Sebutkan beberapa jenis framework untuk IT Risk Management

1. Penetapan Objektif
Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.

2. Identifikasi Resiko
Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :
- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal(dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya

3. Penilaian Resiko
Proses untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko (tabel 2.2). Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

4. Respon Resiko
Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima (acceptable risks), maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 Control Objectives) yang sesuai untuk manajemen resiko adalah :
- PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
- AI6 (Manages Change)
- DS5 (Ensure System and Security) dan DS11 (Manage Data)
- ME1 (Monitor and Evaluate IT Performance)

5. **Monitor Resiko**
Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.

Nama : RANI OKTA FELANI

NIM : 192420048

Beberapa Jenis Framework untuk IT Risk Management.

1. COBIT
2. ITIL
3. ISO 17799
4. ISO 27000
5. ISO/IEC 38500
6. COSO

Berikut ini adalah standar atau *framework* yang paling banyak digunakan dalam pengembangan Manajemen Teknik Informasi :

COBIT

COBIT yang merupakan singkatan dari *Control Objectives for Information and Related Technology*, dimiliki dan didukung oleh ISACA. Pertamakali di luncurkan pada tahun 1996 sebagai COBIT. Versi yang terbaru saat ini adalah COBIT 2019 namun hingga saat ini COBIT 5 masih digunakan secara luas sebagai framework TI untuk Tata Kelola TI. Di mana COBIT 5 merupakan gabungan dari framework COBIT 4.1, VAL IT 2.0, dan Risk IT.

COBIT merupakan framework TI yang digunakan untuk membantu kita dalam mengoptimalisasikan*value* atau nilai suatu organisasi enterprise melalui TI dengan cara menjaga keseimbangan antara realisasi keuntungan, optimalisasi risiko, dan pemanfaatan sumberdaya. Kerangka kerja TI ini mengcover baik bisnis maupun unit TI dalam keseluruhan organisasi. Memberikan model maturity atau model kematangan proses dan metriknya untuk mengukur apakah organisasi TI telah mencapai tujuannya. Sebagai tambahan, COBIT juga menjaga keseimbangan antara kebutuhan stakeholder baik internal maupun eksternal.

ITIL

ITIL, singkatan dari *Information Technology Infrastructure Library*, merupakan seperangkat *guideline*(petunjuk) dan best practices untuk kebutuhan IT Service Management (ITSM) atau Manajemen Layanan Teknologi Informasi (MLTI). Merupakan framework TI yang dikeluarkan oleh AXELOS Limited. ITIL fokus pada penyelarasan IT services atau layanan TI sesuai kebutuhan bisnis dan mendukung proses inti. Terdiri dari lima volume : *Service Strategy*, *Service Design*, *Service Transition*,*Service Operation and Continual Service Improvement*.

Kerangka kerja TI seperti ITIL ini dapat di adaptasi dan diaplikasikan kepada seluruh jenis bisnis dan lingkungan organisasi. Meliputi pentunjuk untuk identifikasi, perencanaan, delivering, dan supporting layanan TI. Jika sukses di adopsi makan ITIL dapat meningkatkan kualitas layanan, dan pada gilirannya dapat menjadi alat mitigasi bagi risiko bisnis dan disrupsi layanan, meningkatkan hubungan dengan pelanggan, dan membuat suatu sistem yang efektif secara biaya bagi pengelolaan kebutuhan terhadap layanan.

CMMI

Framework CMMI merupakan singkatan dari *Capability Maturity Model Integration*, merupakan model yang sudah terkenal secara global sebagai model referensi yang dikembangkan melalui best practices yang memberikan petunjuk untuk meningkatkan proses yang dapat memenuhi target bisnis dari suatu organisasi. Model ini dikembangkan oleh pakar di industri, pemerintahan, dan*Software Engineering Institute* (SEI).

CMMI meningkatkan proses suatu organisiasi dengan menunjukkan keuntungan terukur dari tujuan bisnis dan visinya. Suatu organisasi dapat mengorganisasikan dan memprioritaskan metodologi, SDM, dan aktivitas bisnisnya melalui kerangka kerja yang diberikan oleh CMMI. Kerangka kerja ini mendukung koordinasi antar aktivitas yang multidisiplin dan pemikiran yang sistematis.

PMBOK

Kepanjangan dari PMBOK adalah *Guide to the Project Management Body of Knowledge*, adalah suatu guideline yang secara internasioal diakui untuk digunakan sebagai metode manajemen proyek dan merupakan produk dari PMI (*Project Management Institute*), PMBOK adalah standar yang secara luas diterima dan diakui sebagai basis untuk keseluruhan metode manajemen proyek.

PMBOK memberikan deskripsi yang mendalam mengenai isi dan pokok-pokok yang secara fundamental membahas mengenai manajemen proyek, namun fokusnya tidak pada soalan mengenai saran implementasi teknis. Berkaitan

dengan petunjuk praktis justru diberikan oleh kerangka yang lain seperti PRINCE2. Pada intinya PMBOK terdiri dari 5 proses dasar : Initiating, Planning, Executing, Controlling and Monitoring, and Closing.

PRINCE2

PRINCE2 merupakan singkatan dari *Projects IN a Controlled Environment*, merupakan standar de facto untuk metode manajemen proyekyang dimiliki oleh UK Cabinet Office. PRINCE2 merupakan komplemen dari model PMBOK dengan menyediakan petunjuk yang sifat berbasis proses dan praktis berikut dengan template yang siap digunakan oleh Manajer Proyek dan *Group Project Steering* untuk setiap fase yang berbeda dari proyek. PRINCE2 memastikan kontrol yang lebih besar terhadap sumberdaya serta manajemen yang efektif terhadap risiko bisnis dan proyek.

Sebagai contoh, tujuh prinsip dari PRINCE2 menyatakan bahwa proyek harus dijalankan melalui suatu proses siklus berikut : proyek harus memiliki justifikasi bisnis, definisi yang jelas untuk setiap peran dan tanggungjawab pada setiap fase dan proses, dikelola dalam bentuk tahapan yang detil dan terjadwal, definisi toleransi untuk setiap pengecualian dalam menajemen proyek, fokus pada menghasilkan produk sesuai dengan kebutuhan proyek, dan belajar dari pengalaman untuk peningkatan kualitas organisasi dalam mengelola proyek berikutnya.

ISO/IEC 20000

ISO/IEC 20000 adalah *Service Management System* (SMS) atau sistem manajemen layanan merupakan standarisasi internasional untuk manajemen layanan TI. Dimiliki oleh International Organization for Standardization (ISO) dan the International Electrotechnical Commission (IEC) dan secara umum selaras dengan ITIL.

ISO/IEC 20000 memiliki dua bagian. Bagian pertama mendefinisikan kebutuhan formal dari produksi berkualitas tinggi terhadap layanan kepada bisnis. TI yang meliputi kriteria perencanaan, manajemen layanan, dan produksi layanan dan juga manajemen pelanggan. Bagian kedua menjelaskan proses dari produksi layanan yang secara umum sama dengan proses ITIL yang secara umum memfokuskan pada proses manajemen pelanggan.

ISO 21500

ISO 21500 adalah standar yang secara generik merupakan petunjuk mengenai konsep dan proyek dari manajemen proyek yang merupakan bagian terpenting dalam realisasi proyek yang sukses. Dapat digunakan untuk seluruh jenis organisasi dan dapat diterapkan apda setiap jenis proyek, tanpa terkendala ukuran, kompleksitas, dan durasi.

ISO 21500 adalah standar informal secara umum lebih merupakan guideline ketimbang metodologi yang bersertifikasi. Menyediakan deskripsi *high level* terhadap konsep dan proses yang selama ini diangap sebagai good practices dalam manajemen proyek dan menempatkna proyek dalam konteks program dan portofolio proyek. PMBOK secara umum memiliki kesesuaian dengan ISO 21500 begitu juga sebaliknya.

ISO/IEC 38500

ISO/IEC 38500 merupakan standar yang memberikan prinsip umum mengenai peran dan manejemen IT governance dengan tanggungjawab bisnis (contoh : BoD dan tim manajemen). Dapat digunakan secara luas untuk semua jenis dan ukuran organisasi baik perusahaan privat maupun publik termasuk organisasi non profit.

Standar ini mendukung manajemen bisnis dalam melaksanakan supervisi terhadap organisasi TI dan membantunya memastikan bahwa TI memberikan dampak positif terhadap kinerja perusahaan. Di mana standart terdiri dari 6 prinsip, sebagai berikut :

1. *Responsibility*
2. *Strategy*
3. *Acquisition*
4. *Performance*

5. *Conformance*
6. *Human behaviour*

Selain itu ISO/IEC 38500 juga menjamin bahwa manajemen telah melaksanakan konformitas dengan implementasi tata kelola organisasi yang baik (*good overnance*).

TOGAF

TOGAF adalah kerangka kerja enterprise architecture dari *Open Group Standard* yang memungkinkan setiap organisasi memiliki pendekatan terstruktur untuk pengelolaan implementasi teknologi, secara khusus dalam desain teknologi perangkat lunak, pengembangannya, dan peratawatan. Dipublikasikan tahun 1995 berdasarkan *US Department of Defence Technical Architecture Framework for Information Management* (TAFIM). Kemudian dikembangkan oleh *The Open Group Architecture Forum* dan kemudian secara reguler dirilis di website Open Group.

TOGAF meningkatkan efisiensi bisnis dengan cara memastikannya melalui metode yang konsisten, komunikasi, pemanfaatan sumberdaya yang efisien. Meningkatkan kredibiltias industri dengan bahasa yang umum di kalangan profesional *enterprise architecture*.

ISO/IEC 27001

ISO/IEC 27001 merupakan standarisasi untuk ISMS (Information Security Management System) yang isinya merupakan pedoman pentunjuk dan prosedur praktis pengelolaan Sistem Manajemen Keamanan Informasi. ISO27001 lebih memfokuskan diri pada aspek manajemen pelaksanaan. Dimana output dokumennya merinci hingga detil aktivitas keamanan yang mesti dilakukan. Namun demikian proses implementasi maupun aktivitas audit keamanan sistem informasi sebenarnya bersifat fleksibel tergantung pada tipe dan kebutuhan organisasi serta fokus dan *concern* mereka pada proses bisnis dan proses TI-nya seturut dengan tujuan dan strategis perusahaan.

Framework adalah kerangka kerja yang berfungsi untuk membentuk pondasi sebuah software process dengan mengidentifikasi beberapa aktivitas framework yang dapat dipakai untuk untuk semua projek software tanpa memperhatikan ukuran atau kerumitan mereka.

Beberapa Jenis Framwork Untuk ItnRisk Managemen yaitu :

- *Information Technology Infrastructure Library* (ITIL)
- *Control Objectives for Information and Related Technology* (COBIT)
- *International Organization for Standardization* (ISO)
- *Capability Maturity Model Integration* (CMMI)
- *Sarbanes-Oxley (SoX)*
- *Committee of Sponsoring Organization of the Treadway Commision* (COSO)

Jenis-jenis Framework untuk IT Risk Management, terdiri dari :

1. COBIT 5
2. ISACA
3. PMBOK
4. ISO 31000: 2018

1. Penetapan Objektif
2. Identifikasi Resiko
3. Penilaian Resiko
4. Respon Resiko
5. Monitor Resiko

1. COSO
2. ISACA
3. ISO 31000
4. ISO 27005

Beberapa *framework* risiko yang dikenal di dunia IT antara lain *Risk IT* – ISACA, COSO, ISO 31000, ISO 27005 dan *framework* lain yang digunakan untuk IT.

Pendekataan IT oleh ISACA dikenal dengan 3 domain pengelolaan resiko, terkait dengan *Governance*, Evaluasi dan Respon. Ketiga domain ini dikombinasikan dan dikomunikasikan untuk bisa mengelola resiko.

Framework lain yang cukup terkenal adalah *COSO* dengan delapan pengelolaan komponen risiko, konteksnya adalah terkait dengan sifat dasar strategic, operasional, operasional dan compliance komponen tersebut dikelola berdasarkan level-level disisi enterprise atau sampai bisnis unit proses.

Berikut ini adalah standar atau *framework* dalam IT Risk Management

COBIT

COBIT yang merupakan singkatan dari *Control Objectives for Information and Related Technology*, dimiliki dan didukung oleh ISACA. Pertamakali di luncurkan pada tahun 1996 sebagai COBIT. Versi yang terbaru saat ini adalah COBIT 2019 namun hingga saat ini COBIT 5 masih digunakan secara luas sebagai framework TI untuk Tata Kelola TI. Di mana COBIT 5 merupakan gabungan dari framework COBIT 4.1, VAL IT 2.0, dan Risk IT.

ITIL

ITIL, singkatan dari *Information Technology Infrastructure Library*, merupakan seperangkat *guideline* (petunjuk) dan best practices untuk kebutuhan IT Service Management (ITSM) atau Manajemen Layanan Teknologi Informasi (MLTI). Merupakan framework TI yang dikeluarkan oleh AXELOS Limited. ITIL fokus pada penyelarasan IT services atau layanan TI sesuai kebutuhan bisnis dan mendukung proses inti. Terdiri dari lima volume : *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation and Continual Service Improvement*.

CMMI

Framework CMMI merupakan singkatan dari *Capability Maturity Model Integration*, merupakan model yang sudah terkenal secara global sebagai model referensi yang dikembangkan melalui best practices yang memberikan petunjuk untuk meningkatkan proses yang dapat memenuhi target bisnis dari suatu organisasi. Model ini dikembangkan oleh pakar di industri, pemerintahan, dan *Software Engineering Institute* (SEI).

PMBOK

Kepanjangan dari PMBOK adalah *Guide to the Project Management Body of Knowledge*, adalah suatu guideline yang secara internasioal diakui untuk digunakan sebagai metode manajemen proyek dan merupakan produk dari PMI (*Project Management Institute*), PMBOK adalah standar yang secara luas diterima dan diakui sebagai basis untuk keseluruhan metode manajemen proyek.

PMBOK memberikan deskripsi yang mendalam mengenai isi dan pokok-pokok yang secara fundamental membahas mengenai manajemen proyek, namun fokusnya tidak pada soalan mengenai saran implementasi teknis. Berkaitan dengan petunjuk praktis justru diberikan oleh kerangka yang lain seperti PRINCE2. Pada intinya PMBOK terdiri dari 5 proses dasar : Initiating, Planning, Executing, Controlling and Monitoring, and Closing.

PRINCE2

PRINCE2 merupakan singkatan dari *Projects IN a Controlled Environment*, merupakan standar de facto untuk metode manajemen proyekyang dimiliki oleh UK Cabinet Office. PRINCE2 merupakan komplemen dari model PMBOK dengan menyediakan petunjuk yang sifat berbasis proses dan praktis berikut dengan template yang siap digunakan oleh Manajer Proyek dan *Group Project Steering* untuk setiap fase yang berbeda dari proyek. PRINCE2 memastikan kontrol yang lebih besar terhadap sumberdaya serta manajemen yang efektif terhadap risiko bisnis dan proyek.

ISO/IEC 20000

ISO/IEC 20000 adalah *Service Management System* (SMS) atau sistem manajemen layanan merupakan standarisasi internasional untuk manajemen layanan TI. Dimiliki oleh International Organization for Standardization (ISO) dan the International Electrotechnical Commission (IEC) dan secara umum selaras dengan ITIL.

ISO 21500

ISO 21500 adalah standar yang secara generik merupakan petunjuk mengenai konsep dan proyek dari manajemen proyek yang merupakan bagian terpenting dalam realisasi proyek yang sukses. Dapat digunakan untuk seluruh jenis organisasi dan dapat diterapkan apda setiap jenis proyek, tanpa terkendala ukuran, kompleksitas, dan durasi.

ISO/IEC 38500

ISO/IEC 38500 merupakan standar yang memberikan prinsip umum mengenai peran dan manejemen IT governance dengan tanggungjawab bisnis (contoh : BoD dan tim manajemen). Dapat digunakan secara luas untuk semua jenis dan ukuran organisasi baik perusahaan privat maupun publik termasuk organisasi non profit.

TOGAF

TOGAF adalah kerangka kerja enterprise architecture dari *Open Group Standard* yang memungkinkan setiap organisasi memiliki pendekatan terstruktur untuk pengelolaan implementasi teknologi, secara khusus dalam desain teknologi perangkat lunak, pengembangannya, dan peratawatan. Dipublikasikan tahun 1995 berdasarkan *US Department of Defence Technical Architecture Framework for Information Management* (TAFIM). Kemudian dikembangkan oleh *The Open Group Architecture Forum* dan kemudian secara reguler dirilis di website Open Group.

ISO/IEC 27001

ISO/IEC 27001 merupakan standarisasi untuk ISMS (Information Security Management System) yang isinya merupakan pedoman pentunjuk dan prosedur praktis pengelolaan Sistem Manajemen Keamanan Informasi. ISO27001 lebih memfokuskan diri pada aspek manajemen pelaksanaan. Dimana output dokumennya merinci hingga detil aktivitas keamanan yang mesti dilakukan. Namun demikian proses implementasi maupun aktivitas audit keamanan sistem informasi sebenarnya bersifat fleksibel tergantung pada tipe dan kebutuhan organisasi serta fokus dan *concern* mereka pada proses bisnis dan proses TI-nya seturut dengan tujuan dan strategis perusahaan.

Resiko adalah segala hal yang mungkin berdampak pada kemampuan organisasi dalam mencapai tujuantujuannya. Framework manajemen resiko TI dengan menggunakan COBIT terdiri dari :

1. **Penetapan Objektif**

Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu :
effectiveness,
efficiency,
confidentiality,
integrity,
availability,
compliance,
dan reliability.

2. **Identifikasi Resiko**

Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :

- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal(dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya (lihat tabel event diatas).

3. **Penilaian Resiko**

Proses untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko (tabel 2.2). Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

Sedangkan kecenderungan (likelihood) terjadinya resiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan (inherent risks) dan sisa resiko (residual risks).

4. **Respon Resiko**

Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima (acceptable risks), maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 Control Objectives) yang sesuai untuk manajemen resiko adalah :

- PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
- AI6 (Manages Change)
- DS5 (Ensure System and Security) dan DS11 (Manage Data)
- ME1 (Monitor and Evaluate IT Performance)

5. **Monitor Resiko**

Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.

COBIT

COBIT merupakan framework TI yang digunakan untuk membantu kita dalam mengoptimalisasikan *value* atau nilai suatu organisasi enterprise melalui TI dengan cara menjaga keseimbangan antara realisasi keuntungan, optimalisasi risiko, dan pemanfaatan sumberdaya. COBIT juga menjaga keseimbangan antara kebutuhan stakeholder baik internal maupun eksternal.

ITIL

Merupakan framework TI yang dikeluarkan oleh AXELOS Limited. ITIL fokus pada penyelarasan IT services atau layanan TI sesuai kebutuhan bisnis dan mendukung proses inti. Terdiri dari lima volume : *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation and Continual Service Improvement*.

CMMI

CMMI meningkatkan proses suatu organisiasi dengan menunjukkan keuntungan terukur dari tujuan bisnis dan visinya. Suatu organisasi dapat mengorganisasikan dan memprioritaskan metodologi, SDM, dan aktivitas bisnisnya melalui kerangka kerja yang diberikan oleh CMMI. Kerangka kerja ini mendukung koordinasi antar aktivitas yang multidisiplin dan pemikiran yang sistematis.

PMBOK

PMBOK memberikan deskripsi yang mendalam mengenai isi dan pokok-pokok yang secara fundamental membahas mengenai manajemen proyek, namun fokusnya tidak pada soalan mengenai saran implementasi teknis. Berkaitan dengan petunjuk praktis justru diberikan oleh kerangka yang lain seperti PRINCE2. Pada intinya PMBOK terdiri dari 5 proses dasar : Initiating, Planning, Executing, Controlling and Monitoring, and Closing.

PRINCE2

PRINCE2 merupakan komplemen dari model PMBOK dengan menyediakan petunjuk yang sifat berbasis proses dan praktis berikut dengan template yang siap digunakan oleh Manajer Proyek dan *Group Project Steering* untuk setiap fase yang berbeda dari proyek. PRINCE2 memastikan kontrol yang lebih besar terhadap sumberdaya serta manajemen yang efektif terhadap risiko bisnis dan proyek.

ISO/IEC 20000

ISO/IEC 20000 memiliki dua bagian. Bagian pertama mendefinisikan kebutuhan formal dari produksi berkualitas tinggi terhadap layanan kepada bisnis. TI yang meliputi kriteria perencanaan, manajemen layanan, dan produksi layanan dan juga manajemen pelanggan. Bagian kedua menjelaskan proses dari produksi layanan yang secara umum sama dengan proses ITIL yang secara umum memfokuskan pada proses manajemen pelanggan.

ISO 21500

ISO 21500 adalah standar yang secara generik merupakan petunjuk mengenai konsep dan proyek dari manajemen proyek yang merupakan bagian terpenting dalam realisasi proyek yang sukses. Dapat digunakan untuk seluruh jenis organisasi dan dapat diterapkan apda setiap jenis proyek, tanpa terkendala ukuran, kompleksitas, dan durasi.

ISO/IEC 38500

ISO/IEC 38500 merupakan standar yang memberikan prinsip umum mengenai peran dan manejemen IT governance dengan tanggungjawab bisnis (contoh : BoD dan tim manajemen). Dapat digunakan secara luas untuk semua jenis dan

ukuran organisasi baik perusahaan privat maupun publik termasuk organisasi non profit.

TOGAF

TOGAF adalah kerangka kerja enterprise architecture dari *Open Group Standard* yang memungkinkan setiap organisasi memiliki pendekatan terstruktur untuk pengelolaan implementasi teknologi, secara khusus dalam desain teknologi perangkat lunak, pengembangannya, dan peratawatan. TOGAF meningkatkan efisiensi bisnis dengan cara memastikannya melalui metode yang konsisten, komunikasi, pemanfaatan sumberdaya yang efisien. Meningkatkan kredibiltias industri dengan bahasa yang umum di kalangan profesional *enterprise architecture*.

ISO/IEC 27001

ISO/IEC 27001 merupakan standarisasi untuk ISMS (Information Security Management System) yang isinya merupakan pedoman pentunjuk dan prosedur praktis pengelolaan Sistem Manajemen Keamanan Informasi. ISO27001 lebih memfokuskan diri pada aspek manajemen pelaksanaan. Dimana output dokumennya merinci hingga detil aktivitas keamanan yang mesti dilakukan. Namun demikian proses implementasi maupun aktivitas audit keamanan sistem informasi sebenarnya bersifat fleksibel tergantung pada tipe dan kebutuhan organisasi serta fokus dan *concern* mereka pada proses bisnis dan proses TI-nya seturut dengan tujuan dan strategis perusahaan.

Framework manajemen resiko TI dengan menggunakan COBIT terdiri dari :

1. **Penetapan Objektif**

Kriteria informasi dari COBIT dapat digunakan sebagai dasar dalam mendefinisikan objektif TI. Terdapat tujuh kriteria informasi dari COBIT yaitu : effectiveness, efficiency, confidentiality, integrity, availability, compliance, dan reliability.

2. **Identifikasi Resiko**

Identifikasi resiko merupakan proses untuk mengetahui resiko. Sumber resiko bisa berasal dari :

- Manusia, proses dan teknologi
- Internal (dari dalam perusahaan) dan eksternal(dari luar perusahaan)
- Bencana (hazard), ketidakpastian (uncertainty) dan kesempatan (opportunity).

Dari ketiga sumber resiko tersebut dapat diketahui kejadian-kejadian yang dapat mengganggu perusahaan dalam mencapai objektifnya

3. **Penilaian Resiko**

Proses untuk menilai seberapa sering resiko terjadi atau seberapa besar dampak dari resiko. Dampak resiko terhadap bisnis (business impact) bisa berupa : dampak terhadap financial, menurunnya reputasi disebabkan sistem yang tidak aman, terhentinya operasi bisnis, kegagalan aset yang dapat dinilai (sistem dan data), dan penundaan proses pengambilan keputusan.

Sedangkan kecenderungan (likelihood) terjadinya resiko dapat disebabkan oleh sifat alami dari bisnis, struktur dan budaya organisasi, sifat alami dari sistem (tertutup atau terbuka, teknologi baru dan lama), dan kendali-kendali yang ada. Proses penilaian resiko bisa berupa resiko yang tidak dapat dipisahkan (inherent risks) dan sisa resiko (residual risks).

4. **Respon Resiko**

Untuk melakukan respon terhadap resiko adalah dengan menerapkan kontrol objektif yang sesuai dalam melakukan manajemen resiko. Jika sisa resiko masih melebihi resiko yang dapat diterima (acceptable risks), maka diperlukan respon resiko tambahan. Proses-proses pada framework COBIT (dari 34 Control Objectives) yang sesuai untuk manajemen resiko adalah :

- PO1 (Define a Stretegic IT Plan) dan PO9 (Assess and Manage Risks)
- AI6 (Manages Change)
- DS5 (Ensure System and Security) dan DS11 (Manage Data)
- ME1 (Monitor and Evaluate IT Performance)

5. **Monitor Resiko**

Setiap langkah dimonitor untuk menjamin bahwa resiko dan respon berjalan sepanjang waktu.

Framework adalah kerangka kerja yang berfungsi untuk membentuk pondasi sebuah software process dengan mengidentifikasi beberapa aktivitas framework yang dapat dipakai untuk untuk semua projek software tanpa memperhatikan ukuran atau kerumitan mereka.

Beberapa Jenis Framwork Untuk ItnRisk Managemen yaitu :

- *Information Technology Infrastructure Library* (ITIL)
- *Control Objectives for Information and Related Technology* (COBIT)
- *International Organization for Standardization* (ISO)
- *Capability Maturity Model Integration* (CMMI)
- *Sarbanes-Oxley (SoX)*
- *Committee of Sponsoring Organization of the Treadway Commision* (COSO)