menghitung SLE sesuai Persamaan 1. Hasil perhitungan nilai SLE empat jenis aset TI di BLC dikalikan data pada Tabel 2 digunakan untuk menghitung nilai ALE sesuai Persamaan 2.

Tahap terakhir berupa *Analysis Across Asset* dan *Analysis Across Risk*. Tabel 5 merupakan nilai *Across Asset* yang telah diurutkan berdasarkan nilai tertinggi hingga terendah aset TI. Nilai *Across Asset* tertinggi adalah aset TI berupa CPU sebesar Rp 5,747,400,000 dan nilai terendah adalah stavolt senilai Rp 185,900,000. Sedangkan total nilai *Across Asset* TI pada 44 lokasi BLC adalah Rp 7,483,930,000.

Tabel 5. Ranking dan Nilai *Across Asset*

Jenis Aset TI	Nilai <i>Across Asset</i>
CPU	Rp 5,747,400,000
Monitor	Rp 1,008,185,000
Proyektor	Rp 542,445,000
Stavolt	Rp 185,900,000
Total <i>Across Asset</i>	Rp 7,483,930,000

Tabel 6. Rangkaing dan Nilai *Across Risk*

No	Ancaman	Nilai <i>Across Risk</i>
1.	Hilangnya Aset	Rp 1,847,650,000
2.	Kesalahan Tidak Sengaja	Rp 941,700,000
3.	Pihak luar yang berhasil mengakses Perangkat PC	Rp 894,040,000
4.	Bencana Alam	Rp 671,960,000
5.	Virus Komputer	Rp 638,600,000
6.	Kebakaran	Rp 615,070,000
7.	Kehilangan Daya	Rp 565,020,000
8.	Penghentian Proses Kerja Tanpa Sebab	Rp 543,570,000
9.	Kehilangan Komunikasi	Rp 383,160,000
10.	Percobaan Pengaksesan System oleh pengguna tidak dikenal	Rp 383,160,000
	Total Nilai <i>Across Risk</i>	Rp 7,483,930,000

Rangkaing nilai *Across Risk* untuk empat jenis aset TI di BLC disajikan pada Tabel 6. Nilai *Across Risk* tertinggi adalah bila terjadi hilangnya aset sebesar Rp 1,847,650,000. Total nilai *Across Asset* TI dan nilai *Across Risk* adalah sama yaitu lebih dari tujuh milyar rupiah, tepatnya Rp 7,483,930,000. Sedangkan untuk ancaman berupa *data integrity loss*, penyalahgunaan hak akses oleh pegawai dan *destruction of data/kerusakan data* memiliki nilai *Across Risk* nol rupiah. Hal ini berarti jika ketiga ancaman tersebut terjadi maka tidak menimbulkan kerugian secara finansial.

Hasil analisis menghasilkan beberapa rekomendasi yang diberikan kepada pengambil keputusan BLC E-Gov DINKOMINFO untuk melakukan pengendalian risiko. CPU merupakan

*hardware* terpenting untuk menunjang layanan BLC dan merupakan aset TI dengan nilai tertinggi. Bila terjadi *threat* pada CPU maka akan mengganggu layanan BLC, layanan BLC tidak akan bekerja dengan maksimal atau bahkan dapat melumpuhkan layanan BLC. CPU pada setiap BLC merupakan prioritas utama dalam pengendalian. *Maintenance* secara periodik minimal sekali dalam setiap bulan hendaknya diberikan untuk keempat jenis aset TI. Namun untuk CPU frekuensi *maintenance* ditingkatkan menjadi dua kali dalam setiap bulannya.

Ancaman terbesar pada BLC adalah hilangnya aset TI yang menimbulkan kerugian finansial terbesar. Pengamanan seluruh aset TI perlu ditingkatkan, utamanya CPU. Beberapa rekomendasi yang diberikan di antaranya, menempatkan aset TI pada tempat yang aman dan memberi pengamanan tambahan jika diperlukan. Pembuatan dan penerapan SOP (*Standard Operating Procedure*) terkait penggunaan aset TI. Seluruh pemindahan ataupun pemindahan aset TI harus dilakukan sesuai prosedur yang berlaku secara tertulis maupun elektronik dan ditandatangani oleh pejabat yang berwenang. Pemasangan CCTV pada lokasi aset TI berada.

#### 4. SIMPULAN

BLC E-Gov DINKOMINFO Surabaya memiliki 44 lokasi di Surabaya dan mengelolah aset TI sebesar Rp 1.883.400.000 berupa Monitor, CPU, Projector dan Stavolt. Hasil penelitian menggunakan QRA menunjukkan bahwa CPU merupakan aset TI yang memiliki risiko tertinggi secara finansial dan perlu tindakan pengendalian oleh BLC, berupa pengamanan dan *maintenance* secara periodik. Koordinator BLC perlu melakukan pencatatan data mengenai risiko yang terjadi setiap tahunnya agar dapat digunakan oleh pihak E-gov dalam membuat keputusan dan rencana strategis DINKOMINFO dalam bidang TI. Selain itu Koordinator BLC hendaknya melakukan peningkatan pengendalian untuk meminimalkan risiko TI dengan membentuk suatu satuan kerja yang mengelolah risiko TI.

#### 5. SARAN

Saran untuk penelitian selanjutnya antara lain:

- a. Membangun sistem informasi yang mempermudah pencatatan dan mengelolah aset TI, khususnya pada BLC.
- b. Melakukan pengukuran risiko TI untuk keseluruhan aset TI pada E-Gov DINKOMINFO Pemerintahan Kota Surabaya secara berkala.

#### DAFTAR PUSTAKA

- [1] Republik Indonesia, *UNDANG-UNDANG NOMOR 15 TAHUN 2004 Tentang PEMERIKSAAN PENGELOLAAN DAN TANGGUNG JAWAB KEUANGAN NEGARA*. Jakarta: SEKRETARIS NEGARA REPUBLIK INDONESIA, 2004.
- [2] A. Jones and D. Ashenden, *Risk management for computer security: Protecting your network and information assets*, 1st Edition. Elsevier Butterworth-Heinemann, 2005.
- [3] J. W. Meritt, "A Method for Quantative Risk Analysis," in *Proceedings of the 22nd National Information Systems Security Conference*, 1999.
- [4] T. R. Peltier, *Information Security Risk Analysis*, Second Edition. Boca Raton: CRC Press Taylor & Francis Group, 2005.
- [5] A. Yulianto, A. Ambarwati, and C. Darujati, "ANALISIS MANAJEMEN RISIKO TI PEMELIHARAAN ASET MENGGUNAKAN QUANTITATIVE RISK ANALYSIS (QRA) PADA PT. HMS," in *Prosiding Seminar Nasional Teknologi dan Rekayasa Informasi (SENTRIN) 2016*, 2016, pp. 45–51.
- [6] D. Tan, "Quantitative Risk Analysis Step-By-Step," SANS Institute, 2003.