PENILAIAN RISIKO PADA IMPLEMENTASI SISTEM MANAJEMEN INFORMASI DAERAH (SIMDA)

Dahlia Br Ginting

Sekolah Tinggi Manajemen Informatika dan Komputer LIKMI
Jl. Ir. H. Juanda 96 Bandung 40132

e-mail:dahliaginting@yahoo.co.id

ABSTRAK

E-government didefinisikan sebagai upaya pemanfaatan dan pendayagunaan telematika untuk meningkatkan efisiensi dan *cost-effective* pemerintahan, memberikan berbagai jasa pelayanan kepada masyarakat secara lebih baik, menyediakan akses informasi kepada publik secara lebih luas, dan menjadikan penyelenggaraan pemerintahan lebih bertanggung jawab (*accountable)* serta transparan kepada masyarakat. Proses penilaian risiko (*risk assessment*) Sistem Informasi Manajemen Daerah (SIMDA) dilakukan dengan menggunakan metode manajemen risiko (*risk management* yang merupakan proses menyeluruh yang dilengkapi dengan alat, teknik, dan sains yang diperlukan untuk mengenali, mengukur, dan mengelola risiko secara lebih transparan. Berdasarkan konsep dasar di atas salah satu paradigma penting yang ditawarkan oleh manajemen risiko (*risk management)* di dalam mengelola risiko adalah bahwa risiko dapat didekati dengan menggunakan suatu kerangka pikir yang sangat rasional. Hal ini dimungkinkan berkat berkembangnya teori probabilitas dan statistik yang memungkinkan dimilikinya alat untuk memilah, meng-*quantify* dan mengukur risiko. Asumsi yang mendasari hal ini adalah bahwa statistik mengandung di dalamnya "ingatan numerik" (*numerical memory*). Bertitik tolak dari hal itu maka dapatlah dibaca suatu alur tertentu yang memungkinkan untuk memproyeksikan kemungkinan-kemungkinan yang akan dihadapi di masa mendatang.

Penilaian risiko (*risk assessment*) sistem informasi merupakan proses awal dari manajemen risiko (*risk management*) Sistem Informasi Manajemen Daerah (SIMDA).

Kata-kata kunci: *E-government, risk assessment,* r*isk management, risk determination.*

1. PENDAHULUAN

E-government didefinisikan sebagai upaya pemanfaatan dan pendayagunaan telematika untuk meningkatkan efisiensi dan *cost-effective* pemerintahan, memberikan berbagai jasa pelayanan kepada masyarakat secara lebih baik, menyediakan akses informasi kepada publik secara lebih luas, dan menjadikan penyelenggaraan pemerintahan lebih bertanggung jawab (*accountable)* serta transparan kepada masyarakat.

1.1 TUJUAN E-GOVERNMENT

E-government yang diimplementasikan dalam Sistem Informasi Manajemen Daerah (SIMDA) mempunyai tujuan sebagai berikut:

a. Memberikan kebutuhan informasi secara cepat, tepat, lengkap, akurat, dan terpadu untuk menunjang proses administrasi pemerintahan.
b. Memberikan pelayanan tanpa adanya intervensi pegawai institusi publik dan sistem antrian panjang.
c. Mendukung tata kelola yang baik (*good governance*).
d. Memperluas partisipasi publik dimana masyarakat dapat terlibat aktif dalam pengambilan keputusan pemerintah.
e. Memperbaiki produktivitas dan efisiensi birokrasi serta meningkatkan pertumbuhan ekonomi.
f. Masyarakat sebagai pengguna pelayanan publik dapat menikmati pelayanan yang lebih baik karena pelayanan dapat dilakukan dengan lebih cepat dan mudah tanpa dibatasi oleh dimensi ruang dan waktu.
g. Memperbaiki produktivitas dan efisiensi birokrasi serta meningkatkan pertumbuhan ekonomi.

Secara umum tahapan pelaksanaan *e-government* yang biasanya dipilih adalah:

1. Membangun sistem *e-mail* dan jaringan.
2. Meningkatkan kemampuan organisasi dan publik dalam mengakses informasi.
3. Menciptakan komunikasi dua arah antar pemerintah dan masyarakat.
4. Memulai pertukaran *value* antar pemerintah dan masyarakat.
5. Menyiapkan portal yang informatif.

1.2 BATASAN MASALAH

Penilaian risiko (*risk assessment*) di sini dibatasi hanya pada proses pengembangan dan penerapan Sistem Informasi Manajemen Daerah (SIMDA) pada beberapa daerah di seluruh Indonesia.

2. PEMBAHASAN

2.1 PENDEKATAN PENILAIAN RISIKO

a. Pihak yang melakukan proses manajemen risiko (*risk management*)

Proses manajemen risiko (*risk management*) Sistem Informasi Manajemen Daerah (SIMDA) dilakukan dalam bentuk tim yang terdiri dari beberapa anggota yang memiliki keahlian masing-masing.

b. Teknik untuk memperoleh Informasi

Proses penilaian risiko (*risk assessment*) Sistem Informasi Manajemen Daerah (SIMDA) dilakukan dengan menggunakan metode manajemen risiko (*risk management*) dimana merupakan proses menyeluruh yang dilengkapi dengan alat, teknik, dan sains yang diperlukan untuk mengenali, mengukur, dan mengelola risiko secara lebih transparan.

Berdasarkan konsep dasar di atas salah satu paradigma penting yang ditawarkan oleh manajemen risiko (*risk management*) di dalam mengelola risiko adalah bahwa risiko dapat didekati dengan menggunakan suatu kerangka pikir yang sangat rasional. Hal ini dimungkinkan berkat berkembangnya teori probabilitas dan statistik yang memungkinkan dimilikinya suatu alat untuk memilah, meng-*quantify* dan mengukur risiko. Asumsi yang mendasari hal ini adalah bahwa statistik mengandung di dalamnya “ingatan numerik” (*numerical memory*) yang bertitik tolak dari hal itu maka dapat dibaca suatu alur tertentu yang memungkinkan untuk memproyeksikan kemungkinan-kemungkinan yang akan dihadapi di masa mendatang.

c. Pengembangan dan deskripsi dari skala risiko

Proses manajemen risiko (*risk management*) berikut ini menggunakan matriks risiko 5x5.

2.2 PENILAIAN RISIKO

Langkah 1 Karakterisasi Sistem (*System Characterization*)

Masukan:

1. Perangkat Lunak (*Software*)

   Aplikasi sistem informasi yang mampu menunjang proses administrasi pemerintahan, pelayanan masyarakat, memfasilitasi partisipasi dan dialog publik.
2. Perangkat Keras (*Hardware*)

   Kebutuhan *server* seperti HP Proliant Server dengan spesifikasi yang cukup tinggi untuk melayani administrasi kepemerintahan secara elektronik melalui jaringan internet.
3. Sistem Antarmuka (*Interface System*)

   Merancang tampilan yang *user-friendly* artinya mudah untuk dipelajari dan mudah untuk digunakan.
4. Data (*Data*)

   Data masyarakat yang diolah menjadi informasi. Semua data tersebut disimpan dalam satu basis data yang cukup besar dengan sistem DBMS.
5. Informasi (*Information*)

   Diperoleh dari data yang diinput dan diproses. Merupakan hal yang krusial dalam pengambilan keputusan.
6. Misi Sistem (*System Mission*)

   Memberikan kemudahan dalam melakukan proses administrasi kepemerintahan.

Keluaran:

1. Batasan Sistem (*System Boundary*)

   Dibatasi hanya pada pelayanan administrasi kepemerintahan dalam suatu Pemerintahan Daerah.
2. Fungsi-fungsi Sistem (*System functions*)

   Dapat melaksanakan fungsi administrasi di pemerintahan seperti fungsi pembuatan KTP, fungsi pembuatan passport, fungsi pembuatan akta kelahiran, fungsi pembayaran pajak, dan lain-lain.
3. Kekritisan Sistem dan Data (*System and Data Criticality*)

   Yang harus diamankan adalah data masyarakat atau penduduk.

4. Sensitivitas Sistem dan Data (*System and Data Sensitivity*)
   Data harus dijaga integritasnya, kerahasiaannya, keasliannya.

Langkah 2 Identifikasi Ancaman (*Threat Identification*)

Ancaman Operasional

1. Lingkungan Operasi dan Fasilitas
   Kehilangan atau kerusakan kemampuan operasional yang diakibatkan oleh masalah-masalah yang muncul di tempat kerja, fasilitas, layanan atau peralatan.
2. Kesehatan dan Keselamatan
   Ancaman atas kesehatan dan keselamatan staf, konsumen, dan anggota publik.
3. Keamanan Informasi
   Terbukanya atau termodifikasinya informasi rahasia, atau kehilangan ketersediaan informasi, atau penggunaan informasi tidak pada tempatnya.
4. Kerangka Kerja (*Framework*) Kendali
   Kekurangan dalam rancangan atau kinerja dari infrastruktur manajemen risiko yang ada.
5. Hukum dan Peraturan Pemerintah
   Kegagalan untuk memenuhi persyaratan hukum, standar pelaporan dan perpajakan, kontrak atau kegagalan kontrak untuk melindungi harta (*asset*) usaha.
6. Reputasi
   Efek negatif dari opini publik, opini konsumen, reputasi pasar dan kerusakan atas nama baik yang diakibatkan oleh kegagalan mengelola relasi publik.
7. Strategik
   Kegagalan untuk memenuhi sasaran strategik.

Ancaman Operasional Keterangan

1. Pemrosesan dan perilaku

   Masalah yang timbul dalam layanan yang diakibatkan oleh kegagalan kendali internal, sistem informasi, atau kelemahan dalam prosedur operasional.
2. Teknologi

   Kegagalan merencanakan, mengelola, dan memonitor kinerja sub sistem yang berkaitan dengan teknologi, layanan publik.
3. Manajemen proyek

   Kegagalan merencanakan dan mengelola sumber daya yang diperlukan untuk mencapai sasaran taktis, kegagalan teknis untuk mengelola aspek integrasi dengan bagian-bagian yang sudah ada beserta dampaknya.
4. Kriminal dan tindakan asusila

   Kehilangan yang diakibatkan oleh *fraud, hacker, cracker, computer criminal, terrorist*, pencurian, keteledoran yang disengaja, ketidakdisiplinan, sabotase.
5. Sumber daya manusia

   Kegagalan dalam merekrut, mengembangkan atau melatih karyawan dengan keterampilan dan pengetahuan yang tepat atau kegagalan mengelola relasi dengan karyawan.
6. Informasi manajemen

   Kerusakan yang diakibatkan oleh praktek yang tidak etis, menyangkut diskriminasi.
7. Kultural

   Kegagalan untuk menangani aspek kultural yang mempengaruhi karyawan, publik, meliputi bahasa, agama, moralitas, dan lain sebagainya.
8. Cuaca dan iklim

   Kehilangan atau kerusakan yang diakibatkan oleh kondisi cuaca yang buruk, seperti angin ribut, banjir, suhu panas, kekeringan, polusi, mati listrik dan lain sebagainya.

Langkah 3 Identifikasi Penyerangan (*Vulnerability Identification*)

Dapat terjadi kecurangan (*fraud*) yang dilakukan oleh pemakai (*user*).

1. Dapat terjadi kesalahan (*error*), misalnya kesalahan pada saat pemindahan yang dilakukan oleh operator dari bentuk kertas atau formulir ke bentuk *entry digital*, kesalahan dalam jumlah pembayaran, terjadi transaksi ganda, pemasukan data yang tidak lengkap, kesalahan input, kesalahan proses, kesalahan output, dan lain-lain.
2. Terjadinya kelambatan (*delay*), misalnya keterlambatan dalam pembayaran atau penerimaan uang, keterlambatan dalam pengiriman hasil atau keluaran yang lebih lanjut akan terkait dengan *contractual deadline* yang dapat menimbulkan denda atau penalti.
3. Terjadinya interupsi layanan (*sistem crash*), misalnya terjadi kegagalan dalam memenuhi permintaan layanan yang diminta oleh publik.
4. Terjadinya publikasi informasi yang bersifat rahasia, seperti informasi mengenai keunggulan kompetitf, informasi mengenai keuangan, kekayaan intelektual, data detil penduduk.
5. Pencurian kekayaan intelektual seperti *software code*, dan lain-lain.
6. Permasalahan mengenai konfidensialitas yaitu munculnya *hacker* yang menggunakan berbagai cara, tidak terbatas pada kriptografi, *bug* pada perangkat lunak, pemakai (*user*) yang lengah, manajer yang tidak teliti, terkena serangan virus, dan lain sebagainya.

Langkah 4 Analisis Pengendalian (*Control Analysis*)

Keamanan *Logical*

1. Penamaan unit untuk setiap entitas

   Caranya menetapkan standar penamaan, prosedur penamaan, dan sistem direktori.
2. Registrasi entitas

   Caranya menetapkan kebijakan registrasi, sistem otoritas registrasi, prosedur registrasi.
3. Sertifikasi kredensial entitas

   Caranya dengan menetapkan kebijakan sertifikasi, sistem otoritas sertifikasi, prosedur sertifikasi, standar sintaks atau penulisan sertifikat,

mekanisme publikasi sertifikat, *Certificate Revocation List* (CRL), Pengelolaan dan Publikasi CRL.

4. Otentikasi entitas

   Caranya menetapkan prosedur *login*, *user password*, otentikasi pengguna *client*, protokol pertukaran otentikasi, sistem *server* otentikasi, sistem direktori.

5. Otentikasi sesi

   Caranya menentukan otentikasi dua arah dan tiga arah antara *client* dengan *server*.

6. Otentikasi data tersimpan

   Caranya melakukan *checksum* integritas pesan, tanda tangan *digital*, *hashing*.

7. Otentikasi asal atau pengirim pesan

   Caranya identitas sumber pesan, diproteksi oleh *checksum* integritas pesan, tanda tangan *digital*.

8. Otentikasi penerimaan pesan dan bukti pengiriman tak terbantah

   Caranya ACK/NACK ujung ke ujung, ditandatangani secara *digital*, diberlakukannya *time-out*.

9. Otorisasi

   Caranya menetapkan otorisasi sertifikat.

10. Pengendalian akses lojik (*Logical access control*)

    Caranya adanya agen kendali akses lojik, *Access Control List* (ACL) peran lokal, *Central Access Manager* (CAM), ACL berperan sebagai CAM, agen kendali akses aplikasi pusat.

11. *Audit trails*

    Caranya adanya *tools* untuk mem-*browse event log*, *tools* untuk analisis *event log*, *tools* untuk pelaporan.

12. Pemulihan Bencana (*Disaster recovery*)

    Caranya dengan melakukan *backup* data, *backup* perangkat lunak (*software*), prosedur restorasi data, penyimpanan *backup off-site*, pengindeksan, pelabelan, penyimpanan, dan pengaksesan *backup*, redundansi perangkat keras, redundansi jalur komunikasi, rencana pemulihan, prosedur pemulihan.

13. Konfidensialitas isi pesan

    Caranya dengan enkripsi isi pesan, pengelolaan kunci enkripsi.

14. Jaminan integritas perangkat lunak

    Caranya adalah dengan adanya *tools* anti virus, pengendalian terhadap siklus hidup pengembangan sistem.

15. Manajemen keamanan

    Caranya dengan dibentuknya sub sistem manajemen keamanan, pengendalian akses pada semua agen dan sub sistem, mekanisme otentikasi operator, *operator activity logs*, *managemant event logs*, monitoring sistem secara *real time*, alarm.

16. Monitoring keamanan

    Cara*user activity logs*, *application event logs*, *operator activity logs*, *management event logs*, *browsing* dan analisis terhadap *event logs*, pelaporan, monitoring sistem secara *real-time*, alarm.

17. Pengukuran dan metrik keamanan

    Caranya dengan melakukan pengujian secara statistik, mekanisme uji kriptografi.

18. Tidak ada penyangkalan (*Non repudiation*)

    Caranya dengan menerapkan tanda tangan *digital*, *transaction log.*

19. Keamanan fisik

    Caranya dengan mengunci ruang *server*, proteksi terhadap sistem perkabelan, prosedur otorisasi, *badge* identitas dan prosedur pengunjung atau tamu.

20. Keamanan lingkungan

    Caranya dengan menyediakan alat pemadam kebakaran, pengendalian suhu dan kelembaban ruangan, mekanisme proteksi daya listrik, antisipasi banjir.

21. Antarmuka pemakai (*User interface*)

    Caranya dengan layar login GUI (*Graphical User Interface*), layar pesan keamanan GUI.

Step 5 Likelihood Determination

Untuk ancaman-ancaman di atas, tingkatannya adalah **HIGH**, karena jika sistem pengoperasian terkena salah satu saja dari ancaman yang ada, maka sistem tidak dapat melayani mayarakat atau permintaan publik secara maksimal atau bahkan hal yang paling buruk dapat terjadi yaitu sistem tidak dapat dioperasikan sama sekali.

Step 6 Impact Analysis

Dapat menyebabkan terjadinya kesalahan dalam perkiraan, maksudnya adalah kenyataan yang ada jauh melebihi perkiraan pada perhitungan yang dapat mengakibatkan perubahan jadwal pengerjaan dan biaya operasional.

1. Kesalahan dalam perancangan skala basis data.
2. Kehilangan integritas, *availability*, dan kerahasiaan data.

Step 7 Risk Determination

KELOMPOK/DAFTAR RISIKO
A. RISIKO ESTIMASI
1. Kesalahan perkiraan → terjadi jika perkiraan pada kenyatan yang ada jauh melebihi perkiraan pada perhitungan.
2. Kesalahan perancangan skala basis data → terjadi karena skala basis data yang telah dirancang ternyata tidak sesuai pada proses pengembangan perangkat lunak tersebut yang dapat berakibat berubahnya waktu penyelesaian pekerjaan.
B. RISIKO PENGARUH ORGANISASI
1. Dokumentasi untuk pemerintah dianggap kurang baik oleh masyarakat → terjadi apabila dokumentasi yang diberikan kepada masyarakat tidak seperti yang diharapkan, sehingga masyarakat tidak puas.
C. RISIKO YANG BERHUBUNGAN DENGAN MASYARAKAT
1. Masyarakat belum dapat memastikan apa yang dibutuhkannya → terjadi apabila masyarakat tidak tahu pasti apa yang dibutuhkannya dan belum siap menerima perkembangan teknologi baru.
2. Dinas-dinas terkait kurang berkomunikasi dengan pengembang untuk

saling memberi informasi → terjadi karena kurangnya komunikasi.
3. Masyarakat tidak mengerti proses pengembangan basis data → terjadi karena salah persepsi masyarakat.
D. RISIKO PROSES
1. Tidak semua staf bersedia untuk mengikuti proses yang telah ditentukan → staf tidak mampu mengikuti prosedur yang telah ditentukan.
2. Para staf memiliki jadwal yang berbeda sehingga kurang koordinasi.
3. Metode pengetesan ternyata tidak dapat diterapkan pada perangkat lunak tersebut.
E. RISIKO TEKNOLOGI
1. Tidak semua staf menguasai atau mengenal *tools* yang akan digunakan → Kemampuan staf berbeda.
2. Proyek membutuhkan inovasi oleh pengembang
F. RISIKO PERALATAN PENGEMBANGAN
1. Perangkat lunak tidak tersedia
2. Tidak tersedianya referensi yang cukup untuk peralatan yang digunakan
G. RISIKO YANG BERHUBUNGAN DENGAN SDM
1. Tidak tersedianya staf yang kompeten di bidang tersebut
H. RISIKO KOMPONEN DAN PENGENDALI
1. Performa sistem tidak seperti yang diharapkan
2. Harga perangkat keras dan perangkat lunak di luar perkiraan
3. Perangkat lunak tidak bisa dikoreksi atau diubah

Bahaya yang Berisiko Tinggi

Didasarkan pada dua penilaian ancaman yaitu:

- Probabilitas atau kemungkinan terjadinya peristiwa dan

- Dampak, kerugian atau kerusakan yang ditimbulkannya.

Hasil penelitian kemudian di plot ke dalam matriks pemilihan risiko.

Penilaian bahaya

No	Jenis Ancaman Bahaya	Probabilitas	Dampak
1	Risiko estimasi	3	3
2	Risiko pengaruh organisasi (internal)	2	2
3	Risiko yang berhubungan dengan masyarakat (eksternal)	3	2
4	Risiko proses	2	2
5	Risiko teknologi	2	2
6	Risiko peralatan dan pengembangan	3	2
7	Risiko yang berhubungan dengan jumlah staf dan pengalaman	2	2
8	Risiko komponen dan pengendali	2	2

P = Probabilitas (skala 1 - 5) , D = Dampak (skala 1 - 5)

Probabilitas Kejadian

Skala Probabilitas:

5 - Sangat Pasti (hampir dipastikan 100% terjadi).

4 - Hampir Pasti (75 – 100% terjadi)

3 - Mungkin (50 - 75 % terjadi)

2 - Kemungkinan Kecil (20 - 50 % terjadi)

1 - Tidak Pasti (1 – 20 % terjadi)

Dampak Kejadian

Dampak Kerugian yang ditimbulkan:

5 - Sangat Parah (hampir dipastikan SIMDA tidak dapat dilaksanakan 100%)

4 - Parah (SIMDA dapat terlaksana 50 - 75%)

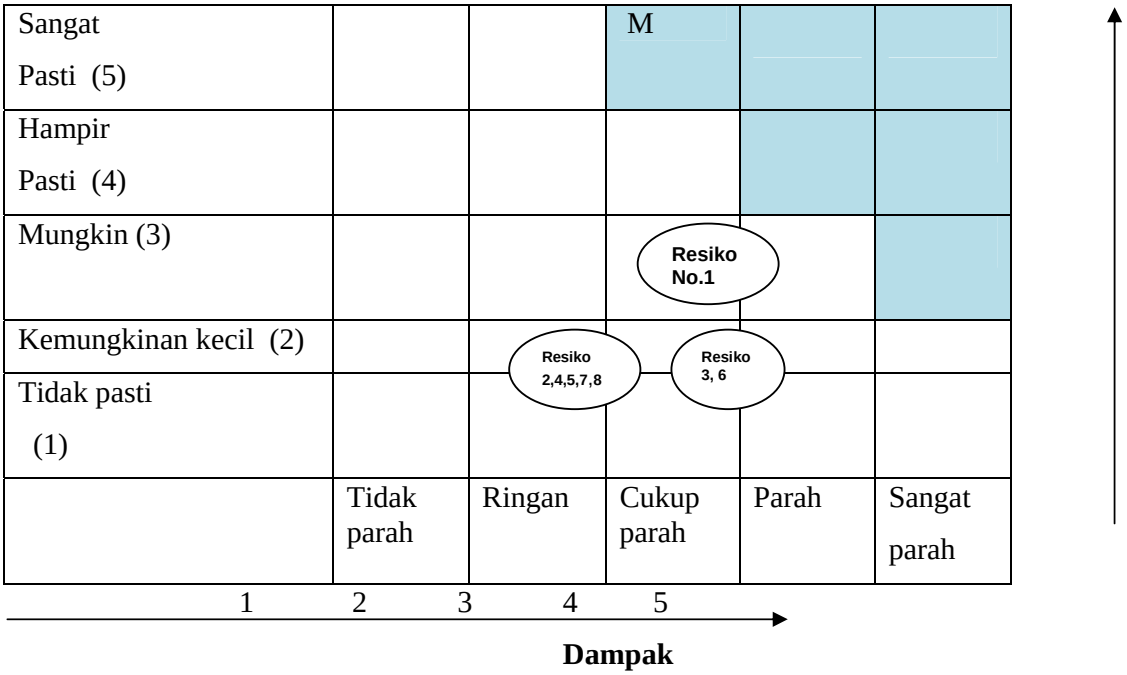
3 - Cukup Parah (SIMDA dapat terlaksana 10 - 50 %)

2 - Ringan (SIMDA dapat terlaksana kurang 10%)

1 - Tidak Parah (dampak terkecil)

MATRIKS RISIKO 5 x 5

Matriks resiko Probabilitas



Step 8 : Control Recommendation

KELOMPOK RESIKO	SOLUSI YANG DIREKOMENDASIKAN
A. RESIKO ESTIMASI	
Kesalahan perkiraan	- Melakukan penjadwalan kembali dan melakukan penyesuaian jadwal dan biaya - Merekrut staf tambahan untuk membantu penyelesaian pelayanan publik agar tepat waktu
Kesalahan perancangan skala basis data	- Mengadakan pertemuan untuk membahas perancangan ulang skala basis data - Memberitahu staf jika terjadi perubahan pada sistem - Menambah jumlah staf agar layanan terhadap publik dapat optimal
B. RESIKO PENGARUH ORGANISASI	
Dokumentasi untuk pemerintah dianggap kurang baik oleh masyarakat	- Lakukan riset dari awal bagaimana membuat dokumentasi yang baik - Meminta saran dari masyarakat

C. RESIKO YANG BERHUBUNGAN DENGAN MASYARAKAT	
Masyarakat belum dapat memastikan apa yang dibutuhkannya	- Mencari tahu apa yang diinginkan dan dibutuhkan oleh masyarakat
Dinas-dinas terkait kurang berkomunikasi dengan pengembang untuk saling memberi informasi	- Mengadakan jajak pendapat melalui beberapa wakil publik - Membuat report dan simulasi yang sesingkat dan sedetil mungkin supaya dapat dilakukan perbaikan
Masyarakat tidak mengerti proses pengembangan perangkat lunak	- Memberi gambaran global tentang pengembangan sistem tersebut
D. RESIKO PROSES	
Tidak semua staf bersedia untuk mengikuti proses yang telah ditentukan	- Menyusun ulang pembagian tugas - Mengganti staf dengan yang lebih mampu
Para staf memiliki jadwal yang berbeda sehingga kurang koordinasi	- Manajer proyek harus dapat mengatur jadwal yang tepat untuk mengadakan pertemuan
Metode pengujian ternyata tidak dapat diterapkan pada perangkat lunak tersebut	- Mencari metode pengujian yang lebih baik dan lebih efektif
E. RESIKO TEKNOLOGI	
Tidak semua staf menguasai atau mengenal *tools* yang akan digunakan	- Memilih staff yang telah mengenal *tools* tersebut - Mengadakan pelatihan bagi staff yang belum menguasainya
Proyek membutuhkan inovasi oleh pengembang	- Mengumpulkan bahan-bahan yang diperlukan dan melakukan riset untuk persiapan proyek tersebut
F. RESIKO PERALATAN PENGEMBANGAN	
Perangkat lunak tidak tersedia	- Mencari perangkat lunak terlebih dahulu dan mencari alternatif perangkat lunak untuk dapat menggantikannya
Tidak tersedianya referensi yang cukup untuk peralatan yang digunakan	- Mencari referensi dari buku, majalah, internet, dll
G. RESIKO YANG BERHUBUNGAN DENGAN SDM	
Tidak tersedianya staf yang kompeten di bidang tersebut	- Merekrut staf yang ahli - Memberikan pelatihan
H. RESIKO KOMPONEN DAN PENGENDALI	
Performa sistem tidak seperti yang diharapkan	- Melakukan kompilasi ulang dengan mengoptimalkan dan memperbaiki perangkat lunak
Harga perangkat keras dan perangkat lunak di luar perkiraan	- Menyediakan dana cadangan
Perangkat lunak tidak bisa dikoreksi atau diubah	- Melakukan kompilasi ulang

Step9 : Select Control

KELOMPOK RESIKO	KONTROL YANG DIPILIH
A. RISIKO ESTIMASI	- Merekrut staf tambahan untuk membantu penyelesaian pelayanan publik agar tepat waktu - Mengadakan pertemuan untuk membahas perancangan ulang skala basis data, termasuk penjadwalan dan pendanaan
B. RISIKO PENGARUH ORGANISASI	- Lakukan riset dari awal bagaimana membuat dokumentasi yang baik - Meminta saran dari masyarakat
C. RISIKO YANG BERHUBUNGAN DENGAN MASYARAKAT	- Membuat laporan dan simulasi yang sesingkat dan sedetil mungkin supaya dapat dilakukan perbaikan - Memberi gambaran global tentang pengembangan sistem tersebut
D. RISIKO PROSES	- Mencari metode pengujian yang lebih baik dan lebih efektif
E. RISIKO TEKNOLOGI	- Mengadakan pelatihan bagi staf yang belum menguasainya
F. RISIKO PERALATAN PENGEMBANGAN	- Mencari perangkat lunak terlebih dahulu dan mencari alternatif perangkat lunak untuk dapat menggantikannya
G. RISIKO YANG BERHUBUNGAN DENGAN SDM	- Merekrut staf yang ahli dan memberikan pelatihan
H. RISIKO KOMPONEN DAN PENGENDALI	- Melakukan kompilasi ulang dengan mengoptimalkan dan memperbaiki perangkat lunak

3. KESIMPULAN

Pada awal penerapan pengendalian (*control*) yang dipilih, membutuhkan biaya yang cukup besar namun untuk jangka panjang akan diterima manfaat yang lebih besar karena pelayanan administrasi kepemerintahan akan lebih efektif dan efsien. Jika pengendalian (*control*) tersebut tidak diimplementasikan, maka dampaknya antar lain adalah terjadinya keterlambatan (*delay*), misalnya keterlambatan dalam pembayaran atau penerimaan uang, keterlambatan dalam pengiriman hasil atau output, yang lebih lanjut akan terkait dengan *contractual deadline* yang dapat menimbulkan denda atau penalti, juga terjadinya interupsi layanan (*sistem crash*),

misalnya terjadi kegagalan dalam memenuhi permintaan layanan yang diminta oleh publik.

Jika sistem pengoperasian terkena salah satu saja dari ancaman yang ada, maka sistem tidak dapat melayani mayarakat atau permintaan publik secara maksimal atau bahkan hal yang paling buruk dapat terjadi yaitu sistem tidak dapat dioperasikan sama sekali.

4. DAFTAR PUSTAKA

[1]. Gary Stonebumer, Alice Goguen, and Alexis Feringa, " *Risk Management Guide for Information Technology System*", 2002.

[2]. Gary Stonebumer, Alice Goguen, and Alexis Feringa, "*Engineering principles for IT Security*", NIST, 2001

[3]. Marianne Swanson and Barbara Guttman, "*Geneally Accepted principles and practices for securing information Technology systems*", NIST, 1996

[4]. http: //e-pemerintah.Com
(diakses tanggal 2 April 2010 pk. 19:12:10)

[5]. http: //www.garutkab.go.id/download–files/article/e–government menuju pelayanan . doc
(diakses tanggal 3 April 2010 pk 20:15:00)