DAFTAR PUSTAKA

Alvin, Soekamto, W., dan Harsono, R. (2013). *Analisis dan Evaluasi Tata kelola IT Pada PT FIF dengan Standar COBIT 5*. Jakarta: Universitas Bina Nusantara

Chartered Institute of Management Accountants. (2007). *Enterprise Governance*.

Gay, L.R. & Diehl, P.L. (1992). *Research Methods for Business and Management*. New York: MacMillan Publishing Company.

Gelbstein, E. (2012). Strengthening Information Security Governance. *Journal of Information Systems and Audit Control Association.*

Information Systems Audit and Control Association. (2012). *COBIT 5 Enabling Process.*

Information Systems Audit and Control Association. (2012). *COBIT 5 for Information Security*.

Information Systems Audit and Control Association. (2012). *Process Assessment Model (PAM): Using COBIT 5*.

Information Systems Audit and Control Association. (2012). *Self-Assessment Guide: Using COBIT 5*.

Information Systems Audit and Control Association. (2013). *CISA Review Manual 2013.*

Information Systems Audit and Control Association. (2013). *CISM Review Manual 2013*.

ISO & IEC. (2005). *ISO/IEC 27001:2005*.

Information Technology Governance Institute. (2006). *Information Security Governance: Guidance for Boards of Directors and Executive Management* (2nd Ed.).

Information Technology Governance Institute. (2006). *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the design and Implementation of Internal Control over Financial Reporting* (2nd Ed.).

Information Technology Governance Institute. (2008). *Information Security Governance: Guidance for Information Security Managers*.

Kaban, E. I. (2009). Tata Kelola Teknologi Informasi (IT Governance*). Journal of CommIT*, Vols.3, No.1, p.1-5.

Kesumawardhani, D. R. (2012). *Evaluasi IT Governance berdasarkan COBIT 4.1 (Studi Kasus Di PT Timah (PERSERO) Tbk)*. Depok: Universitas Indonesia.

Moeller, R. R. (2013). *Executive's Guide to IT Governance: Improving Systems Processes with Service Management, COBIT, and ITIL*. New Jersey: John Wiley & Sons.

PricewaterhouseCoopers. (2006). *IT Governance in Practice: Insight from Leading CIOs.*

PricewaterhouseCoopers. (2013). *2013 Information Security Braeches Survey*.

PT Toyota Motor Manufacturing Indonesia Information Security Compliance Commitee. (2013). *Information Security Policy* (2nd Ed.). Jakarta: PT Toyota Motor Manufacturing Indonesia.

PT Toyota Motor Manufacturing Indonesia. (2014). *PT Toyota Motor Manufacturing Indonesia Company Profile 2014*.

Sari, D. P. (2013). *Peranan Auditor Internal PT Toyota Motor Manufacturing Indonesia dalam Kepatuhan Divisi Pada Pelaksanaan All Toyota Security Guideline dan Rekomendasi Audit*. Jakarta: Universitas Bakrie.

Suryana. (2010). *Metodologi Penelitian Model Praktis Kualitatif Kuantitatif*. Bandung: Universitas Pendidikan Indonesia.

Wibowo, P. M. (2008). *Analisis Tingkat Kematangan (Maturity Level) Pengawasan dan Evaluasi Kinerja Teknologi Informasi Otomasi Perpustakaan dengan COBIT (Control Objective for Information and Related Technology): Studi Kasus di Perpustakaan Universitas Indonesia*. Depok: Universitas Indonesia.

Williams, P. (2007). Executive and Board Roles in Information Security. *Journal of Information Systems and Audit Control Association*.

Lampiran 1 : Kuesioner Tingkat Harapan

KUESIONER TINGKAT HARAPAN PENERAPAN TATA KELOLA KEAMANAN INFORMASI PADA PT TOYOTA MOTOR MANUFACTURING INDONESIA

Topik penelitian ini yaitu mengenai tata kelola keamanan informasi dengan studi kasus pada PT TMMIN. Penelitian ini bertujuan untuk mengetahui hal-hal yang berkaitan dengan penerapan tata kelola keamanan informasi pada PT TMMIN, termasuk mengetahui sejauh mana tata kelola keamanan informasi yang telah diterapkan, dan mengetahui tingkat harapan penerapan tata kelola keamanan informasi pada PT TMMIN dengan berpedoman pada COBIT 5 *for Information Security*.

I. Gambaran Umum dan Tujuan Kuesioner

a. Gambaran Umum Kuesioner

Kuesioner ini terdiri dari 5 bagian. Setiap bagian mewakili sebuah proses dari domain yang termasuk dalam area tata kelola menurut COBIT *5 for Information Security*, yaitu domain *Evaluate, Direct,* and *Monitor* (EDM).

Pada setiap bagian terdapat sejumlah pertanyaan dan terdapat 2 pilihan jawaban untuk setiap pertanyaan, yaitu "Perlu" dan "Tidak Perlu".

b. Tujuan Kuesioner

Kuesioner ini bertujuan **untuk mengetahui tingkat harapan terhadap penerapan tata kelola keamanan informasi pada PT TMMIN**.

II. Instruksi Pengisian Kuesioner

Berikan tanda "O" pada salah satu pilihan jawaban.

Kuesioner

No.	Pertanyaan	Perlu	Tidak Perlu
I. Proses*: EDM01 - Ensure Governance Framework Setting and Maintenance*			
1	Sistem Tata Kelola Keamanan Informasi ditanamkan dalam sistem perusahaan		
2	Adanya jaminan *(Assurance)* atas Sistem Tata Kelola Keamanan Informasi		
3	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)		
4	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: pedoman prinsip, strategi, penilaian kepatuhan tata kelola, regulasi & hukum, budaya lingkungan, dan faktor eksternal dan internal keamanan informasi		
5	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya		
6	*Standard Process* dikembangkan untuk mencapai hasil proses (sistem tata kelola keamanan informasi ditanamkan dalam sistem perusahaan dan adanya jaminan atas sistem tersebut)		
7	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis		
8	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan		

9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses		
10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses		
II. Proses: *EDM02 - Ensure Benefits Delivery*			
1	Risiko, biaya, dan manfaat investasi keamanan informasi diseimbangkan, dikelola, dan menghasilkan nilai (*value*) yang optimal		
2	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)		
3	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: evaluasi kesesuaian strategi keamanan informasi dengan tujuan bisnis, tipe dan kriteria investasi keamanan informasi, update tipe dan kriteria investasi, *feedback* terhadap *value delivery (hasil program keamanan informasi*, strategi, dll.) keamanan informasi		
4	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya		
5	*Standard Process* dikembangkan untuk mencapai hasil proses (risiko, biaya, dan manfaat investasi keamanan informasi diseimbangkan, dikelola, dan menghasilkan nilai yang optimal)		
6	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis		

7	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan		
8	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses		
9	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses		
III. Proses: *EDM03 - Ensure Risk Optimisation*			
1	Manajemen Risiko Informasi (*Information Risk Management*) merupakan bagian dari keseluruhan Manajemen Risiko Perusahaan (*Enterprise Risk Management*)		
2	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)		
3	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: *Enterprise Key Risk Indicators*, pedoman risiko perusahaan, *mapping* KRIs perusahaan dengan KRI keamanan informasi, *Information Security Risk Acceptable Level*, kebijakan keamanan informasi, *update* kebijakan manajemen risiko keamanan informasi, *remedial action* mengenai deviasi manajemen risiko keamanan informasi		
4	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya		

5	*Standard Process* dikembangkan untuk mencapai hasil proses (*Information Risk Management* merupakan bagian dari keseluruhan *Enterprise Risk Management*)		
6	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis		
7	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan		
8	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses		
9	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses		
IV. Proses: *EDM04 - Ensure Resource Optimisation*			
1	Sumber daya keamanan informasi dioptimalisasikan		
2	Sumber daya keamanan informasi sesuai dengan kebutuhan bisnis		
3	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)		
4	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: perencanaan sumber daya yang telah disetujui, penempatan tanggung jawab untuk pengelolaan sumber daya, *update* sumber daya keamanan informasi, *remedial action* mengenai deviasi manajemen		

	sumber daya keamanan informasi		
5	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya		
6	*Standard Process* dikembangkan untuk mencapai hasil proses (sumber daya keamanan informasi dioptimalisasikan dan sesuai dengan kebutuhan bisnis)		
7	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis		
8	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan		
9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses		
10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses		
V. Proses: *EDM05 - Ensure Stakeholder Transparency*			
1	Pelaporan keamanan informasi disusun dengan tepat waktu dan akurat		
2	Para pemangku kepentingan (stakeholders) diinformasikan mengenai status keamanan informasi saat ini dan risiko informasi perusahaan		

3	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)		
4	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: evaluasi kebutuhan laporan perusahaan, pelaporan dan *channel* komunikasi keamanan informasi, dan laporan status program keamanan informasi.		
5	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya		
6	*Standard Process* dikembangkan untuk mencapai hasil proses (pelaporan keamanan informasi disusun dengan tepat waktu, akurat, dan status keamanan informasi diinformasikan kepada *stakeholder*)		
7	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis		
8	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan		
9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses		
10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses		

TERIMA KASIH ATAS PARTISIPASINYA ☺

Lampiran 2 : *Mapping Process Capability Attribute* dan *Process Capability Level* dengan Pertanyaan

	Level	*Attributes*	Pertanyaan
EDM01	1	1	1 Sistem Tata Kelola Keamanan Informasi ditanamkan dalam sistem perusahaan
			2 Adanya jaminan *(Assurance)* atas Sistem Tata Kelola Keamanan Informasi
	2	2.1	3 Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)
		2.2	4 Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: pedoman prinsip, strategi, penilaian kepatuhan tata kelola, regulasi & hukum, budaya lingkungan, dan faktor eksternal dan internal keamanan informasi
	3	3.1	5 *Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya
		3.2	6 *Standard Process* dikembangkan untuk mencapai hasil proses (sistem tata kelola keamanan informasi ditanamkan dalam sistem perusahaan dan adanya jaminan atas sistem tersebut)
	4	4.1	7 Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis
		4.2	8 Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan

	5	5.1	9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses
		5.2	10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses
EDM02	1	1	1	Risiko, biaya, dan manfaat investasi keamanan informasi diseimbangkan, dikelola, dan menghasilkan nilai (*value*) yang optimal
	2	2.1	2	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)
		2.2	3	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: evaluasi kesesuaian strategi keamanan informasi dengan tujuan bisnis, tipe dan kriteria investasi keamanan informasi, update tipe dan kriteria investasi, *feedback* terhadap *value delivery (hasil program keamanan informasi*, strategi, dll.) keamanan informasi
	3	3.1	4	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya
		3.2	5	*Standard Process* dikembangkan untuk mencapai hasil proses (risiko, biaya, dan manfaat investasi keamanan informasi diseimbangkan, dikelola, dan menghasilkan nilai yang optimal)
	4	4.1	6	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis
		4.2	7	Proses dikelola secara kuantitatif untuk

			memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan
	5	5.1	8 Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses
		5.2	9 Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses
EDM03	1	1	1 Manajemen Risiko Informasi (*Information Risk Management*) merupakan bagian dari keseluruhan Manajemen Risiko Perusahaan (*Enterprise Risk Management*)
	2	2.1	2 Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)
		2.2	3 Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: *Enterprise Key Risk Indicators*, pedoman risiko perusahaan, *mapping* KRIs perusahaan dengan KRI keamanan informasi, *Information Security Risk Acceptable Level*, kebijakan keamanan informasi, *update* kebijakan manajemen risiko keamanan informasi, *remedial action* mengenai deviasi manajemen risiko keamanan informasi
	3	3.1	4 *Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya
		3.2	5 *Standard Process* dikembangkan untuk mencapai hasil proses (*Information Risk Management* merupakan bagian dari keseluruhan *Enterprise Risk Management*)

	4	4.1	6	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis
		4.2	7	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan
	5	5.1	8	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses
		5.2	9	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses
EDM04	1	1	1	Sumber daya keamanan informasi dioptimalisasikan
			2	Sumber daya keamanan informasi sesuai dengan kebutuhan bisnis
	2	2.1	3	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)
		2.2	4	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: perencanaan sumber daya yang telah disetujui, penempatan tanggung jawab untuk pengelolaan sumber daya, *update* sumber daya keamanan informasi, *remedial action* mengenai deviasi manajemen sumber daya keamanan informasi
	3	3.1	5	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses

				sebelumnya
		3.2	6	*Standard Process* dikembangkan untuk mencapai hasil proses (sumber daya keamanan informasi dioptimalisasikan dan sesuai dengan kebutuhan bisnis)
	4	4.1	7	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis
		4.2	8	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan
	5	5.1	9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses
		5.2	10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses
EDM05	1	1	1	Pelaporan keamanan informasi disusun dengan tepat waktu dan akurat
			2	Para pemangku kepentingan (stakeholders) diinformasikan mengenai status keamanan informasi saat ini dan risiko informasi perusahaan
	2	2.1	3	Kinerja proses dikelola (direncanakan, diawasi, dan di perkirakan)
		2.2	4	Produk kerja* dikelola (diciptakan, dikontrol, dan di-*maintain*) dengan tepat *Contoh produk kerja: evaluasi kebutuhan laporan perusahaan, pelaporan dan *channel* komunikasi

				keamanan informasi, dan laporan status program keamanan informasi.
	3	3.1	5	*Standard Process* di-*maintain* untuk mendukung pengembangan dari proses sebelumnya
		3.2	6	*Standard Process* dikembangkan untuk mencapai hasil proses (pelaporan keamanan informasi disusun dengan tepat waktu, akurat, dan status keamanan informasi diinformasikan kepada *stakeholder*)
	4	4.1	7	Adanya pengukuran kinerja proses sehingga hasil pengukuran digunakan untuk memastikan bahwa kinerja proses mendukung tujuan bisnis
		4.2	8	Proses dikelola secara kuantitatif untuk memproduksi proses yang stabil, mapan, dan dapat diprediksi dengan batasan yang didefinisikan perusahaan
	5	5.1	9	Perubahan terhadap proses diidentifikasi dari analisis variasi umum dalam kinerja proses, dan dari invetigasi pendekatan inovatif terhadap definisi dan pengembangan proses
		5.2	10	Perubahan terhadap definisi, pengelolaan, dan kinerja dari hasil proses mempengaruhi pencapaian tujuan perbaikan (*improvement*) proses

Lampiran 3 : Lembar Kerja Observasi – EDM01

EDM01 - Ensure Governance Framework Setting and Maintenance						
Level	***Attribute***	**Pertanyaan**		**Diimplementasikan**	**Persentase**	***Rating***
I. *Performed Process*						
***Level* 1**	**1.1**	1	Sistem Tata Kelola Keamanan Informasi ditanamkan dalam sistem perusahaan	**Ya**	100,0%	F
		2	Adanya jaminan *(Assurance)* atas Sistem Tata Kelola Keamanan Informasi	**Ya**		
II. *Managed Process*						
***Level* 2**	**2.1**	1	Tujuan kinerja proses teridentifikasi	**Ya**	100,0%	F
		2	Kinerja proses direncanakan dan di-*monitor*	**Ya**		
		3	Kinerja proses dijalankan sesuai dengan perencanaan	**Ya**		
		4	Tanggung Jawab (*responsibilities*) dan Otorisasi (*authorities*) dalam melaksanakan proses didefiniskan, di-*assign*, dan dikomunikasikan	**Ya**		
		5	Keperluan Sumber Daya dan Informasi untuk menjalankan proses diidentifikasi, tesedia, dialokasikan, dan digunakan	**Ya**		
		6	Pertemuan antara pihak-pihak yang terlibat dalam proses, dikelola untuk memastikan adanya komunikasi yang efektif dan pemberian (assignment) tanggung jawab yang jelas	**Ya**		
	2.2	7	Kebutuhan produk kerja* dari proses terdefinisikan	**Ya**	100,0%	F
		8	Kebutuhan dokumentasi dan kontrol terhadap produk kerja* dari proses terdefiniskan	**Ya**		
		9	Produk kerja* dari proses didefinisikan, didokumentasikan, dan dikontrol secara tepat	**Ya**		

		10	Produk kerja* dari proses di-*review* sesuai dengan perencanaan dan disesuaikan seperlunya untuk memenuhi persyaratan.	**Ya**		
III. *Established Process*						
***Level* 3**	**3.1**	1	*Standard Proces* didefinisikan dengan mendeskripsikan elemen dasar yang harus disatukan kedalam proses	**Ya**	100,0%	F
		2	Urutan dan interaksi dari *Standard Process* dengan proses lainnya ditentukan	**Ya**		
		3	Kompetensi dan peran yang dibutuhkan untuk mengerjakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		4	Kebutuhan infrastruktur dan lingkungan kerja dalam melaksanakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		5	Metode yang sesuai untuk me-*monitor* efektivitas dan kesesuaian dari proses telah ditentukan	**Ya**		
	3.2	6	Proses yang telah didefinisikan dibangun berdasarkan pada S*tandard Process* yang dipilih secara tepat	**Ya**	100%	F
		7	Peran, tanggung jawab, dan otoritas yang dibutuhkan untuk menjalankan proses yang telah didefinisikan di-*assign* dan dikomunikasikan	**Ya**		
		8	Karyawan yang menjalankan proses yang telah didefiniskan memiliki kompetensi dari pendidikan, pelatihan, dan pengalaman yang sesuai	**Ya**		
		9	Kebutuhan sumber daya dan informasi yang diperlukan untuk melaksanakan proses yang telah didefinisikan tersedia, dialokasikan, dan digunakan	**Ya**		
		10	Kebutuhan infrastruktur dan lingkungan kerja untuk melaksanakan proses yang telah didefinisikan tersedia, dikelola,	**Ya**		

			dan di-*maintain*			
		11	Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami proses, untuk mendemonstrasikan kesesuaian dan efektivitas, dan untuk mengevaluasi dimana *continous improvement* dari proses harus dilakukan	**Ya**		
IV. *Predictable Process*						
***Level* 4**	**4.1**	1	Informasi dari proses yang dibutuhkan dalam mendukung tujuan bisnis telah didefinisikan	**Ya**	50,0%	P
		2	Tujuan pengukuran terhadap proses diturunkan atau berasal dari kebutuhan informasi dari proses keamanan informasi	**Ya**		
		3	Tujuan kuantitatif dari kinerja proses dalam mendukung tujuan bisnis didefinisikan	Tidak		
		4	Ukuran dan frekuensi dari pengukuran diidentifikasi dan didefinisikan sesuai dengan tujuan pengukuran proses dan tujuan kuantitatif dari kinerja proses	Tidak		
		5	Hasil pengukuran dikumpulkan, dianalisis dan dilaporkan untuk melihat sejauh mana kesesuiaan tujuan kuantitatif pada kinerja proses	Tidak		
		6	Hasil pengukuran digunakan untuk mengkarakteristikan kinerja proses	**Ya**		
	4.2	7	Teknik analisis dan kontrol ditentukan dan diaplikasikan jika *applicable*	**Ya**	40,0%	P
		8	Adanya variasi batas kontrol untuk kinerja proses normal	Tidak		
		9	Pengukuran data dianalisis untuk menangani penyebab khusus dari variasi	Tidak		
		10	*Corrective actions* diambil untuk menangani penyebab khusus dari variasi	**Ya**		
		11	Batasan kontrol ditebitkan ulang (jika perlu) untuk disesuaikan dengan *corrective actions*	Tidak		

V. *Optimizing Process*						
***Level* 5**	**5.1**	1	Tujuan *process improvement* didefinisikan dengan mendukung tujuan bisnis	**Ya**	20%	**N**
		2	Data yang tepat dianalisis untuk mengidentifikasi penyebab umum dari varisasi dalam kinerja proses	Tidak		
		3	Data yang tepat dianalisis untuk mengidentifikasi kesempatan dan menjadikannya sebagai *best practice* atau inovasi baru	Tidak		
		4	Kesempatan untuk *process improvement* diturunkan/berasal dari teknologi baru dan konsep proses yang telah diidentifikasi	Tidak		
		5	Strategi implementasi dibuat untuk mencapai tujuan *process improvement*	Tidak		
	5.2	6	Pengaruh dari seluruh perubahan yang dianjurkan untuk dinilai terhadap tujuan dari proses yang didefinisikan dan *standard process*	Tidak	0%	**N**
		7	Implementasi dari seluruh perubahaan yang telah disetujui dikelola untuk memastikan bahwa gangguan pada kinerja proses dipahami dan dikerjakan	Tidak		
		8	Berdasarkan kinerja aktual, efektivitas dari perubahan proses dievaluasi terhadap hasil kebutuhan yang didefiniskan dan tujuan untuk menentukan apakah hasilnya karena penyebab umum atau penyebab khusus	Tidak		

Keterangan	
F	*Fully Achieved*
L	*Largely Achieved*
P	*Partially Achieved*
N	*No Achieved*
	Process Capability Level Aktual

Lampiran 4 : Lembar Kerja Observasi – EDM02

EDM02 - Ensure Benefits Delivery						
Level	***Attribute***	**Pertanyaan**		**Diimplementasikan**	**Persentase**	***Rating***
I. *Performed Process*						
***Level* 1**	**1.1**	1	Resiko, biaya, dan manfaat investasi Keamanan Informasi diseimbangkan, dikelola, dan menghasilkan nilai (value) yang optimal	**Ya**	100,0%	F
II. *Managed Process*						
	2.1	1	Tujuan kinerja proses teridentifikasi	**Ya**	100,0%	F
		2	Kinerja proses direncanakan dan di-*monitor*	**Ya**		
		3	Kinerja proses dijalankan sesuai dengan perencanaan	**Ya**		
		4	Tanggung Jawab (*responsibilities*) dan Otorisasi (*authorities*) dalam melaksanakan proses didefiniskan, di-*assign*, dan dikomunikasikan	**Ya**		
		5	Keperluan Sumber Daya dan Informasi untuk menjalankan proses diidentifikasi, tesedia, dialokasikan, dan digunakan	**Ya**		
		6	Pertemuan antara pihak-pihak yang terlibat dalam proses, dikelola untuk memastikan adanya komunikasi yang efektif dan pemberian (assignment) tanggung jawab yang jelas	**Ya**		
	2.2	7	Kebutuhan produk kerja* dari proses terdefinisikan	**Ya**	100,0%	F
		8	Kebutuhan dokumentasi dan kontrol terhadap produk kerja* dari proses terdefiniskan	**Ya**		
		9	Produk kerja* dari proses didefinisikan, didokumentasikan, dan dikontrol secara tepat	**Ya**		

		10	Produk kerja* dari proses di-*review* sesuai dengan perencanaan dan disesuaikan seperlunya untuk memenuhi persyaratan.	**Ya**		
III. *Established Process*						
***Level* 3**	**3.1**	1	*Standard Proces* didefinisikan dengan mendeskripsikan elemen dasar yang harus disatukan kedalam proses	**Ya**	100,0%	F
		2	Urutan dan interaksi dari *Standard Process* dengan proses lainnya ditentukan	**Ya**		
		3	Kompetensi dan peran yang dibutuhkan untuk mengerjakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		4	Kebutuhan infrastruktur dan lingkungan kerja dalam melaksanakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		5	Metode yang sesuai untuk me-*monitor* efektivitas dan kesesuaian dari proses telah ditentukan	**Ya**		
	3.2	6	Proses yang telah didefinisikan dibangun berdasarkan pada S*tandard Process* yang dipilih secara tepat	**Ya**	100%	F
		7	Peran, tanggung jawab, dan otoritas yang dibutuhkan untuk menjalankan proses yang telah didefinisikan di-*assign* dan dikomunikasikan	**Ya**		
		8	Karyawan yang menjalankan proses yang telah didefiniskan memiliki kompetensi dari pendidikan, pelatihan, dan pengalaman yang sesuai	**Ya**		
		9	Kebutuhan sumber daya dan informasi yang diperlukan untuk melaksanakan proses yang telah didefinisikan tersedia, dialokasikan, dan digunakan	**Ya**		
		10	Kebutuhan infrastruktur dan lingkungan kerja untuk melaksanakan proses yang telah didefinisikan tersedia, dikelola, dan di-*maintain*	**Ya**		

		11	Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami proses, untuk mendemonstrasikan kesesuaian dan efektivitas, dan untuk mengevaluasi dimana *continous improvement* dari proses harus dilakukan	**Ya**		
IV. *Predictable Process*						
***Level* 4**	**4.1**	1	Informasi dari proses yang dibutuhkan dalam mendukung tujuan bisnis telah didefinisikan	**Ya**	83,3%	L
		2	Tujuan pengukuran terhadap proses diturunkan atau berasal dari kebutuhan informasi dari proses keamanan informasi	**Ya**		
		3	Tujuan kuantitatif dari kinerja proses dalam mendukung tujuan bisnis didefinisikan	**Ya**		
		4	Ukuran dan frekuensi dari pengukuran diidentifikasi dan didefinisikan sesuai dengan tujuan pengukuran proses dan tujuan kuantitatif dari kinerja proses	**Ya**		
		5	Hasil pengukuran dikumpulkan, dianalisis dan dilaporkan untuk melihat sejauh mana kesesuiaan tujuan kuantitatif pada kinerja proses	**Ya**		
		6	Hasil pengukuran digunakan untuk mengkarakteristikan kinerja proses	Tidak		
	4.2	7	Teknik analisis dan kontrol ditentukan dan diaplikasikan jika *applicable*	**Ya**	80,0%	L
		8	Adanya variasi batas kontrol untuk kinerja proses normal	**Ya**		
		9	Pengukuran data dianalisis untuk menangani penyebab khusus dari variasi	**Ya**		
		10	*Corrective actions* diambil untuk menangani penyebab khusus dari variasi	**Ya**		
		11	Batasan kontrol ditebitkan ulang (jika perlu) untuk disesuaikan dengan *corrective actions*	Tidak		

V. *Optimizing Process*						
***Level* 5**	**5.1**	1	Tujuan *process improvement* didefinisikan dengan mendukung tujuan bisnis	**Ya**	60%	P
		2	Data yang tepat dianalisis untuk mengidentifikasi penyebab umum dari varisasi dalam kinerja proses	**Ya**		
		3	Data yang tepat dianalisis untuk mengidentifikasi kesempatan dan menjadikannya sebagai *best practice* atau inovasi baru	Tidak		
		4	Kesempatan untuk *process improvement* diturunkan/berasal dari teknologi baru dan konsep proses yang telah diidentifikasi	Tidak		
		5	Strategi implementasi dibuat untuk mencapai tujuan *process improvement*	**Ya**		
	5.2	6	Pengaruh dari seluruh perubahan yang dianjurkan untuk dinilai terhadap tujuan dari proses yang didefinisikan dan *standard process*	Tidak	33%	P
		7	Implementasi dari seluruh perubahaan yang telah disetujui dikelola untuk memastikan bahwa gangguan pada kinerja proses dipahami dan dikerjakan	**Ya**		
		8	Berdasarkan kinerja aktual, efektivitas dari perubahan proses dievaluasi terhadap hasil kebutuhan yang didefiniskan dan tujuan untuk menentukan apakah hasilnya karena penyebab umum atau penyebab khusus	Tidak		

Keterangan	
F	*Fully Achieved*
L	*Largely Achieved*
P	*Partially Achieved*
N	*No Achieved*
	Process Capability Level Aktual

Lampiran 5 : Lembar Kerja Observasi – EDM03

EDM03 - Ensure Risk Optimisation						
Level	***Attribute***	**Pertanyaan**		**Diimplementasikan**	**Persentase**	***Rating***
I. *Performed Process*						
***Level* 1**	**1.1**	1	Menejemen Resiko Informasi (Information Risk management) merupakan bagian dari keseluruhan Menejemen Resiko Perusahaan (Enterprise Risk Management)	**Ya**	100,0%	F
II. *Managed Process*						
***Level* 2**	**2.1**	1	Tujuan kinerja proses teridentifikasi	**Ya**	100,0%	F
		2	Kinerja proses direncanakan dan di-*monitor*	**Ya**		
		3	Kinerja proses dijalankan sesuai dengan perencanaan	**Ya**		
		4	Tanggung Jawab (*responsibilities*) dan Otorisasi (*authorities*) dalam melaksanakan proses didefiniskan, di-*assign*, dan dikomunikasikan	**Ya**		
		5	Keperluan Sumber Daya dan Informasi untuk menjalankan proses diidentifikasi, tesedia, dialokasikan, dan digunakan	**Ya**		
		6	Pertemuan antara pihak-pihak yang terlibat dalam proses, dikelola untuk memastikan adanya komunikasi yang efektif dan pemberian (assignment) tanggung jawab yang jelas	**Ya**		
	2.2	7	Kebutuhan produk kerja* dari proses terdefinisikan	**Ya**	100,0%	F
		8	Kebutuhan dokumentasi dan kontrol terhadap produk kerja* dari proses terdefiniskan	**Ya**		
		9	Produk kerja* dari proses didefinisikan,	**Ya**		

			didokumentasikan, dan dikontrol secara tepat			
		10	Produk kerja* dari proses di-*review* sesuai dengan perencanaan dan disesuaikan seperlunya untuk memenuhi persyaratan.	**Ya**		
III. *Established Process*						
***Level* 3**	**3.1**	1	*Standard Proces* didefinisikan dengan mendeskripsikan elemen dasar yang harus disatukan kedalam proses	**Ya**	100,0%	F
		2	Urutan dan interaksi dari *Standard Process* dengan proses lainnya ditentukan	**Ya**		
		3	Kompetensi dan peran yang dibutuhkan untuk mengerjakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		4	Kebutuhan infrastruktur dan lingkungan kerja dalam melaksanakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		5	Metode yang sesuai untuk me-*monitor* efektivitas dan kesesuaian dari proses telah ditentukan	**Ya**		
	3.2	6	Proses yang telah didefinisikan dibangun berdasarkan pada S*tandard Process* yang dipilih secara tepat	**Ya**	100%	F
		7	Peran, tanggung jawab, dan otoritas yang dibutuhkan untuk menjalankan proses yang telah didefinisikan di-*assign* dan dikomunikasikan	**Ya**		
		8	Karyawan yang menjalankan proses yang telah didefiniskan memiliki kompetensi dari pendidikan, pelatihan, dan pengalaman yang sesuai	**Ya**		
		9	Kebutuhan sumber daya dan informasi yang diperlukan untuk melaksanakan proses yang telah didefinisikan tersedia, dialokasikan, dan digunakan	**Ya**		
		10	Kebutuhan infrastruktur dan lingkungan kerja untuk melaksanakan proses yang telah	**Ya**		

			didefinisikan tersedia, dikelola, dan di-*maintain*			
		11	Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami proses, untuk mendemonstrasikan kesesuaian dan efektivitas, dan untuk mengevaluasi dimana *continous improvement* dari proses harus dilakukan	**Ya**		
IV. *Predictable Process*						
***Level* 4**	**4.1**	1	Informasi dari proses yang dibutuhkan dalam mendukung tujuan bisnis telah didefinisikan	**Ya**	100,0%	F
		2	Tujuan pengukuran terhadap proses diturunkan atau berasal dari kebutuhan informasi dari proses keamanan informasi	**Ya**		
		3	Tujuan kuantitatif dari kinerja proses dalam mendukung tujuan bisnis didefinisikan	**Ya**		
		4	Ukuran dan frekuensi dari pengukuran diidentifikasi dan didefinisikan sesuai dengan tujuan pengukuran proses dan tujuan kuantitatif dari kinerja proses	**Ya**		
		5	Hasil pengukuran dikumpulkan, dianalisis dan dilaporkan untuk melihat sejauh mana kesesuiaan tujuan kuantitatif pada kinerja proses	**Ya**		
		6	Hasil pengukuran digunakan untuk mengkarakteristikan kinerja proses	**Ya**		
	4.2	7	Teknik analisis dan kontrol ditentukan dan diaplikasikan jika *applicable*	**Ya**	80,0%	L
		8	Adanya variasi batas kontrol untuk kinerja proses normal	**Ya**		
		9	Pengukuran data dianalisis untuk menangani penyebab khusus dari variasi	**Ya**		
		10	*Corrective actions* diambil untuk menangani penyebab khusus dari variasi	**Ya**		
		11	Batasan kontrol ditebitkan ulang (jika perlu) untuk disesuaikan dengan *corrective actions*	Tidak		

V. *Optimizing Process*						
***Level* 5**	**5.1**	1	Tujuan *process improvement* didefinisikan dengan mendukung tujuan bisnis	**Ya**	60%	P
		2	Data yang tepat dianalisis untuk mengidentifikasi penyebab umum dari varisasi dalam kinerja proses	**Ya**		
		3	Data yang tepat dianalisis untuk mengidentifikasi kesempatan dan menjadikannya sebagai *best practice* atau inovasi baru	Tidak		
		4	Kesempatan untuk *process improvement* diturunkan/berasal dari teknologi baru dan konsep proses yang telah diidentifikasi	Tidak		
		5	Strategi implementasi dibuat untuk mencapai tujuan *process improvement*	**Ya**		
	5.2	6	Pengaruh dari seluruh perubahan yang dianjurkan untuk dinilai terhadap tujuan dari proses yang didefinisikan dan *standard process*	Tidak	33%	P
		7	Implementasi dari seluruh perubahaan yang telah disetujui dikelola untuk memastikan bahwa gangguan pada kinerja proses dipahami dan dikerjakan	**Ya**		
		8	Berdasarkan kinerja aktual, efektivitas dari perubahan proses dievaluasi terhadap hasil kebutuhan yang didefiniskan dan tujuan untuk menentukan apakah hasilnya karena penyebab umum atau penyebab khusus	Tidak		

Keterangan	
F	*Fully Achieved*
L	*Largely Achieved*
P	*Partially Achieved*
N	*No Achieved*
	Process Capability Level Aktual

Lampiran 6 : Lembar Kerja Observasi – EDM04

EDM04 - Ensure Resource Optimisation						
Level	***Attribute***	**Pertanyaan**		**Diimplementasikan**	**Persentase**	***Rating***
I. *Performed Process*						
	1.1	1	Sumber Daya Keamanan Informasi dioptimalisasikan	**Ya**	100,0%	F
		2	Sumber Daya Keamanan Informasi sesuai dengan kebutuhan bisnis	**Ya**		
II. *Managed Process*						
***Level* 2**	**2.1**	1	Tujuan kinerja proses teridentifikasi	**Ya**	100,0%	F
		2	Kinerja proses direncanakan dan di-*monitor*	**Ya**		
		3	Kinerja proses dijalankan sesuai dengan perencanaan	**Ya**		
		4	Tanggung Jawab (*responsibilities*) dan Otorisasi (*authorities*) dalam melaksanakan proses didefiniskan, di-*assign*, dan dikomunikasikan	**Ya**		
		5	Keperluan Sumber Daya dan Informasi untuk menjalankan proses diidentifikasi, tesedia, dialokasikan, dan digunakan	**Ya**		
		6	Pertemuan antara pihak-pihak yang terlibat dalam proses, dikelola untuk memastikan adanya komunikasi yang efektif dan pemberian (assignment) tanggung jawab yang jelas	**Ya**		
	2.2	7	Kebutuhan produk kerja* dari proses terdefinisikan	**Ya**	100,0%	F
		8	Kebutuhan dokumentasi dan kontrol terhadap produk kerja* dari proses terdefiniskan	**Ya**		
		9	Produk kerja* dari proses didefinisikan, didokumentasikan, dan dikontrol secara tepat	**Ya**		

		10	Produk kerja* dari proses di-*review* sesuai dengan perencanaan dan disesuaikan seperlunya untuk memenuhi persyaratan.	**Ya**		
III. *Established Process*						
***Level* 3**	**3.1**	1	*Standard Proces* didefinisikan dengan mendeskripsikan elemen dasar yang harus disatukan kedalam proses	**Ya**	100,0%	F
		2	Urutan dan interaksi dari *Standard Process* dengan proses lainnya ditentukan	**Ya**		
		3	Kompetensi dan peran yang dibutuhkan untuk mengerjakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		4	Kebutuhan infrastruktur dan lingkungan kerja dalam melaksanakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		5	Metode yang sesuai untuk me-*monitor* efektivitas dan kesesuaian dari proses telah ditentukan	**Ya**		
	3.2	6	Proses yang telah didefinisikan dibangun berdasarkan pada S*tandard Process* yang dipilih secara tepat	**Ya**	100%	F
		7	Peran, tanggung jawab, dan otoritas yang dibutuhkan untuk menjalankan proses yang telah didefinisikan di-*assign* dan dikomunikasikan	**Ya**		
		8	Karyawan yang menjalankan proses yang telah didefiniskan memiliki kompetensi dari pendidikan, pelatihan, dan pengalaman yang sesuai	**Ya**		
		9	Kebutuhan sumber daya dan informasi yang diperlukan untuk melaksanakan proses yang telah didefinisikan tersedia, dialokasikan, dan digunakan	**Ya**		
		10	Kebutuhan infrastruktur dan lingkungan kerja untuk melaksanakan proses yang telah didefinisikan tersedia, dikelola, dan di-*maintain*	**Ya**		

		11	Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami proses, untuk mendemonstrasikan kesesuaian dan efektivitas, dan untuk mengevaluasi dimana *continous improvement* dari proses harus dilakukan	**Ya**		
IV. *Predictable Process*						
***Level* 4**	**4.1**	1	Informasi dari proses yang dibutuhkan dalam mendukung tujuan bisnis telah didefinisikan	**Ya**	100,0%	F
		2	Tujuan pengukuran terhadap proses diturunkan atau berasal dari kebutuhan informasi dari proses keamanan informasi	**Ya**		
		3	Tujuan kuantitatif dari kinerja proses dalam mendukung tujuan bisnis didefinisikan	**Ya**		
		4	Ukuran dan frekuensi dari pengukuran diidentifikasi dan didefinisikan sesuai dengan tujuan pengukuran proses dan tujuan kuantitatif dari kinerja proses	**Ya**		
		5	Hasil pengukuran dikumpulkan, dianalisis dan dilaporkan untuk melihat sejauh mana kesesuiaan tujuan kuantitatif pada kinerja proses	**Ya**		
		6	Hasil pengukuran digunakan untuk mengkarakteristikan kinerja proses	**Ya**		
	4.2	7	Teknik analisis dan kontrol ditentukan dan diaplikasikan jika *applicable*	**Ya**	60,0%	P
		8	Adanya variasi batas kontrol untuk kinerja proses normal	**Ya**		
		9	Pengukuran data dianalisis untuk menangani penyebab khusus dari variasi	Tidak		
		10	*Corrective actions* diambil untuk menangani penyebab khusus dari variasi	**Ya**		
		11	Batasan kontrol ditebitkan ulang (jika perlu) untuk disesuaikan dengan *corrective actions*	Tidak		

V. *Optimizing Process*						
***Level* 5**	**5.1**	1	Tujuan *process improvement* didefinisikan dengan mendukung tujuan bisnis	**Ya**	60%	P
		2	Data yang tepat dianalisis untuk mengidentifikasi penyebab umum dari varisasi dalam kinerja proses	**Ya**		
		3	Data yang tepat dianalisis untuk mengidentifikasi kesempatan dan menjadikannya sebagai *best practice* atau inovasi baru	Tidak		
		4	Kesempatan untuk *process improvement* diturunkan/berasal dari teknologi baru dan konsep proses yang telah diidentifikasi	Tidak		
		5	Strategi implementasi dibuat untuk mencapai tujuan *process improvement*	**Ya**		
	5.2	6	Pengaruh dari seluruh perubahan yang dianjurkan untuk dinilai terhadap tujuan dari proses yang didefinisikan dan *standard process*	Tidak	33%	P
		7	Implementasi dari seluruh perubahaan yang telah disetujui dikelola untuk memastikan bahwa gangguan pada kinerja proses dipahami dan dikerjakan	**Ya**		
		8	Berdasarkan kinerja aktual, efektivitas dari perubahan proses dievaluasi terhadap hasil kebutuhan yang didefiniskan dan tujuan untuk menentukan apakah hasilnya karena penyebab umum atau penyebab khusus	Tidak		

Keterangan	
F	*Fully Achieved*
L	*Largely Achieved*
P	*Partially Achieved*
N	*No Achieved*
	Process Capability Level Aktual

Lampiran 7 : Lembar Kerja Observasi – EDM05

EDM03 - Ensure Resource Optimisation					
Level	***Attribute***	**Pertanyaan**	**Diimplementasikan**	**Persentase**	***Rating***
I. *Performed Process*					
***Level* 1**	**1.1**	1 Pelaporan Keamanan Informasi disusun secara lengkap, tepat waktu dan akurat	**Ya**	100,0%	F
		2 Para pemangku kepentingan (stakeholders) diinformasikan mengenai status keamanan informasi saat ini dan risiko informasi perusahaan	**Ya**		
II. *Managed Process*					
***Level* 2**	**2.1**	1 Tujuan kinerja proses teridentifikasi	**Ya**	100,0%	F
		2 Kinerja proses direncanakan dan di-*monitor*	**Ya**		
		3 Kinerja proses dijalankan sesuai dengan perencanaan	**Ya**		
		4 Tanggung Jawab (*responsibilities*) dan Otorisasi (*authorities*) dalam melaksanakan proses didefiniskan, di-*assign*, dan dikomunikasikan	**Ya**		
		5 Keperluan Sumber Daya dan Informasi untuk menjalankan proses diidentifikasi, tesedia, dialokasikan, dan digunakan	**Ya**		
		6 Pertemuan antara pihak-pihak yang terlibat dalam proses, dikelola untuk memastikan adanya komunikasi yang efektif dan pemberian (assignment) tanggung jawab yang jelas	**Ya**		
	2.2	7 Kebutuhan produk kerja* dari proses terdefinisikan	**Ya**	100,0%	F
		8 Kebutuhan dokumentasi dan kontrol terhadap produk kerja* dari proses terdefiniskan	**Ya**		

		9	Produk kerja* dari proses didefinisikan, didokumentasikan, dan dikontrol secara tepat	**Ya**		
		10	Produk kerja* dari proses di-*review* sesuai dengan perencanaan dan disesuaikan seperlunya untuk memenuhi persyaratan.	**Ya**		
III. *Established Process*						
***Level* 3**	**3.1**	1	*Standard Proces* didefinisikan dengan mendeskripsikan elemen dasar yang harus disatukan kedalam proses	**Ya**	100,0%	F
		2	Urutan dan interaksi dari *Standard Process* dengan proses lainnya ditentukan	**Ya**		
		3	Kompetensi dan peran yang dibutuhkan untuk mengerjakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		4	Kebutuhan infrastruktur dan lingkungan kerja dalam melaksanakan proses diidentifikasi sebagai bagian dari *Standard Process*	**Ya**		
		5	Metode yang sesuai untuk me-*monitor* efektivitas dan kesesuaian dari proses telah ditentukan	**Ya**		
	3.2	6	Proses yang telah didefinisikan dibangun berdasarkan pada S*tandard Process* yang dipilih secara tepat	**Ya**	100%	F
		7	Peran, tanggung jawab, dan otoritas yang dibutuhkan untuk menjalankan proses yang telah didefinisikan di-*assign* dan dikomunikasikan	**Ya**		
		8	Karyawan yang menjalankan proses yang telah didefiniskan memiliki kompetensi dari pendidikan, pelatihan, dan pengalaman yang sesuai	**Ya**		

		9	Kebutuhan sumber daya dan informasi yang diperlukan untuk melaksanakan proses yang telah didefinisikan tersedia, dialokasikan, dan digunakan	**Ya**		
		10	Kebutuhan infrastruktur dan lingkungan kerja untuk melaksanakan proses yang telah didefinisikan tersedia, dikelola, dan di-*maintain*	**Ya**		
		11	Data yang tepat dikumpulkan dan dianalisis sebagai dasar untuk memahami proses, untuk mendemonstrasikan kesesuaian dan efektivitas, dan untuk mengevaluasi dimana *continous improvement* dari proses harus dilakukan	**Ya**		
IV. *Predictable Process*						
***Level* 4**	**4.1**	1	Informasi dari proses yang dibutuhkan dalam mendukung tujuan bisnis telah didefinisikan	**Ya**	50,0%	P
		2	Tujuan pengukuran terhadap proses diturunkan atau berasal dari kebutuhan informasi dari proses keamanan informasi	**Ya**		
		3	Tujuan kuantitatif dari kinerja proses dalam mendukung tujuan bisnis didefinisikan	Tidak		
		4	Ukuran dan frekuensi dari pengukuran diidentifikasi dan didefinisikan sesuai dengan tujuan pengukuran proses dan tujuan kuantitatif dari kinerja proses	Tidak		
		5	Hasil pengukuran dikumpulkan, dianalisis dan dilaporkan untuk melihat sejauh mana kesesuiaan tujuan kuantitatif pada kinerja proses	Tidak		
		6	Hasil pengukuran digunakan untuk mengkarakteristikan kinerja proses	**Ya**		
	4.2	7	Teknik analisis dan kontrol	**Ya**	20,0%	N

			ditentukan dan diaplikasikan jika *applicable*		
		8	Adanya variasi batas kontrol untuk kinerja proses normal	Tidak	
		9	Pengukuran data dianalisis untuk menangani penyebab khusus dari variasi	Tidak	
		10	*Corrective actions* diambil untuk menangani penyebab khusus dari variasi	Tidak	
		11	Batasan kontrol ditebitkan ulang (jika perlu) untuk disesuaikan dengan *corrective actions*	Tidak	
V. *Optimizing Process*					
***Level* 5**	**5.1**	1	Tujuan *process improvement* didefinisikan dengan mendukung tujuan bisnis	**Ya**	20%	N
		2	Data yang tepat dianalisis untuk mengidentifikasi penyebab umum dari varisasi dalam kinerja proses	Tidak		
		3	Data yang tepat dianalisis untuk mengidentifikasi kesempatan dan menjadikannya sebagai *best practice* atau inovasi baru	Tidak		
		4	Kesempatan untuk *process improvement* diturunkan/berasal dari teknologi baru dan konsep proses yang telah diidentifikasi	Tidak		
		5	Strategi implementasi dibuat untuk mencapai tujuan *process improvement*	Tidak		
	5.2	6	Pengaruh dari seluruh perubahan yang dianjurkan untuk dinilai terhadap tujuan dari proses yang didefinisikan dan *standard process*	Tidak	0%	N
		7	Implementasi dari seluruh perubahaan yang telah disetujui dikelola untuk memastikan bahwa gangguan pada kinerja proses dipahami dan dikerjakan	Tidak		

		8	Berdasarkan kinerja aktual, efektivitas dari perubahan proses dievaluasi terhadap hasil kebutuhan yang didefiniskan dan tujuan untuk menentukan apakah hasilnya karena penyebab umum atau penyebab khusus	Tidak		

Keterangan	
F	*Fully Achieved*
L	*Largely Achieved*
P	*Partially Achieved*
N	*No Achieved*
	Process Capability Level Aktual

Lampiran 8 : Daftar Pertanyaan Wawancara

Narasumber: ISCC *Member* – PiC Internal Audit dan Former Reviewer ATSG

a. Hal apa saja yang memicu terbentuknya tata kelola keamanan informasi?
- PT TMMIN telah mendapat predikat sebagai perusahaan Toyota dengan Kategori 1 yang artinya bahwa PT TMMIN memiliki jumlah investasi yang tinggi dan merupakan afiliasi Toyota yang mempunyai pengaruh yang penting. Proyek-proyek investasi besar mulai dieksekusi sehingga diwajibkan oleh TMC untuk melindungi aset informasi agar informasi tidak bocor. Informasi rahasia yang bocor dapat mempengaruhi daya saing perusahaan dan kepercayaan TMC untuk memberikan model baru.
- Adanya insiden keamanan informasi yang dialami PT TMMIN, yaitu *hacking* yang dilakukan oleh karyawan

b. Regulasi dan hukum apa yang mempengaruhi tata kelola keamanan informasi perusahaan?
- PKB (Perjanjian Kerja Bersama)
- *IT Policy*
- *Information Management Policy*

c. Bagaimana alur penyampaian/ *feedback* keamanan informasi? Apakah ada fasilitas untuk menampung *feedback* yang langsung ke BoD?
- Jika ada *feedback*, yang bersangkutan menyampaikannya melalui PiC ATSG yang ada disetiap Divisi, lalu disampaikan ke anggota ISCC, setelah itu disampaikan ke *Leader* ISCC, baru pesan akan disampaikan selanjutnya ke Direktur dan BoD.
- Untuk saat ini, belum ada *whistle-blowing* program yang khusus untuk ATSG

d. *Framework* apa yang dijadikan sebagai pedoman implementasi ATSG?
- *Framework* ATSG yang dirancang oleh TMC. Selain itu, ISO 27001:2005 dan COBIT 3 juga dijadikan referensi dalam pelaksanaan ATSG

e. Kontrol apa saja yang dipakai atau yang dirujuk dari ISO 27001:2005 atau COBIT 3?
- Untuk ISO 27001:2005: hanya mengadopsi konsep P-D-C-A (*Plan Design Check Act*)
- COBIT 3 dijadikan referensi untuk ITGC (*IT General Control*) yang merupakan kontrol yang digunakan untuk mencapai SOX *Compliance*. ATSG juga mendukung ITGC untuk mencapai SOX *Compliance*.

f. Bagaimana sistem pelaporan ATSG kepada *stakeholder*?

- Setiap 4 bulan sekali, ATSG melaporkan progress keamanan informasi.
- Pelaporan kepada *BoD* melalui *BoD Meeting*
- Pelaporan kepada para Division Head melalui Division Head Forum
- Selain itu, setiap 4 bulan sekali juga diadakan pertemuan antar anggota ISCC

g. Bagaimana peran BoD dalam pelaksanaan ATSG?

- BoD mendukung penuh ATSG bahkan ATSG atau keamanan informasi dijadikan sebagai salah satu poin di *Company Hoshin* (strategi jangka panjang perusahaan)
- BoD selalu mengawasi penerapan ATSG

h. Apakah ada *Key Risk Indicator* (KRI) Kemanan Informasi atau KRI Perusahaan pada PT TMMIN?

- KRI ada disetiap Divisi. Setiap Divisi wajib memiliki KRI masing-masing. Kumpulan KRI itu lah yang merupakan KRI Perusahaan
- Untuk KRI mengenai keamanan informasi belum menjadi kesatuan, terpencar di beberapa Divisi, seperti di GAD, di ISTD.

Lampiran 9 : *Template* Proses-Proses EDM

Process ID	EDM01		
Process Name	Ensure Governance Framework Setting and Maintenance		
Process Description	Analyse and articulate the requirements for the governance of enterprise IT, and put in place and maintain effective enabling structures, principles, processes and practices, with clarity of responsibilities and authority to achieve the enterprise's mission, goals and objectives.		
Process Purpose Statement	Provide a consistent approach integrated and aligned with the enterprise governance approach. To ensure that IT-related decisions are made in line with the enterprise's strategies and objectives, ensure that IT-related processes are overseen effectively and transparently, compliance with legal and regulatory requirements are confirmed, and the governance requirements for board members are met.		
Outcomes (Os)			
Number	**Description**		
EDM01 - O1	The information security governance system is embedded in the enterprise.		
EDM01 - O2	Assurance is obtained over the information security governance system.		
Base Practices (BPs)			
Number	**Description**		**Supports**
EDM01 - BP1	**Evaluate the governance system** Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and make judgement on the current and future design of governance of enterprise IT.		EDM01 - O1
EDM01 - BP2	**Direct the governance system** Inform leadership and obtain their support, buy-in and commitment. Guide the structures, processes, and practices for the governance of IT in line with agreed-on governance design principles, decisionmaking models and authority levels. Define the information required for informed decision		EDM01 - O1
EDM01 - BP3	**Monitor the governance system** Monitor the effectiveness and performance of the enterprise's governance of IT. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of IT.		EDM01 - O2
Work Products (WPs)			
Inputs			
Number	**Description**		**Supports**
Outside COBIT 5 for Information Security	Internal and external environmental factors (legal, regulatory, and contractual obligations) and trends		EDM01 - BP1 EDM01 - O1
EDM01 - WP1	Information security guiding principles		EDM01 - BP2 EDM01 - O1
APO02 - WP5	Information security strategy		EDM01 - BP2 EDM01 - O1
Outside COBIT 5 for Information Security	Information security-related legislation and regulation		EDM01 - BP3 EDM01 - O2
Outputs			
Number	**Description**	**Input to**	**Supports**
EDM01 - WP1	Information security guiding principles	EDM01.02 APO01.01 APO01.03 APO01.04 APO02.01 APO02.05 APO12.03	EDM01 - BP1 EDM01 - O1
EDM01 - WP2	Information security-positive culture and environment	Internal	EDM01 - BP2 EDM01 - O2
EDM01 - WP3	Governance compliance assessment	Internal	EDM01 - BP3 EDM01 - O2

Process ID	EDM02		
Process Name	Ensure Benefits Delivery		
Process Description	Optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs.		
Process Purpose Statement	Secure optimal value from IT-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.		
Outcomes (Os)			
Number	**Description**		
EDM02 - O1	Benefits, costs and risk of information security investments are balanced and managed and contribute optimal value.		
Base Practices (BPs)			
Number	**Description**		**Supports**
EDM02 - BP1	**Evaluate value optimisation** Continually evaluate the portfolio of IT-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value at a reasonable cost. Identify and make judgement on any changes in direction that need to be given to management to optimise value creation.		EDM02 - O1
EDM02 - BP2	**Direct value optimisation.** Direct value management principles and practices to enable optimal value realisation from IT-enabled investments throughout their full economic life cycle.		EDM02 - O1
EDM02 - BP3	**Monitor value optimisation.** Monitor the key goals and metrics to determine the extent to which the business is generating the expected value and benefits to the enterprise from IT-enabled investments and services. Identify significant issues and consider corrective actions.		EDM02 - O1
Work Products (WPs)			
Inputs			
Number	**Description**		**Supports**
Outside COBIT 5 for Information Security	Evaluation of strategic alignment		EDM02 - BP1 EDM02 - O1
Outside COBIT 5 for Information Security	Investment types and criteria		EDM02 - BP2 EDM02 - O1
Outputs			
Number	**Description**	**Input to**	**Supports**
EDM02 - WP1	Update portfolio	Internal	EDM02 - BP1 EDM02 - O1
EDM02 - WP2	Update investement types and criteria	Internal	EDM02 - BP2 EDM02 - O1
EDM02 - WP3	Feedback on value delivery of information security initiatives	Internal	EDM02 - BP3 EDM02 - O1

Process ID	EDM03
Process Name	Ensure Risk Optimisation
Process Description	Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed.
Process Purpose Statement	Ensure that IT-related enterprise risk does not exceed risk appetite and risk tolerance, the impact of IT risk to enterprise value is identified and managed, and the potential for compliance failures is minimised.

Outcomes (Os)

Number	Description
EDM03 - O1	Information risk management is part of overall enterprise risk management (ERM).

Base Practices (BPs)

Number	Description	Supports
EDM03 - BP1	**Evaluate risk management.** Continually examine and make judgement on the effect of risk on the current and future use of IT in the enterprise. Consider whether the enterprise's risk appetite is appropriate and that risk to enterprise value related to the use of IT is identified and managed.	EDM03 - O1
EDM03 - BP2	**Direct risk management.** Direct the establishment of risk management practices to provide reasonable assurance that IT risk management practices are appropriate to ensure that the actual IT risk does not exceed the board's risk appetite.	EDM03 - O1
EDM03 - BP3	**Monitor risk management.** Monitor the key goals and metrics of the risk management processes and establish how deviations or problems will be identified, tracked and reported on for remediation.	EDM03 - O1

Work Products (WPs)

Inputs

Number	Description	Supports
Outside COBIT 5 for Information Security	- Enterprise Key Risk Indicator (KRIs) - Enterprise risk appetite guidance	EDM03 - BP1 EDM03 - O1
EDM03 - WP1	Alignment of enterprise KRIs with information security KRIs	EDM03 - BP2 EDM03 - O1
EDM03 - WP2	Information security risk acceptable level	EDM03 - BP2/3 EDM03 - O1
APO01 - WP3	Information security and related policy	EDM03 - BP3 EDM03 - O2

Outputs

Number	Description	Input to	Supports
EDM03 - WP1	Alignment of enterprise KRIs with information security KRIs	EDM03.02	EDM02 - BP1 EDM02 - O1
EDM03 - WP2	Information security risk acceptable level	EDM03.02 EDM03.03	EDM03 - BP1 EDM03 - O1
EDM03 - WP3	Update risk management policies	Internal	EDM03 - BP2 EDM03 - O1
EDM03 - WP4	Remedial actions to address risk management deviations	Internal	EDM03 - BP3 EDM03 - O1

Process ID	EDM04		
Process Name	Ensure Resource Optimisation		
Process Description	Ensure that adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost.		
Process Purpose Statement	Ensure that the resource needs of the enterprise are met in the optimal manner, IT costs are optimised, and there is an increased likelihood of benefit realisation and readiness for future change.		
Outcomes (Os)			
Number	**Description**		
EDM04 - O1	Information security resources are optimised.		
EDM04 - O2	Information security resources are in alignment with business requirements.		
Base Practices (BPs)			
Number	**Description**		**Supports**
EDM04 - BP1	**Evaluate resource management.** Continually examine and make judgement on the current and future need for IT-related resources, options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.		EDM04 - O1
EDM04 - BP2	**Direct resource management.** Ensure the adoption of resource management principles to enable optimal use of IT resources throughout their full economic life cycle.		EDM04 - O2
EDM04 - BP3	**Monitor resource management.** Monitor the key goals and metrics of the resource management processes and establish how deviations or problems will be identified, tracked and reported for remediation.		
Work Products (WPs)			
Inputs			
Number	**Description**		**Supports**
Outside COBIT 5 for Information Security	Approved resource plan		EDM04 - BP1 EDM04 - O1
Outside COBIT 5 for Information Security	Assigned responsibilities for resource management		EDM04 - BP2 EDM04 - O2
Outputs			
Number	**Description**	**Input to**	**Supports**
EDM03 - WP1	Updated information security resources	Internal	EDM04 - BP1/2 EDM04 - O1/O2
EDM03 - WP2	Remedial actions to address resource management deviations	Internal	EDM04 - BP3 EDM04 - O2

Process ID	EDM05
Process Name	Ensure Stakeholder Transparency
Process Description	Ensure that enterprise IT performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and the necessary remedial actions.
Process Purpose Statement	Make sure that the communication to stakeholders is effective and timely and the basis for reporting is established to increase performance, identify areas for improvement, and confirm that IT-related objectives and strategies are in line with the enterprise's strategy.

Outcomes (Os)

Number	Description
EDM05 - O1	Information security reporting is established and is complete, timely, and accurate.
EDM05 - O2	Stakeholders are informed of the current status of information security and information risk across the enterprise.

Base Practices (BPs)

Number	Description	Supports
EDM05 - BP1	**Evaluate stakeholder reporting requirements.** Continually examine and make judgement on the current and future requirements for stakeholder communication and reporting, including both mandatory reporting requirements (e.g., regulatory) and communication to other stakeholders. Establish the principles for communication.	EDM05 - O1
EDM05 - BP2	**Direct stakeholder communication and reporting.** Ensure the establishment of effective stakeholder communication and reporting, including mechanisms for ensuring the quality and completeness of information, oversight of mandatory reporting, and creating a communication strategy for stakeholders.	EDM05 - O2
EDM05 - BP3	**Monitor stakeholder communication.** Monitor the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability, and effectiveness, and ascertain whether the requirements of different stakeholders are met.	

Work Products (WPs)

Inputs

Number	Description	Supports
Outside COBIT 5 for Information Security	Evaluation of enterprise reporting requirements	EDM05 - BP1 EDM05 - O1

Outputs

Number	Description	Input to	Supports
EDM05 - WP1	Information security reporting requirements and communication channels	Internal	EDM05 - BP1 EDM05 - O1
EDM05 - WP2	Information security status reports	Internal	EDM05 - BP2 EDM05 - O2
EDM05 - WP3	Information security monitoring and reporting	Internal	EDM05 - BP3 EDM05 - O2