SEMINAR NASIONAL TEKNOKA

Vol. 2, 2017
ISSN No. 2502-8782

Audit Aplikasi Zahir di PT Radisa Mahardi Rekatama Menggunakan *Framework COBIT* 5

Ardi Gunawan[1*], Johanes Fernandes Andry[2]

Sistem Informasi, Universitas Bunda Mulia
Jl. Lodan Raya Ancol No. 2, Jakarta 14430 Indonesia
E-mail: elnavaro@live.com [1], jandry@bundamulia.ac.id [2]

Abstrak – *Berdiri pada tahun 2009, PT. Radisa Mahardi Rekatama bergerak di bidang planning, engineering, manufacturing, installing dan customizing. Dalam aktivitas harian mereka menggunakan Aplikasi Office seperti Word dan Excel untuk pembukuan mereka. Namun mereka beralih ke Aplikasi Zahir Project kerena mereka sering kehilangan data ketika terjadi mati listrik secara tiba-tiba. Tujuan dari Audit ini adalah untuk mengetahui seberapa besar penggunaan dan keefektifan dan efisiensi dari Aplikasi Zahir Project dalam Perusahaan. Hal ini untuk mencari tahu apakah penggunaan Aplikasi Zahir Project sudah tepat untuk Perusahaan ini atau belum. Manfaat untuk Perusahaan sendiri adalah untuk menjadi evaluasi apakah mereka sudah tepat menggunakan Aplikasi Zahir Project di Perusahaan mereka. COBIT merupakan salah satu framework yang sering digunakan oleh para auditor terutama auditor sistem informasi. Ini karena COBIT dapat dipakai sebagai alat yang komprehensif untuk menciptakan tata kelola teknologi informasi pada suatu perusahaan. Hasil dari kajian yang dilakukan adalah membuat pengukuran kinerja aplikasi customized yang berupa analisa, pemetaan level of capability dan rekomendasi bagi perusahaan tersebut. Standar yang digunakan pada penelitian ini adalah COBIT 5 yang berfokus pada domain Delivery-Support-and-Service (DSS).*

***Kata kunci**: PT. Radisa Mahardi Rekatama, Audit, Cobit 5, Delivery-Support-and-Service (DSS)*
.

1 Pendahuluan

Banyaknya perusahaan Teknologi informasi yang berdiri, makin banyak pula aplikasi-aplikasi yang beredar diluar sana. Aplikasi-aplikasi yang ditawarkan juga sangat bervariasi, mulai dari yang paling murah sampai yang paling mahal, dari yang paling buruk hingga yang paling baik, semua itu banyak dipakai oleh perusahaan-perusahaan kecil hingga besar [1].

PT. Radisa Mahardi Rekatama adalah salah satu dari banyak Perusahaan yang bergerak dibidang *planning, engineering, manufacturing, installing* dan *customizing* yang menggunakan Aplikasi Zahir *Project* untuk laporan keuangan mereka. Untuk selanjutnya, kalimat PT. Radisa Mahardi Rekatama akan disingkat menjadi RMR.

Tujuan dari penelitian ini adalah mendapatkan gambaran mengenai kinerja, efektivitas serta efisiensi dari Aplikasi *Zahir Project* di RMR yang sedang berjalan saat ini, dengan berbagai aspek yang diperhatikan seperti: efektivitas (*effectiveness*), efisiensi (*efficiency*), *data integrity, realibility, confidentiality, availability*, dan *security*.

COBIT ialah acuan atau kerangka kerja untuk pengukuran dan pengendalian TI. Kerangka kerja *COBIT* merupakan standar yang dinilai paling lengkap dan menyeluruh sebagai framework audit TI, karena dikembangkan berdasarkan aturan atau prosedur internal perusahaan atau institusi, sehingga saat dilakukan pengukuran akan sesuai dengan kondisi, aturan, prosedur kerja dan norma yang ada di perusahaan tersebut. *COBIT* telah dikembangkan secara berkelanjutan oleh lembaga profesional auditor yang tersebar hampir di seluruh dunia [2].

2 Dasar Teori

2.1. Audit Sistem Informasi

Audit Teknologi informasi pada hakekatnya merupakan salah satu dari bentuk audit operasional, tetapi kini audit

Manuscript received 20 September 2017, revised 29 September 2017

teknologi informasi sudah dikenal sebagai satu satuan jenis audit tersendiri yang tujuan utamanya lebih untuk meningkatkan tata kelola TI. Sebagai suatu audit operasional terhadap manajemen sumber daya informasi, yaitu efektivitas, efisiensi, dan ekonomis tidaknya unit fungsional sistem informasi pada suatu organisasi. Dengan diperkenalkan *COBIT*, kini tujuan audit bukan hanya terbatas pada konsep klasik saja, melainkan kini menjadi: efektivitas, efisiensi, kerahasiaan, keterpaduan, ketersediaan, kepatuhan pada kebijakan/aturan dan keandalan sistem informasi. Dalam pelaksanaannya, jenis audit ini berkembang dalam beberapa variannya:

1. Pemeriksaaan operasional (*operational audit*) terhadap pengelolaan sistem informasinya, atau lebih tepatnya/tegasnya terhadap tata-kelola teknologi informasi (*IT governance*),
2. *General information review*, audit terhadap sistem informasi secara umum pada suatu organisasi tertentu,
3. Audit terhadap aplikasi tertentu yang sedang dikembangkan (*quality assurance* pada tahap *system development*) [3].

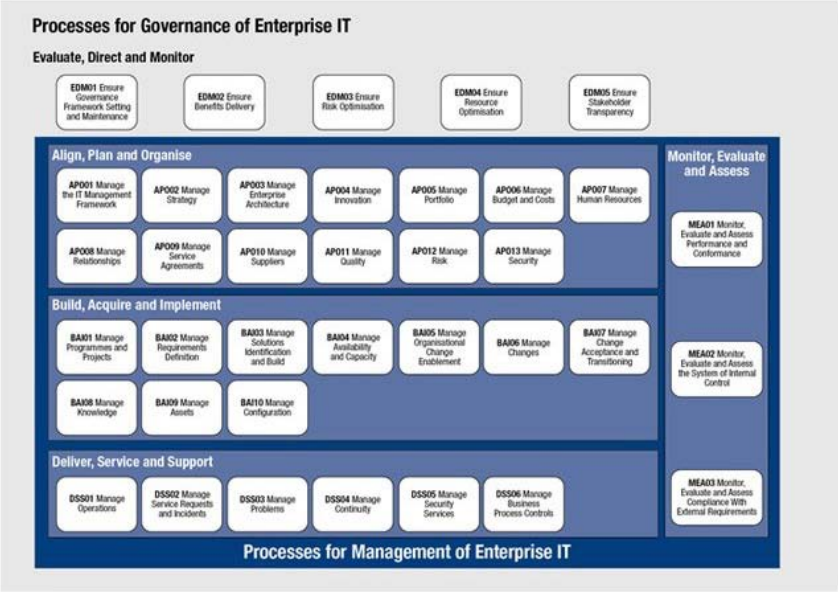
2.2. COBIT 5

Control Objectives for Information and Related Technology (*COBIT*) adalah *framework* yang dibuat oleh *Information Systems Audit and Control Association* (ISACA) untuk manajemen TI dan tata kelola TI dan sekarang banyak digunakan oleh bisnis. ISACA adalah pemimpin dunia yang diakui dalam tata kelola, kontrol, keamanan dan kepastian TI [4], [5].

COBIT 5 bersifat umum dan berguna untuk segala jenis ukuran perusahaan, baik itu sektor komersial, sektor *nonprofit* atau pada sektor pemerintahan atau publik. *COBIT* 5 didasarkan pada lima prinsip kunci untuk tata kelola dan manajemen TI perusahaan. Kelima prinsip ini memungkinkan perusahaan untuk membangun sebuah kerangka tata kelola dan manajemen yang efektif, yang dapat mengoptimalkan investasi dan penggunaan TI untuk mendapatkan keuntungan bagi para *stakeholder* [6].

Secara teori, perusahaan dapat mengatur prosesnya sesuai keinginan, selama tujuan pengelolaan dan pengelolaan dasar tercakup. Usaha kecil mungkin memiliki lebih sedikit proses; Perusahaan yang lebih besar dan lebih kompleks mungkin memiliki banyak proses, semuanya mencakup tujuan yang sama. Model referensi proses *COBIT* 5 adalah penerus model proses *COBIT* 4.1, dengan model proses TI Risiko dan Val IT terintegrasi juga. Gambar 1. Model Referensi Proses *COBIT* 5 menunjukkan rangkaian lengkap 37 proses tata kelola dan manajemen dalam *COBIT*. *COBIT* 5 *Process Reference Model* menunjukkan rangkaian lengkap 37 proses tata kelola dan manajemen dalam *COBIT* 5 [7], [9].

Bahkan dalam *COBIT* 5 juga ada tujuan terkait TI tentang keamanan dan ada salah satu produk dari *COBIT* 5 yang khusus fokus pada keamanan informasi, yaitu *COBIT* 5 for Information Security [8]. Hal itulah yang menjadi pertimbangan bagi peneliti untuk melakukan Audit Aplikasi Zahir menggunakan *COBIT*, terutama pada domain DSS01, DSS02, DSS04 dan juga pada Domain DSS05.



Gambar 1 *Model Referensi Proses dalam COBIT 5* [5], [6], [7], [8], [9].

ISSN No. 2502-8782

2.3. Capability Model

Model penilaian kapabilitas proses pada COBIT 5 berdasarkan pada ISO/IEC 15504, standar mengenai *Software Engineering* dan *Process Assessment*.

Kapabilitas proses merupakan karakteristik dari kemampuan sebuah proses untuk mencapai tujuan bisnis saat ini ataupun saat mendatang. Penilaian kapabilitas proses dilakukan untuk mengidentifikasi *level* kapabilitas proses tertentu dan kemudian menentukan langkah selanjutnya untuk melakukan peningkatan terhadap kapabilitas proses tersebut. Setiap atribut mendefinisikan aspek tertentu dari kapabilitas proses. Kombinasi pencapai atribut proses tersebut akan menentukan *level* kapabilitas proses [10].

Dari Tabel 1 dapat dilihat bahwa *Level* kapabilitas proses yang digunakan di dalam penilaian proses terdiri dari enam *level* yaitu:

Tabel 1 Capability Level di dalam COBIT 5 [10].

Level	**Definisi Proses**
0	*Incomplete process* Proses tidak diimplementasi atau gagal mencapai tujuan proses. Terdapat sedikit atau tidak ada bukti pencapaian tujuan proses secara sistematis
1	*Performed process* Implementasi proses mencapai tujuannya. Atribut proses yang mencerminkan pencapaian level ini adalah PA1.1 process performance. PA 1.1 mengukur sampai sejauh mana tujuan proses dicapai. Hasil pencapaian atribut ini tercermin dari setiap proses menghasilkan keluaran yang diharapkan.
2.1	*Performance Management* Mengukur sampai sejauh mana pelaksanaan proses diatur.
2.2	*Work Product Management* Mengukur sampai sejauh mana produk kerja diproduksi oleh proses yang telah diatur dengan baik.
3.1	*Process Definition* Mengukur sejauh mana proses didefinisikan untuk mendukung pelaksanaan proses.
3.2	*Process Deployment* Mengukur sejauh mana standar proses dilaksanakan secara efektif.
4.1	*Process Measurement* Mengukur sejauh mana hasil pengukuran digunakan untuk menjamin pelaksanaan proses dapat mendukung pencapaian tujuan organisasi.
4.2	*Process Control* Mengukur sejauh mana proses diatur secara kuantitatif untuk menghasilkan sebuah proses yang stabil dan dapat diprediksi sesuai dengan batasan yang didefinisikan.
5.1	*Process Innovation* Pengukuran sejauh mana perubahan proses diidentifikasi dari pelaksanaan proses dan dari pendekatan inovasi terhadap pelaksanaan proses.
5.2	*Process Optimization* Mengukur sejauh mana perubahan didefinisikan, mengelola pelaksanaan proses secara efektif untuk mendukung pencapaian tujuan peningkatan proses.

Skala yang digunakan untuk menilai atribut proses yaitu [11]:

N: *not achieved* (0 sampai dengan 15%) Terdapat sedikit atau tidak terdapat sama sekali bukti pencapaian atribut terhadap proses yang dinilai.

P: *partially achieved* (>15% sampai dengan 50%) Terdapat beberapa bukti pendekatan dan beberapa pencapaian atribut proses yang dinilai. Beberapa aspek pencapaian atribut mungkin tidak dapat diprediksi.

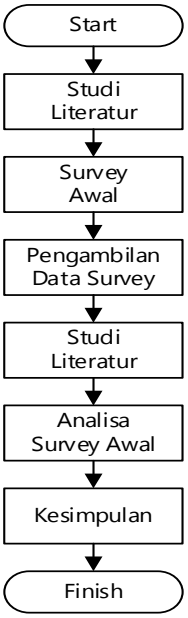
L: *largely achieved* (>50% sampai dengan 85%) Terdapat bukti pendekatan sistematik dan pencapaian yang signifikan terhadap atribut proses yang dinilai. Beberapa kelemahan terkait atribut ini mungkin terdapat di dalam proses yang dinilai.

F: *fully achieved* (>85% sampai dengan 100%) Terdapat bukti lengkap dan pendekatan sistematik serta pencapaian penuh terhadap atribut proses yang dinilai. Tidak terdapat kelemahan terkait atribut yang terdapat di dalam proses yang dinilai.

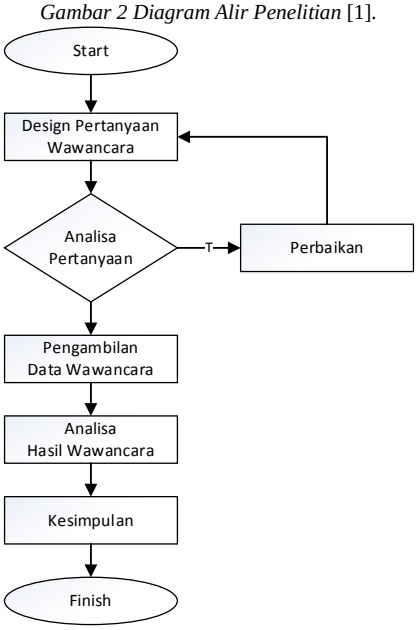
3 Metodologi Penelitian

Metodologi penelitian yang dilakukan dan tahapan-tahapan penulis dalam mengambil ataupun memperoleh data dari sumber, mulai dari studi literatur, survei awal, dan wawancara ditujukan pada Gambar 2. Diagram Alir Penelitian, Gambar 3 Diagram Alir Wawancara.

ISSN No. 2502-8782



Gambar 2 Diagram Alir Penelitian [1].



Gambar 3 Diagram Alir Wawancara [1].

4 Hasil dan Pembahasan

Pada bab ini, akan dibahas hasil Analisa dari Domain DSS yang berfokus pada Domain DSS dan proses-proses nya. RMR mengharapkan bahwa mereka mendapatkan hasil *process capability* bernilai 3, yaitu *Established Process*.

4.1. DSS01 Process Practices, Inputs/Outputs and Activities
Mengkoordinasikan dan melaksanakan kegiatan dan prosedur operasional yang diperlukan untuk memberikan layanan TI *internal* dan *outsource*, termasuk pelaksanaan prosedur operasi standar yang telah ditentukan sebelumnya dan kegiatan pemantauan yang diperlukan.

4.1.1. DSS01.01 Manage Operations
Menjaga dan melaksanakan prosedur operasional dan tugas operasional secara andal dan konsisten**.**

Hasil audit didapatkan bahwa RMR telah mempunyai prosedur tetap dan juga telah melaksanakan penggunaan Aplikasi Zahir sesuai dari prosedur yang telah ditetapkan. *Level capability* 3.1 yaitu *Process Definition*.

4.1.2. DSS01.02 Manage outsourced IT services
Mengelola pengoperasian layanan TI dari *Outsource* untuk menjaga perlindungan informasi perusahaan dan keandalan pemberian layanan.

Pihak Aplikasi Zahir tidak memiliki *ToS Agreement* didalam Aplikasi mereka yang mengikat Perusahaan, namun pihak RMR masih dapat menghubungi pihak Zahir ketika ada *error* yang terjadi pada program Zahir tersebut. Pihak Zahir akan langsung menangani masalah pada RMR saat itu juga. *Level Capability* 2.2 yaitu *Work Product Management*

4.1.3. DSS01.03 Monitor IT infrastructure
Memantau infrastruktur TI dan acara terkait. Simpan informasi kronologis yang cukup dalam *log* operasi untuk memungkinkan rekonstruksi, peninjauan dan pemeriksaan terhadap urutan waktu operasi dan aktivitas lain yang mengelilingi atau mendukung operasi.

RMR sudah mempunyai *log* tentang keuangan keluar masuk yang terjadi di dalam Perusahaan tetapi belum di urutkan dari yang terpenting dan tidak terlalu penting. Semua masuk dalam 1 *log* di dalam aplikasi Zahir. *Level Capability* 2.2 yaitu *Work Product Management*.

4.1.4. DSS01.04 Manage the environment
Mengelola pengoperasian layanan TI secara *outsource* untuk menjaga perlindungan informasi perusahaan dan keandalan pemberian layanan.

RMR sudah mengetahui ancaman yang mungkin terjadi di dalam ruang *Server*, namun Karena kondisi lingkungan yang baik, sehingga perusahaan belum berpikir untuk melindungi *Server* ketika terjadi bencana seperti banjir, gempa bumi, dsb. Namun perusahaan telah mempunyai prosedur untuk para karyawan ketika terjadi bencana alam, yaitu pertama menyelamatkan diri untuk para karyawan lalu sebisa mungkin melindungi data yang bias diselamatkan didalam ruang *Server*. *Level Capability* 2.1 yaitu *Performance Management*.

4.1.5. DSS01.05 Manage facilities
Mengelola fasilitas, termasuk peralatan listrik dan komunikasi, sesuai dengan peraturan perundang-undangan, persyaratan teknis dan bisnis, spesifikasi *vendor*, dan pedoman keselamatan dan kesehatan kerja.

ISSN No. 2502-8782

RMR telah memiliki salah satu dari hal wajib untuk penangan ketika listrik padam, yaitu *UPS* yang mampu menahan daya hingga 2 jam ketika listrik padam. Hal ini sudah lebih dari cukup ketika terjadi pemadaman listrik Karena dalam waktu tersebut perusahaan masih bisa menggunakan alat TI dan masih memiliki banyak waktu untuk menyimpan data penting perusahaan.

Selain itu didapat bahwa seluruh penanganan kabel dari tiang listrik hingga kedalam gedung dikelola oleh PLN, sementara untuk pembagian listrik untuk penggunaan IT dan manufaktur sudah dilakukan oleh pihak perusahaan sendiri. *Level Capability* 2.2 yaitu *Work Product Management*.

4.2. DSS02 Manage Service Requests and Incidents

Memberikan respon yang tepat waktu dan efektif terhadap permintaan pengguna dan penyelesaian semua jenis insiden. Kembalikan layanan normal; Merekam dan memenuhi permintaan pengguna; Dan mencatat, menyelidiki, mendiagnosis, meningkatkan dan menyelesaikan insiden.

4.2.1. DSS02.01 Define incident and service request classification schemes

Menentukan skema klasifikasi dan model permintaan dan permintaan.

RMR telah mengetahui proses tentang insiden keamanan ini, namun mereka belum memiliki prosedur seperti pencatatan apa saja yang akan dilakukan ketika terjadi bencana. *Level Capability* 1.1 yaitu *Process Performance*

4.2.2. DSS02.02 Record, classify and prioritise requests and incidents

Mengidentifikasi, mencatat dan mengklasifikasikan permintaan layanan dan insiden, dan menetapkan prioritas sesuai dengan kekritisan dan kesepakatan layanan bisnis.

RMR telah mengetahui dan mengidentifikasikan informasi di Perusahaan dan telah mengurutkan catatan pada masing-masing topik, namun belum mengurutkan dari hal yang terpending hingga tidak terlalu penting. *Level Capability* 2.1 yaitu *Performance Management*.

4.2.3. DSS02.03 Verify, approve and fulfil service requests

Memilih prosedur permintaan yang sesuai dan verifikasi bahwa permintaan layanan memenuhi kriteria permintaan yang ditentukan. Dapatkan persetujuan, jika diperlukan, dan memenuhi permintaan. Dengan kekritisan dan kesepakatan layanan bisnis.

RMR telah mengetahui proses ini namun mereka belum menerapkan di dalam standar operasional mereka. *Level Capability* 1.1 yaitu *Process Performance*

4.2.4. DSS02.04 Investigate, diagnose and allocate incidents

Mengidentifikasi dan mencatat gejala kejadian, menentukan penyebab yang mungkin, dan mengalokasikan untuk resolusi.

RMR telah mengetahui proses ini dan telah meletakkan hal yang mungkin terkena bencana alam di tempat yang aman, namun mereka belum memiliki standar untuk mencatat, dan menganalisa bencana alam yang kemungkinan bias terjadi secara tiba-tiba. *Level Capability* 1.1 yaitu *Process Performance*

4.2.5. DSS02.05 Resolve and recover from incidents

Mendokumentasikan, menerapkan dan menguji solusi dan solusi yang teridentifikasi dan melakukan tindakan pemulihan untuk memulihkan layanan terkait TI.

RMR memiliki Server yang terpisah yang digunakan sebagai *Master Backup* ketika terjadi bencana dan hal-hal yang tidak diinginkan. Ketika komputer *Client* yang digunakan *IT Manager* maupun Manager terkena serangan *virus, malware* dan sebagainya ataupun ketika *hardware* dari komputer tiba-tiba rusak, makan data RMR akan tetap aman karena tersimpan pada *storage* yang berbeda. Ketika hal yang diinginkan pun itu terjadi, maka RMR sudah memiliki prosedur sendiri untuk memulihkan data mereka ke masing-masing komputer Client. *Level capability* 3.2 yaitu *Process Deployment*.

4.2.6. DSS02.06 Close service requests and incidents

Melakukan verifikasi penyelesaian insiden yang memuaskan dan / atau pemenuhan permintaan, dan tutup.

RMR akan melakukan verifikasi apakah masalah yang mereka hadapi sudah terselesaikan atau belum, jika sudah maka mereka akan membuat laporan bahwa masalah tersebut sudah selesai, namun jika belum maka mereka akan meminta *vendor* terkait untuk melakukan *crosscheck* hingga masalah mereka terselesaikan. *Level Capability* 2.2 yaitu *Work Product Management*.

4.2.7. DSS02.07 Track status and produce reports

Secara teratur melacak, menganalisa dan melaporkan kejadian dan meminta pemenuhan tren untuk memberikan informasi perbaikan terus-menerus.

RMR sudah menerapkan pencatatan masalah TI yang terjadi namun hanya sebatas informasi saja, belum sampai ke pembukuan dan mereka belum sampai ke integrase data secara *online*. *Level Capability* 1.1 yaitu *Process Performance*

4.3. DSS03 Manage Problems

Mengidentifikasi masalah dan mengklasifikasikan masalah dan akar permasalahannya dan memberikan resolusi tepat waktu untuk mencegah kejadian berulang. Memberikan rekomendasi untuk perbaikan.

4.3.1. DSS03.01 Identify and classify problems

Menentukan dan menerapkan kriteria dan prosedur untuk melaporkan masalah yang teridentifikasi, termasuk klasifikasi masalah, kategorisasi dan prioritas.

RMR tidak terlalu berfokus kepada manajemen TI di Perusahaan mereka karena RMR bergerak di bidang

ISSN No. 2502-8782

manufacturing produk yang tidak terlalu membutuhkan infrastruktur TI yang besar, sehingga mereka tidak memiliki standar ketika terjadi perubahan besar pada bidang TI di dalam Perusahaan. Mereka akan menyerahkan tugas TI kepada pihak yang bersangkutan untuk menangani masalah tersebut. Tetapi untuk masalah penentuan ahli TI untuk *hardware* dan *software* yang bersifat *simple* di, RMR telah menunjuk seorang ahli TI di Perusahaan untuk mengatur hal tersebut. *Level Capability* 1.1 yaitu *Process Performance.*

4.3.2. DSS03.02 Investigate and diagnose problems

Menyelidiki dan mendiagnosa masalah dengan menggunakan ahli manajemen subjek yang relevan untuk menilai dan menganalisis akar permasalahan.

RMR telah memiliki prosedur ketika terjadi masalah *error* pada program mereka yaitu menghubungi *Developer* aplikasi Zahir untuk melakukan konsultasi langsung melalui telfon, namun RMR belum sampai memiliki catatan khusus tentang masalah-masalah yang mereka hadapi untuk menjadi pedoman di kemudian hari. *Level Capability* 1.1 yaitu *Process Performance*

4.3.3. DSS03.03 Raise known errors

Segera setelah akar penyebab masalah diidentifikasi, buat catatan kesalahan yang diketahui dan solusi yang sesuai, dan identifikasi solusi potensial.

RMR sampai saat ini belum memiliki kasus kesalahan di bidang Aplikasi Zahir yang sangat fatal hingga terjadi *error* yang membuat lumpuh Perusahaan, maka dari itu RMR belum sampai memiliki catatan dari kesalahan apa dan solusi apa yang harus dilakukan ketika Aplikasi terjadi *error*. Mereka akan langsung menghubungi pihak *Developer* ketika hal tersebut terjadi. *Level Capability* 0 yaitu *Incomplete Process*.

4.3.4. DSS03.04 Resolve and close problems

Mengidentifikasi dan memulai solusi berkelanjutan yang menangani akar permasalahan, meningkatkan permintaan perubahan melalui proses manajemen perubahan yang mapan jika diperlukan untuk menyelesaikan kesalahan. Pastikan personil yang terkena dampak sadar akan tindakan yang diambil dan rencana yang dikembangkan untuk mencegah kejadian di masa depan.

RMR memiliki pengaturan jadwal ketika terjadi kerusakaan hal TI di dalam Perusahaan seperti sambungan kabel yang putus, *hardware* atau *software* komputer yang *error*, semua hal itu mereka jadwalkan untuk kapan diperbaiki oleh teknisi terkait.

RMR juga akan memberikan laporan konfirmasi bahwa masalah yang mereka hadapi telah selesai, sehingga pihak terkait mengetahui bahwa masalah yang mereka hadapi telah terselesaikan. *Level capability* 3.1 yaitu *Process Definition*.

4.3.5. DSS03.05 Perform proactive problem managements

Mengumpulkan dan menganalisis data operasional (terutama kejadian dan catatan perubahan) untuk mengidentifikasi kecenderungan yang muncul yang mungkin mengindikasikan masalah. *Log* catatan masalah untuk mengaktifkan penilaian.

RMR belum mengetahui proses ini, mereka belum memiliki *log* masalah dan mereka tidak melakukan penilaian terhadap masalah terkait dengan TI yang terjadi.

Mereka juga belum memikirkan jadwal teratur untuk mengadakan pertemuan antar manager dan pemilik RMR untuk membahas masalah perubahan tata kelola TI. *Level Capability* 0 yaitu *Incomplete Process.*

4.4. DSS05 Manage Security Services

Melindungi informasi perusahaan untuk menjaga tingkat risiko keamanan informasi yang dapat diterima oleh perusahaan sesuai dengan kebijakan keamanan. Menetapkan dan memelihara peran keamanan informasi dan hak akses dan melakukan pemantauan keamanan.

4.4.1. DSS05.01 Protect against malware

Melaksanakan dan memelihara tindakan pencegahan, detektif dan perbaikan yang ada (terutama *patch* keamanan dan pengendalian *virus* terkini) di seluruh perusahaan untuk melindungi sistem informasi dan teknologi dari perangkat lunak perusak (misal *Virus, worm, spyware, spam*).

RMR sudah memiliki *Anti-virus* di dalam masing-masing komputer *Client*. Perusahaan juga menetapkan bahwa komputer *Client* hanya boleh digunakan untuk proses kerja, dan tidak boleh untuk hal lain seperti melakukan *install* aplikasi dari luar.

RMR menerima order melalui telfon dan sms dan mereka juga memiliki alamat *e-mail* bernama support@radisa-mr.com yang belum memiliki fitur *auto-filter* pesan spam sehingga seluruh pesan akan masuk tanpa dilakukan *filter* terlebih dahulu.

Namun untuk pemantauan secara teratur, pihak RMR belum sampai melakukan hal tersebut.

Ketika hal paling buruk seperti *Harddisk* komputer *Client* rusak, terkena *virus* dan serangan lainnya, mereka sudah memiliki *backup Server* di ruangan yang berbeda sehingga kehilangan data dapat diminimalisir. *Level capability* 3.1 yaitu *Process Definition*.

4.4.2. DSS05.02 Manage network and connectivity security

Gunakan tindakan pengamanan dan prosedur manajemen terkait untuk melindungi informasi dari semua metode konektivitas.

RMR membagi menjadi 2 bagian operasional komputer mereka, yaitu *Client* dan *Server*. Masing-masing tentu saja memiliki *password* yang dibutuhkan ketika ingin melakukan penggunaannya.

RMR memiliki jalur sendiri dan tidak berhubungan dengan jalur lain yaitu dengan menggunakan *Wireless* yang di *password* untuk menghubungkan *Client* dan *Server* mereka.

Namun RMR belum melakukan proses enkripsi data sehingga data yang keluar masuk adalah data asli yang dapat

ISSN No. 2502-8782

dengan mudah dibaca oleh semua orang tanpa proses lebih lanjut lagi.

RMR belum pernah melakukan ujian penetrasi sistem mereka dan tidak memiliki jadwal pengujian sistem secara berkala untuk mengetahui seberapa kuat keamanan dari *Server* mereka. *Level Capability* 2.2 yaitu *Work Product Management*.

4.4.3. DSS05.03 Manage endpoint security

Memastikan titik akhir (misalnya, *laptop, desktop, server*, dan perangkat seluler dan jaringan seluler atau perangkat lunak lainnya) dijamin pada tingkat yang sama atau lebih besar dari persyaratan keamanan yang ditetapkan dari informasi yang diproses, disimpan atau dikirim.

Pihak RMR telah melakukan konfigurasi sistem operasi dengan aman yaitu menggunakan *Windows Original* pada perusahaan mereka. Namun mereka sama sekali tidak melakukan proses enkripsi data masuk dan keluar dalam Perusahaan.

Pihak RMR juga belum mengetahui proses isi lebih lanjut namun beberapa proses sudah mereka ketahui. *Level Capability* 1.1 yaitu *Process Performance*

4.4.4. DSS05.04 Manage user identity and logical access

Memastikan semua pengguna memiliki hak akses informasi sesuai dengan kebutuhan bisnis mereka dan berkoordinasi dengan unit bisnis yang mengelola hak akses mereka sendiri dalam proses bisnis.

Hanya *manager* dan ahli TI terkait yang boleh menggunakan komputer di dalam ruangan TI, dan hanya ahli TI yang boleh masuk keruangan *Server* sehingga bencana oleh manusia sudah diminimalisir oleh RMR.

Namun untuk hak akses istimewa hanya ada *password* ketika *login Windows* tanpa ada akses *eksklusif* dengan *Username* yang berbeda.

Pihak RMR juga belum memiliki jadwal untuk manajemen rutin terkait dengan peninjauan akun istimewa. *Level Capability* 1.1 yaitu *Process Performance*

4.4.5. DSS05.05 Manage physical access to IT assets

Menentukan dan menerapkan prosedur untuk memberi, membatasi dan mencabut akses terhadap bangunan, bangunan dan area sesuai kebutuhan bisnis, termasuk keadaan darurat. Akses ke bangunan, bangunan dan area harus dibenarkan, disahkan, dicatat dan dipantau. Ini harus berlaku untuk semua orang yang memasuki tempat itu, termasuk staf, staf sementara, klien, *vendor*, pengunjung atau pihak ketiga lainnya.

RMR berjalan dalam sebuah gedung yang memiliki ruangan *Server*, ruangan kantor/kerja dan ruangan untuk proses *manufacturing*. Karena gedung hanya terdiri dari tiga lantai dan tidak terlalu besar, makan akses untuk masuk tidak terlalu ketat, pengunjung tidak memerlukan tanda pengenal dan tidak diharuskan menggunakan *nametag* untuk masuk ke dalam.

Di RMR juga belum ada kartu tanda pengenal yang sampai digunakan untuk proses *authentification* dan disini belum ada pembatasan akses antar ruang, semua bekerja di dalam satu ruangan kantor, satu ruangan untuk *manufacture* dan satu ruangan untuk *Server*, namun untuk ruangan *Server* dijaga 24 jam 7 hari untuk memastikan tidak boleh ada orang yang tidak berwenang masuk ke dalam ruangna *Server*.

Untuk penggunaan *biometric*, RMR menggunakan sidik jari hanya untuk sebatas melakukan absen harian. *Level Capability* 1.1 yaitu *Process Performance*

4.4.6. DSS05.06 Manage sensitive documents and output devices

Menetapkan pengamanan fisik, praktik akuntansi dan pengelolaan persediaan yang tepat atas aset TI yang sensitif, seperti formulir khusus, instrumen yang dapat dinegosiasikan, printer tujuan khusus atau token keamanan.

Semua dokumen yang masuk harus diterima oleh *manager* dan melalui proses pengecekan terlebih dahulu, namun belum ada penetapan hak akses terhadap dokumen apa saja yang boleh dilihat oleh masing-masing *manager*.

RMR membuang sampah dokumen yang pernah dianggap penting dengan cara di rusak terlebih dahulu seperti perobekan kertas sehingga jika ada orang yang menemukan dokumen tersebut, maka orang tersebut akan kesulitan untuk mengetahui informasi apa yang ada di dalam dokumen tersebut, namun RMR tidak menyediakan tempat terpisah untuk sampah pembuangan dokumen dan menjadikan 1 dengan sampah lainnya. *Level Capability* 2.1 yaitu *Performance Management*.

4.4.7. *DSS05.07 Monitor the infrastructure for security-related events*

Menggunakan alat deteksi intrusi, memantau infrastruktur untuk akses yang tidak sah dan memastikan bahwa setiap peristiwa diintegrasikan dengan pemantauan kejadian dan pengelolaan kejadian secara umum.

RMR belum memiliki laporan kejadian terkait TI yang terjadi di perusahaan, mereka juga belum mempunyai alat TI seperti *Metal Detector* namun mereka sudah mempunyai *CCTV* untuk bagian keamanan.

Karyawan di RMR dilatih untuk bisa secara terus mematuhi aturan dan standar prosedur yang berlaku dan mereka juga dituntut untuk bisa bekerja dibawah tekanan agar proyek yang mereka kerjakan bisa selesai tepat waktu sesuai dengan permintaan *Client*. *Level Capability* 1.1 yaitu *Process Performance.*

Dari hasil diatas, maka didapatkan hasil rata-rata Domain DSS beserta proses-prosesnya seperti terlihat pada tabel 2.

ISSN No. 2502-8782

Tabel 2 Summary Hasil Rata-rata.

No.	*Sub Domain*	*Current*	*Expected*
DSS01	*Process Practices, Inputs/Outputs and Activities*	2.4	3
DSS02	*Manage Service Requests and Incidents*	1.7	3
DSS03	*Manage Problems*	1.1	3
DSS05	*Manage Security Services*	1.7	3

5 Simpulan dan Saran

5.1. Simpulan

Dari pembahasan diatas, bias dikatakan bahwa RMR sudah menggunakan Aplikasi Zahir dan sudah mengimplementasikan standar pengoperasionalan IT di Perusahaan mereka.

Mereka juga sudah melakukan tindakan preventif untuk penanggulangan bencana dengan menempatkan Server yang berbeda dengan ruang kerja mereka.

RMR belum memiliki prosedur pencatatan akan bencana yang kemungkinan dapat terjadi dan belum memiliki pembukuan tentang bencana apa saja yang pernah terjadi di dalam Perusahaan.

5.2. Saran

RMR harus secara rutin melakukan *maintenance Server* serta membuat *backup* data yang ada di *Server,* dan juga membuat persiapan untuk menanggulangi ketika terjadi bencana baik dari alam maupun dari manusia, hal ini untuk meminimalisir adanya kehilangan data ketika terjadi hal yang tidak diinginkan.

RMR juga harus membuat prosedur yang perlu dilakukan ketika terjadi bencana ataupun hal yang tidak diinginkan, dan melakukan pencatatan *history error* apa saja yang terjadi di dalam aplikasi Zahir sehingga ketika kedepan nya terjadi pergantian orang ataupun penambahan pekerja yang terkait dalam bidang TI di dalam Perusahaan, maka orang tersebut bisa melihat hal apa yang harus ia lakukan ketika terjadi *error* pada aplikasi Zahir.

Kepustakaan

[1] Andry, J.F., *Audit Tata Kelola TI Menggunakan Kerangka Kerja COBIT pada Domain DS dan ME di Perusahaan Kreavi Informatika Solusindo,* Seminar Nasional Teknologi Informasi dan Komunikasi 2016, Yogyakarta, 18-19 Maret 2016.

[2] Hidayat, A.E., *Audit Control Capability Level Tata Kelola Sistem Informasi Menggunakan COBIT 5*, Jurnal Informasi, Bandung, November 2015.

[3] Andry, J.F., *Audit Sistem Informasi Sumber Daya Manusia Pada Training Center di Jakarta Menggunakan Framework COBIT 4.1*, Jurnal Ilmiah FIFO Vol. 8, No.1, Mei 2016.

[4] Pasquini, A., *COBIT 5 and the Process Capability Model. Improvements Provided for IT Governance Process, Proceedings of FIKUSZ '13 Symposium for Young Researchers*, pp. 67-76, 2013.

[5] Andry, J.F., *Performance Measurement IT of Process Capability Model Based on COBIT: A Study Case*, Jurnal Ilmiah DASI Vol.17 No. 3, Yogyakarta, September 2016.

[6] Putri, R.E., *Teknik Informatika Program Studi Sistem Komputer FTI Universitas Andalas*, Jurnal CoreIT, Vol.2, No.1, Juni 2016, Padang: Jl. Kampus Limau Manis. (2016).

[7] ISACA COBIT 5, 2012, *Enabling Process Institute*, www.itgi.org.

[8] Ciptaningrum, D., Nugroho, E. & Adhipta, D., *Audit Keamanan Sistem Informasi pada Kantor Pemerintah Kota Yogyakarta menggunakan COBIT 5*, Seminar Nasional Teknologi Informasi dan Komunikasi 2015, Yogyakarta, 28 Maret 2015.

[9] Andry, J.F., *Process Capability Model Based on COBIT 5 Assessments (Case Study)*, Jatisi, Vol. 3 No. 1 September 2016, Palembang.

[10] ISO/IEC 15504-2, "*Software Engineering Process Assessment Part* 2: *Performing an assessment*", 2003.