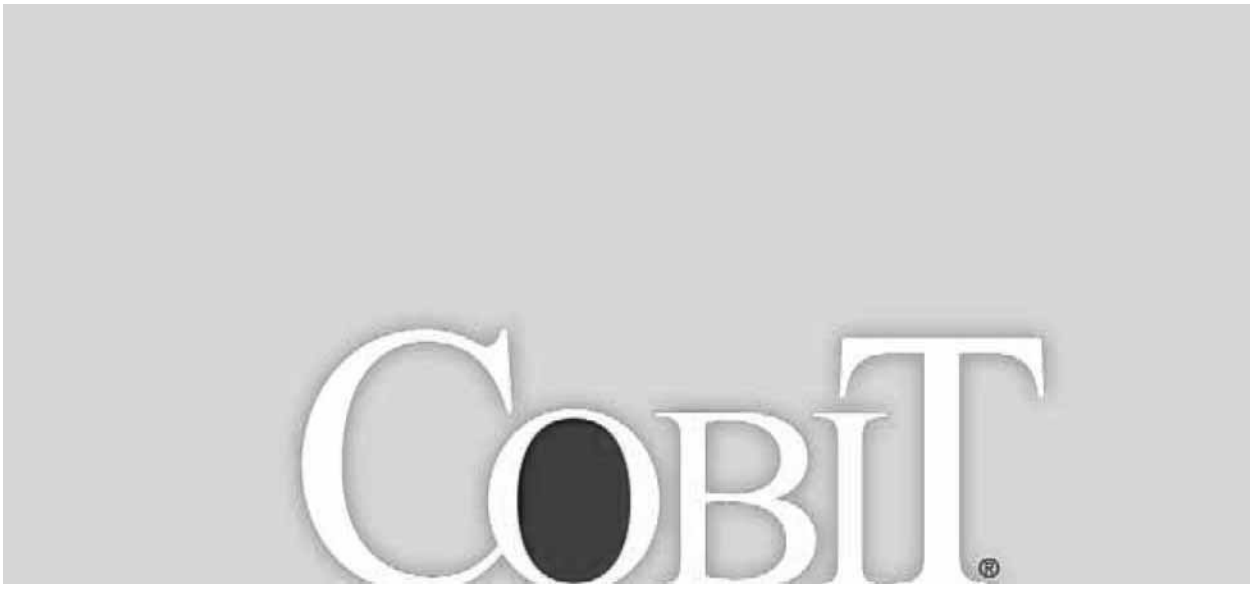
GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY



4.1

Kerangka

C ontrol TUJUAN

M anajemen uidelines G

M aturity odels M

C

Institut IT Governance®

IT Governance Institute (ITGI™) *(www.itgi.org)* didirikan pada tahun 1998 untuk memajukan pemikiran dan standar internasional dalam mengarahkan dan mengendalikan teknologi informasi sebuah perusahaan. tata kelola TI yang efektif membantu memastikan bahwa TI mendukung tujuan bisnis, mengoptimalkan investasi bisnis di IT, dan tepat mengelola risiko dan peluang yang berkaitan dengan IT. ITGI menawarkan penelitian asli, sumber daya elektronik dan studi kasus untuk membantu para pemimpin perusahaan dan dewan direksi dalam tanggung jawab pengelolaan TI mereka.

Penolakan

ITGI ("Pemilik") telah dirancang dan dibuat publikasi ini, berjudul COBIT® 4.1 (yang "Kerja"), terutama sebagai sumber pendidikan bagi petugas chief informasi (CIO), manajemen senior, manajemen dan kontrol IT profesional. Pemilik tidak membuat klaim bahwa penggunaan salah Kerja akan menjamin hasil yang sukses. Kerja tidak harus dianggap termasuk setiap informasi yang tepat, prosedur dan tes atau eksklusif informasi lainnya, prosedur dan tes yang cukup diarahkan untuk memperoleh hasil yang sama. Dalam menentukan kepatutan dari setiap informasi yang spesifik, prosedur atau tes, CIO, manajemen senior, manajemen dan kontrol TI profesional harus menerapkan pertimbangan profesional mereka sendiri dengan keadaan spesifik yang disajikan oleh sistem tertentu atau lingkungan TI.

Institut IT Governance
3701 Algonquin Road, Suite 1010 di Rolling
Meadows, IL 60.008 USA Telepon:
+1.847.590.7491 Fax: +1.847.253.1443
E-mail: *info@itgi.org*

Situs web: *www.itgi.org*

ISBN 1-933284-72-2 COBIT®
4.1
Dicetak di Amerika Serikat

SEBUAH CKNOWLEDGEMENTS

IT Governance Institute ingin mengenali:

Ahli Pengembang dan Reviewer

Mark Adler, CISA, CISM, CIA, CISSP, Allstate Ins. Co, USA Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSC, PBA, Solvay Business School, Belgia Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA Gary S. Baker, CA, Deloitte & Touche, Kanada David H. Barnett, CISM, CISSP, Applera Corp, USA Christine Bellino, CPA, CITP, Jefferson Wells, Amerika Serikat

John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Kantor Negara Auditor, USA Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgia Don Canilglia, CISA, CISM, USA

Luis A. Capua, CISM, Sindicatura General de la Nacion, Argentina Boyd Carter, PMP, Elegantsolutions.ca, Kanada Dan Casciano, CISA, Ernst & Young LLP, USA
Sean V. Casey, CISA, CPA, USA Sushil Chatterji, EduTech, Singapura

Edward Chavannes, CISA, CISSP, Ernst & Young LLP, USA Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA Beverly G. Davis, CISA, federal Home Loan Bank of San Francisco, Amerika Serikat Peter De Bruyne, CISA, Banksys, Belgia

Steven De Haes, University of Antwerp Management School, Belgia Peter De Koninck, CISA, CFSA, CIA, SC SWIFT, Belgia Philip De Picker, CISA, MCA, National Bank of Belgium, Belgia Kimberly de Vries, CISA, PMP, Zurich Financial Services , USA Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA Zama Dlamini, Deloitte & Touche LLP, Afrika Selatan Rupert Dodds, CISA, CISM, FCA, KPMG, Selandia Baru Troy DuMoulin, pink Elephant, Kanada

Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Kanada Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Swiss Christopher Fox, ACA, PricewaterhouseCoopers, USA Bob Frelinger, CISA, Sun Microsystems Inc., USA Zhiwei Fu, Ph. D, Fannie Mae, USA Monique Garsoux, Dexia Bank, Belgia Edson Gin, CISA, CFE , SSCP, USA

Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgia Gary Hardy, Pemenang IT, Afrika Selatan Jimmy Heschl, CISA, CISM, KPMG, Austria

Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp, USA Tom Hughes, ketajaman Alliance, Australia Monica Jain, CSQA, Covansys Corp, AS

Wayne D. Jones, CISA, Kantor Audit Nasional Australia, Australia John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Sistem Pengendalian dan Keamanan Inc, USA Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgia Linda Kostic, CISA, CPA, USA

John W. Lainhart IV, CISA, CISM, IBM, USA Philip Le Grand, Kapita Layanan Pendidikan, UK.
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc, USA Kenny K. Lee, CISA, CISSP, Countrywide SMART Tata Kelola, USA Debbie Lew, CISA, Ernst & Young LLP, USA

SEBUAH CKNOWLEDGEMENTS *CONT.*

Donald Lorete, CPA, Deloitte & Touche LLP, USA Addie CP Lui, MCSA, MCSE, Pertama Hawaii Bank, USA Debra Mallette, CISA, CSSBB, Kaiser Permanente, USA Charles Mansour, CISA, Charles Mansour Audit & Service Risiko, UK Mario Micallef , CPAA, FIA, Australia Grup Bank Nasional, Australia Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark

John Mitchell, CISA, CFE, CITP, FBCS, FIIA, Miia, QiCA, LHS Bisnis Control, UK Anita Montgomery, CISA, CIA, Countrywide, USA Karl Muise, CISA, National City Bank, USA

Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp, USA Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA Ed O'Donnell, Ph.D., CPA, University of Kansas, Amerika Serikat Sue Owen, Departemen Urusan Veteran, Australia

Robert G. Parker, CISA, CA, CMC, FCA, Robert G. Parker Consulting, Kanada Robert Payne, Jasa Trencor (Pty) Ltd, Afrika Selatan Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA Vitor Prisca, CISM, Novabase, Portugal

Martin Rosenberg, Ph.D., IT Business Management, UK Claus Rosenquist, CISA, TrygVesata, Denmark Jaco Sadie, Sasol, Afrika Selatan
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA Chad Smith, Great-West Life, Kanada

Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd, UK Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgia Robert E. Stroud, CA Inc, USA

Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, Kota Phoenix IT Divisi Audit, USA Wim Van Grembergen, Ph.D., University of Sekolah Manajemen Antwerp, Belgia Johan Van Grieken, CISA, Deloitte, Belgia Greet Volders, Voquals NV, Belgia Thomas M. Wagner, Gartner Inc, USA

Robert M. Walters, CISA, CPA, CGA, Kantor Pengawas Keuangan Umum, Kanada Freddy Withagels, CISA, Capgemini, Belgia Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Kanada Amanda Xu, CISA, PMP, KPMG LLP , USA

ITGI Dewan Pengawas
Everett C. Johnson, CPA, Deloitte & Touche LLP (pensiun), Amerika Serikat, Presiden International Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgia, Wakil Presiden William C. Boni, CISM, Motorola, Amerika Serikat, Wakil Presiden
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd, India, Wakil Presiden Jean-Louis Leignel, MAGE Conseil, Perancis, Wakil Presiden Lucio Augusto Molina Focazzio, CISA, Kolombia, Wakil Presiden Howard Nicholson, CISA, Kota Salisbury, Australia, Wakil Presiden

Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, PKC, CFSA, Focus Strategic Group, Hong Kong, Wakil Presiden Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past President International Robert S. Roussey, CPA, University of Southern California, Amerika Serikat, Past President International Ronald Saull, CSP, besar-Barat hidup dan IGM Keuangan, Kanada, Trustee

Komite Tata IT
Tony Hayes, FCPA, Pemerintah Queensland, Australia, Ketua Max Blecher, Virtual Alliance, Afrika Selatan Sushil Chatterji, EduTech, Singapura

Anil Jogani, CISA, FCA, Tally Solusi Limited, UK John W. Lainhart IV, CISA, CISM, IBM, USA Rómulo Lomparte, CISA, Banco de Crédito BCP, Peru Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria Ronald Saull, CSP, Life assurance besar-Barat dan IGM Keuangan, Kanada

C OBI Komite Pengarah T
Roger Debreceny, Ph.D., FCPA, University of Hawaii, USA, Ketua Gary S. Baker, CA, Deloitte & Touche, Kanada Dan Casciano, CISA, Ernst & Young LLP, USA

Steven De Haes, University of Antwerp Management School, Belgia Peter De Koninck, CISA, CFSA, CIA, SC SWIFT, Belgia Rafael Eduardo Fabius, CISA, República AFAP SA, Uruguay Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life , Swiss

Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgia Gary Hardy, Pemenang IT, Afrika Selatan Jimmy Heschl, CISA, CISM, KPMG, Austria Debbie A. Lew, CISA, Ernst & Young LLP, USA

Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia Dirk Steuperaert, CISA, PricewaterhouseCoopers LLC, Belgia Robert E. Stroud, CA Inc, USA

ITGI Advisory Panel
Ronald Saull, CSP, besar-Barat Life Assurance dan IGM Keuangan, Kanada, Ketua Roland Bader, F. Hoffmann-La Roche AG, Swiss Linda Betz, IBM Corporation, USA Jean-Pierre Corniou, Renault, Perancis Rob Clyde, CISM, Symantec , USA

Richard Granger, NHS Menghubungkan untuk Kesehatan, UK Howard Schmidt, CISM, R & H Keamanan Consulting LLC, USA Alex Siow Yuen Khong, StarHub Ltd, Singapura Amit Yoran, Yoran Associates, USA

ITGI Afiliasi dan Sponsor
bab ISACA
Institut Amerika untuk Akuntan Publik ASIS International

Pusat Internet Security
Commonwealth Asosiasi Corporate Governance FIDA Menginformasikan

Forum Keamanan Informasi
Asosiasi Keamanan Sistem Informasi Institut de la Gouvernance des Systèmes d'Informasi Institut Akuntan Manajemen ISACA ITGI Jepang

Solvay Business School
University of Antwerp Management School Aldion Consulting Pte. LTE. CA

Hewlett-Packard IBM

LogLogic Inc.
Solusi Phoenix Bisnis dan Proses Systems Inc
Symantec Corporation Wolcott Group LLC Dunia Lulus IT

C

T MAMPU OF C ONTENTS

Ikhtisar eksekutif. . . . . **5 C OBI T Kerangka**. . . . . 9 Rencana dan Mengatur. . . . . 29 Acquire dan Melaksanakan. . . . . 73 Memberikan dan Dukungan. . . . . 101 Memantau dan Mengevaluasi. . . . . 153 Lampiran I-Tabel Menghubungkan Tujuan dan Proses. . . . . 169 Lampiran II-Pemetaan **IT Proses untuk IT Governance Fokus Area, COSO, C OBI T Resources IT dan C OBI Kriteria T Informasi**. . . . . 173 Lampiran III-Maturity Model Pengendalian Intern. . . . . 175 Lampiran **IV-C OBI T 4.1 Reference Material Primer**. . . . . **177 Lampiran V-Cross-referensi Antara C OBI T 3rd Edition dan C OBI T 4.1**. . . . . **179 Lampiran VI-Pendekatan Penelitian dan Pengembangan**. . . . . 187 Lampiran VII-Istilah. . . . . 189 **Lampiran VIII-C OBI T dan Produk Terkait**. **195**

Masukan Anda pada C OBI T 4.1 disambut. Silahkan kunjungi *www.isaca.org/cobitfeedback* untuk mengirimkan komentar.

E XECUTIVE HAI khtisar

E XECUTIVE HAI khtisar

Bagi banyak perusahaan, informasi dan teknologi yang mendukungnya mewakili mereka yang paling berharga, tetapi sering paling sedikit dipahami, aset. perusahaan yang sukses mengakui keunggulan teknologi informasi dan menggunakannya untuk mendorong nilai stakeholder mereka. perusahaan ini juga memahami dan mengelola risiko yang terkait, seperti meningkatkan kepatuhan terhadap peraturan dan ketergantungan kritis banyak proses bisnis pada teknologi informasi (TI).

Kebutuhan untuk jaminan tentang nilai TI, manajemen risiko yang berkaitan dengan IT dan meningkatnya kebutuhan untuk kontrol atas informasi sekarang dipahami sebagai elemen kunci dari tata kelola perusahaan. Nilai, risiko dan pengendalian merupakan inti dari tata kelola TI.

IT governance merupakan tanggung jawab eksekutif dan dewan direksi, dan terdiri dari kepemimpinan, struktur organisasi dan proses yang memastikan bahwa perusahaan ini IT menopang dan memperluas strategi dan tujuan organisasi.

Selanjutnya, IT terintegrasi pemerintahan dan melembagakan praktek-praktek yang baik untuk memastikan bahwa perusahaan adalah IT mendukung tujuan bisnis. tata kelola TI memungkinkan perusahaan untuk mengambil keuntungan penuh dari informasinya, sehingga memaksimalkan manfaat, memanfaatkan peluang dan mendapatkan keunggulan kompetitif. hasil ini memerlukan kerangka kerja untuk kontrol atas TI yang sesuai dengan dan mendukung Committee of Sponsoring Organizations of the Treadway Commission (COSO ini) *Pengendalian Internal-Terpadu Framework,* kerangka kontrol diterima secara luas untuk pemerintahan perusahaan dan manajemen risiko, dan kerangka kerja compliant serupa.

Organisasi harus memenuhi kualitas, persyaratan fidusia dan keamanan informasi mereka, seperti untuk semua aset. Manajemen juga harus mengoptimalkan penggunaan sumber daya yang tersedia TI, termasuk aplikasi, informasi, infrastruktur dan orang-orang. Untuk menjalankan tanggung jawab ini, serta untuk mencapai tujuannya, manajemen harus memahami status arsitektur enterprise untuk IT dan memutuskan apa tata kelola dan kontrol harus menyediakan.

Tujuan pengendalian bagi informasi dan teknologi terkait (C OBI T®, memberikan praktek yang baik di seluruh domain dan kerangka proses dan menyajikan kegiatan dalam struktur dikelola dan logis. C OBI praktek yang baik T mewakili konsensus para ahli. Mereka sangat terfokus pada kontrol, kurang pada eksekusi. Praktik-praktik ini akan membantu mengoptimalkan investasi IT-enabled, memastikan pengiriman layanan dan memberikan ukuran terhadap yang untuk menilai ketika sesuatu yang salah.

Untuk IT untuk menjadi sukses dalam memberikan terhadap kebutuhan bisnis, manajemen harus menempatkan sistem pengendalian internal atau kerangka di tempat. C OBI Kerangka T kontrol kontribusi untuk kebutuhan tersebut dengan:

- Membuat link dengan kebutuhan bisnis
- Menyelenggarakan kegiatan TI menjadi model proses yang berlaku umum
- Mengidentifikasi sumber daya utama TI untuk menjadi leveraged
- Mendefinisikan tujuan pengendalian manajemen untuk dipertimbangkan

Orientasi bisnis C OBI T terdiri dari menghubungkan tujuan bisnis dengan tujuan IT, menyediakan metrik dan model kedewasaan untuk mengukur prestasi mereka, dan mengidentifikasi tanggung jawab terkait bisnis dan proses IT pemilik.

Proses Fokus C OBI T digambarkan oleh model proses yang membagi TI menjadi empat domain dan 34 proses sejalan dengan bidang tanggung jawab merencanakan, membangun, menjalankan dan memantau, menyediakan end-to-end pandangan IT. Perusahaan konsep arsitektur membantu mengidentifikasi sumber daya penting bagi keberhasilan proses, yaitu, aplikasi, informasi, infrastruktur dan orang-orang.

Singkatnya, untuk memberikan informasi bahwa perusahaan perlu untuk mencapai tujuannya, sumber daya TI harus dikelola oleh serangkaian proses dikelompokkan secara alami.

Tapi bagaimana perusahaan mendapatkan IT di bawah kontrol sedemikian rupa sehingga memberikan informasi kebutuhan perusahaan? Bagaimana cara mengelola risiko dan mengamankan sumber daya TI yang begitu tergantung? Bagaimana perusahaan memastikan bahwa TI mencapai tujuannya dan mendukung bisnis?

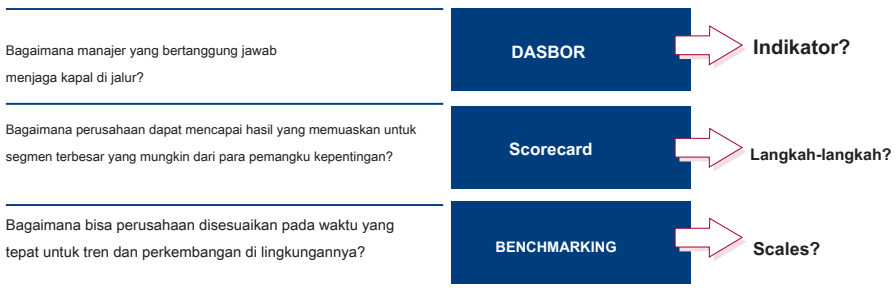
Pertama, manajemen perlu tujuan pengendalian yang mendefinisikan tujuan akhir dari pelaksanaan kebijakan, rencana dan prosedur, dan struktur organisasi yang dirancang untuk memberikan keyakinan memadai bahwa:

- tujuan bisnis tercapai
- peristiwa yang tidak diinginkan dicegah atau dideteksi dan diperbaiki

Kedua, dalam lingkungan yang kompleks saat ini, manajemen terus mencari informasi kental dan tepat waktu untuk membuat keputusan sulit pada nilai, risiko dan pengendalian cepat dan berhasil. Apa yang harus diukur, dan bagaimana? Perusahaan perlu ukuran yang obyektif dari mana mereka berada dan di mana perbaikan diperlukan, dan mereka perlu untuk mengimplementasikan kit alat manajemen untuk memantau perbaikan ini.

Gambar 1 menunjukkan beberapa pertanyaan tradisional dan alat-alat informasi manajemen yang digunakan untuk menemukan tanggapan, tapi dashboard ini perlu indikator, Scorecard perlu langkah-langkah dan benchmarking membutuhkan skala untuk perbandingan.

Gambar 1-Manajemen Informasi



Jawaban persyaratan ini penentuan dan pemantauan pengendalian TI dan tingkat kinerja yang tepat adalah C OBI Definisi T dari:

- **benchmarking** kinerja proses TI dan kemampuan, dinyatakan sebagai model jatuh tempo, berasal dari Capability Maturity Model Rekayasa Perangkat Lunak Institute (CMM)
- **Tujuan dan metrik** dari proses TI untuk mendefinisikan dan mengukur hasil dan kinerja mereka berdasarkan prinsip-prinsip Robert Kaplan dan scorecard bisnis seimbang David Norton
- **tujuan kegiatan** untuk mendapatkan proses ini di bawah kontrol, berdasarkan C OBI tujuan pengendalian T

Penilaian kemampuan proses didasarkan pada C OBI model T jatuh tempo adalah bagian penting dari pelaksanaan tata kelola TI. Setelah mengidentifikasi proses TI kritis dan kontrol, pemodelan jatuh tempo memungkinkan kesenjangan dalam kemampuan untuk diidentifikasi dan menunjukkan kepada manajemen. rencana aksi kemudian dapat dikembangkan untuk membawa proses ini hingga level target kemampuan yang diinginkan.

Dengan demikian, C OBI T mendukung pemerintahan (TI **Gambar 2**) dengan menyediakan kerangka kerja untuk memastikan bahwa:

- TI sejalan dengan bisnis
- IT memungkinkan bisnis dan memaksimalkan manfaat
- sumber daya TI digunakan secara bertanggung jawab
- risiko TI dikelola dengan tepat

Pengukuran kinerja sangat penting untuk tata kelola TI. Hal ini didukung oleh C OBI T dan termasuk pengaturan dan pemantauan tujuan yang terukur dari apa proses TI perlu memberikan (proses hasil) dan bagaimana menyampaikannya (kemampuan proses dan kinerja). Banyak survei telah mengidentifikasi bahwa kurangnya transparansi biaya, nilai IT dan risiko adalah salah satu driver yang paling penting bagi tata kelola TI. Sementara area fokus lainnya berkontribusi, transparansi terutama dicapai melalui pengukuran kinerja.

Gambar 2-IT Area Governance Fokus

- **keselarasan strategis** berfokus pada memastikan hubungan bisnis dan rencana TI; mendefinisikan, memelihara dan memvalidasi nilai IT proposisi; dan menyelaraskan operasi dengan operasi perusahaan IT.
- **pengiriman nilai** adalah tentang menjalankan proposisi nilai seluruh siklus pengiriman, memastikan bahwa IT memberikan manfaat yang dijanjikan terhadap strategi, berkonsentrasi pada biaya mengoptimalkan dan membuktikan nilai intrinsik dari IT.
- **Pengelolaan sumber daya** adalah tentang investasi yang optimal dalam, dan pengelolaan yang baik, sumber daya kritis TI: aplikasi, informasi, infrastruktur dan orang-orang. isu-isu kunci berhubungan dengan optimasi pengetahuan dan infrastruktur.
- **Manajemen risiko** membutuhkan kesadaran risiko dengan pejabat perusahaan senior, pemahaman yang jelas nafsu makan perusahaan itu untuk risiko, pemahaman persyaratan kepatuhan, transparansi tentang risiko yang signifikan terhadap perusahaan dan embedding tanggung jawab manajemen risiko dalam organisasi.
- **pengukuran kinerja** trek dan monitor implementasi strategi, penyelesaian proyek, penggunaan sumber daya, kinerja proses dan pelayanan, menggunakan, misalnya, scorecard seimbang yang menerjemahkan strategi ke dalam tindakan untuk mencapai tujuan yang terukur di luar akuntansi konvensional.

area fokus tata kelola TI ini menggambarkan topik yang manajemen eksekutif perlu alamat untuk memerintah TI dalam perusahaan mereka. manajemen operasional menggunakan proses untuk mengatur dan mengelola kegiatan IT yang sedang berlangsung. C OBI T menyediakan model proses generik yang mewakili semua proses biasanya ditemukan dalam fungsi IT, menyediakan model referensi umum dipahami operasional TI dan bisnis manajer. C OBI T model proses telah dipetakan ke area fokus tata kelola TI (lihat lampiran II, Pemetaan IT Proses untuk IT Governance Fokus Area, COSO, C OBI T Resources IT dan C OBI T Informasi Kriteria), menyediakan jembatan antara apa yang manajer operasional harus menjalankan dan eksekutif apa yang ingin memerintah.

Untuk mencapai pemerintahan yang efektif, eksekutif mengharuskan kontrol dilaksanakan oleh manajer operasional dalam kerangka kontrol ditetapkan untuk semua proses IT. C OBI tujuan pengendalian TI T yang diselenggarakan oleh proses IT; Oleh karena itu, kerangka menyediakan link yang jelas antara persyaratan tata kelola TI, proses TI dan kontrol TI.

C OBI T difokuskan pada apa yang dibutuhkan untuk mencapai pengelolaan dan pengendalian TI yang memadai, dan diposisikan pada tingkat tinggi. C OBI T telah selaras dan harmonis dengan lainnya, yang lebih rinci, standar IT dan praktik yang baik (lihat lampiran IV, C OBI T 4.1 Primer Reference Material). C OBI T bertindak sebagai integrator dari bahan-bahan ini bimbingan yang berbeda, meringkas tujuan utama di bawah satu kerangka payung yang juga link ke pemerintahan dan bisnis persyaratan.

COSO (dan kerangka kerja compliant serupa) secara umum diterima sebagai kerangka pengendalian internal untuk perusahaan. C OBI T adalah kerangka pengendalian internal yang berlaku umum untuk TI.

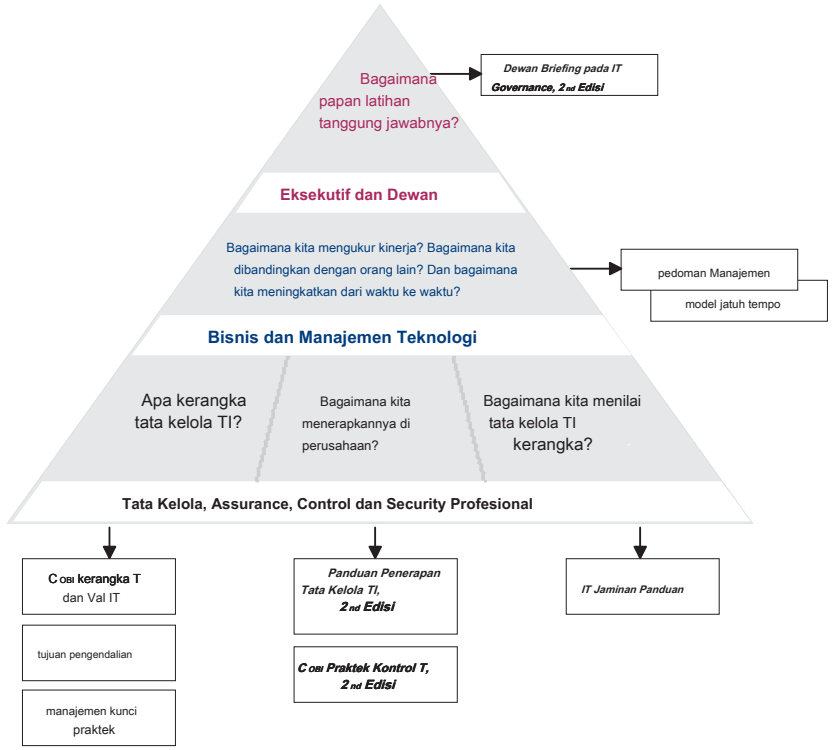
C OBI produk T telah disusun dalam tiga tingkatan (**Gambar 3)** dirancang untuk mendukung:

- manajemen eksekutif dan papan
- Bisnis dan manajemen TI
- Tata Kelola, jaminan, kontrol dan profesional keamanan

Secara singkat, C OBI produk T meliputi:

- *Dewan Briefing pada IT Governance, 2nd Edisi* eksekutif -Membantu memahami mengapa IT governance penting, apa masalah yang dan apa tanggung jawab mereka untuk mengelola itu
- pedoman manajemen / jatuh tempo model-Bantuan menetapkan tanggung jawab, mengukur kinerja, dan benchmark dan alamat kesenjangan dalam kemampuan
- Kerangka-Mengatur IT tujuan pemerintahan dan praktek-praktek yang baik oleh IT domain dan proses, dan link mereka untuk kebutuhan bisnis
- Kontrol objectives- Menyediakan satu set lengkap persyaratan tingkat tinggi untuk dipertimbangkan oleh manajemen untuk kontrol yang efektif dari setiap proses TI
- *Panduan Penerapan Tata Kelola TI: Menggunakan C OBI T e dan Val IT TM, 2nd Edisi* - Menyediakan peta jalan umum untuk menerapkan tata kelola TI menggunakan C OBI T dan Val IT TM sumber

Gambar 3-C OBI T Konten Diagram



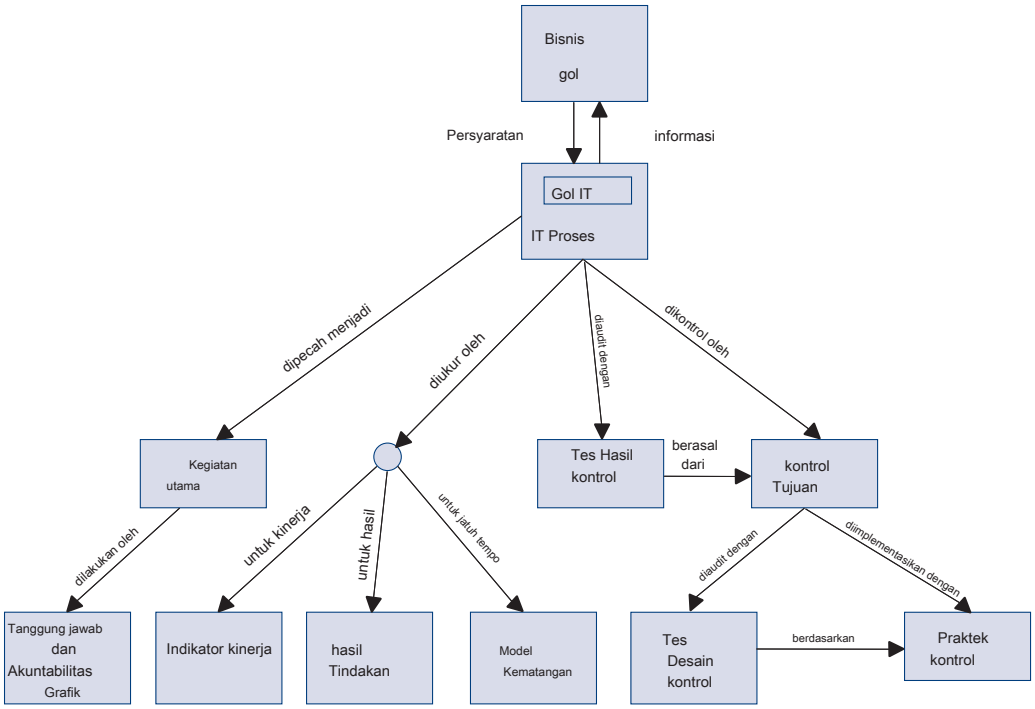
Ini C OBI Berbasis T diagram produk menyajikan produk yang berlaku secara umum dan penonton utama mereka. Ada juga produk yang berasal untuk tujuan tertentu (*IT Kontrol Tujuan untuk Sarbanes-Oxley, 2nd Edisi*), untuk domain seperti keamanan (C OBI T *keamanan Dasar* dan *Keamanan Informasi Pemerintahan: Pedoman Direksi dan Manajemen Eksekutif*),
atau untuk perusahaan tertentu (C OBI T *Mulai cepat* untuk usaha kecil dan menengah atau perusahaan besar yang ingin jalan sampai dengan implementasi tata kelola TI yang lebih luas).

- *C OBI T e Praktek Control: Panduan untuk Mencapai Tujuan Control untuk Sukses IT Governance, 2nd Edisi* bimbingan-Menyediakan mengapa kontrol yang layak melaksanakan dan bagaimana menerapkan mereka
- *IT Jaminan Panduan: Menggunakan C OBI T e* bimbingan-Menyediakan tentang bagaimana C OBI T dapat digunakan untuk mendukung berbagai kegiatan jaminan bersama-sama dengan langkah-langkah pengujian disarankan untuk semua proses TI dan tujuan pengendalian

C OBI T diagram konten digambarkan dalam **angka 3** menyajikan khalayak primer, pertanyaan mereka tentang tata kelola TI dan produk berlaku umum yang memberikan respon. Ada juga produk yang berasal untuk tujuan tertentu, untuk domain seperti keamanan atau untuk perusahaan tertentu.

Semua C ini OBI komponen T saling berhubungan, memberikan dukungan untuk pemerintahan, manajemen, kontrol dan jaminan kebutuhan audiens yang berbeda, seperti yang ditunjukkan pada **Gambar 4.**

Gambar 4-hubungan timbal balik dari C OBI Komponen T



C OBI T adalah kerangka kerja dan mendukung set alat yang memungkinkan manajer untuk menjembatani kesenjangan sehubungan dengan persyaratan kontrol, masalah teknis dan risiko bisnis, dan berkomunikasi tingkat kontrol kepada pemangku kepentingan. C OBI T memungkinkan pengembangan kebijakan yang jelas dan praktik yang baik untuk kontrol TI di seluruh perusahaan. C OBI T terus terus up to date dan diselaraskan dengan standar dan bimbingan lainnya. Oleh karena itu, C OBI T telah menjadi integrator untuk IT praktek yang baik dan kerangka payung untuk tata kelola TI yang membantu dalam memahami dan mengelola risiko dan manfaat yang terkait dengan IT. Proses Struktur C OBI T dan tingkat tinggi, pendekatan berorientasi bisnis yang memberikan end-to-end pandangan IT dan keputusan yang harus dibuat tentang IT.

Manfaat menerapkan C OBI T sebagai kerangka tata kelola lebih IT meliputi:

- keselarasan yang lebih baik, berdasarkan fokus bisnis
- Pandangan, dimengerti untuk manajemen, apa IT tidak
- Jelas kepemilikan dan tanggung jawab, berdasarkan orientasi proses
- penerimaan umum dengan pihak ketiga dan regulator
- pemahaman bersama antara semua pemangku kepentingan, berdasarkan bahasa yang umum
- Pemenuhan persyaratan COSO untuk lingkungan pengendalian TI

Sisa dokumen ini memberikan gambaran tentang C OBI Kerangka T dan semua inti C OBI komponen T, yang diselenggarakan oleh C OBI T empat domain IT dan 34 proses TI. Ini menyediakan buku referensi yang berguna untuk semua utama C OBI bimbingan T. Beberapa lampiran juga disediakan sebagai referensi berguna.

Informasi yang paling lengkap dan up-to-date pada C OBI T dan produk terkait, termasuk alat-alat online, panduan implementasi, studi kasus, newsletter dan materi pendidikan dapat ditemukan di *www.isaca.org/cobit*.

COBIT FRAMEWORK

C OBI TF RAMEWORK

C OBI T Mission:

Untuk meneliti, mengembangkan, mempublikasikan dan mempromosikan otoritatif, up-to-date, yang diterima secara internasional IT kerangka pengendalian tata kelola untuk diadopsi oleh perusahaan dan penggunaan sehari-hari oleh manajer bisnis, profesional TI dan profesional jaminan

KEBUTUHAN KERANGKA PENGENDALIAN TATA IT

Sebuah kerangka kontrol untuk tata kelola TI mendefinisikan alasan tata kelola TI yang dibutuhkan, para pemangku kepentingan dan apa yang dibutuhkan untuk mencapai.

Mengapa

Semakin, manajemen puncak adalah menyadari dampak yang signifikan bahwa informasi dapat memiliki pada keberhasilan perusahaan. Manajemen mengharapkan tinggi pemahaman tentang cara TI dioperasikan dan kemungkinan yang sedang memanfaatkan berhasil untuk keunggulan kompetitif. Secara khusus, manajemen puncak perlu tahu apakah informasi ini dikelola oleh perusahaan sehingga:

- Kemungkinan untuk mencapai tujuannya
- cukup tangguh untuk belajar dan beradaptasi
- Bijaksana mengelola risiko yang dihadapinya
- Tepat mengenali peluang dan bertindak atas mereka

perusahaan yang sukses memahami risiko dan mengeksploitasi manfaat IT dan menemukan cara untuk menangani:

- Menyelaraskan strategi TI dengan strategi bisnis
- Menjamin investor dan pemegang saham bahwa 'standar perawatan karena' sekitar mitigasi risiko TI dipenuhi oleh organisasi
- Cascading strategi IT dan gol ke perusahaan
- Memperoleh nilai dari investasi TI
- Menyediakan struktur organisasi yang memfasilitasi pelaksanaan strategi dan tujuan
- Menciptakan hubungan yang konstruktif dan komunikasi yang efektif antara bisnis dan TI, dan dengan mitra eksternal
- Mengukur kinerja TI

Perusahaan tidak dapat memberikan secara efektif terhadap kebutuhan bisnis dan pemerintahan ini tanpa mengadopsi dan menerapkan kerangka kerja tata kelola dan kontrol untuk IT untuk:

- Membuat link dengan kebutuhan bisnis
- Membuat kinerja terhadap persyaratan ini transparan
- Mengatur kegiatannya menjadi model proses yang berlaku umum
- Mengidentifikasi sumber daya besar untuk dimanfaatkan
- Tentukan tujuan pengendalian manajemen untuk dipertimbangkan

Selain itu, tata kelola dan pengendalian kerangka kerja yang menjadi bagian dari praktek manajemen TI yang baik dan enabler untuk membangun IT governance dan memenuhi terus meningkat persyaratan peraturan.

IT praktek yang baik telah menjadi signifikan karena sejumlah faktor:

- manajer bisnis dan papan menuntut hasil yang lebih baik dari investasi TI, yaitu, bahwa IT memberikan apa yang perlu bisnis untuk meningkatkan nilai stakeholder
- Keprihatinan atas tingkat umumnya meningkat pengeluaran IT
- Kebutuhan untuk memenuhi persyaratan peraturan untuk IT kontrol di berbagai bidang seperti privasi dan pelaporan keuangan (misalnya, AS Sarbanes-Oxley Act, Basel II) dan di sektor-sektor tertentu seperti keuangan, farmasi dan kesehatan
- Pemilihan penyedia layanan dan pengelolaan layanan outsourcing dan akuisisi
- Semakin kompleks terkait IT risiko, seperti keamanan jaringan
- inisiatif tata kelola TI yang mencakup adopsi kerangka kontrol dan praktek-praktek yang baik untuk membantu memantau dan meningkatkan kegiatan TI penting untuk meningkatkan nilai bisnis dan mengurangi risiko bisnis
- Kebutuhan untuk mengoptimalkan biaya dengan mengikuti, mana mungkin, standar, bukan khusus dikembangkan, pendekatan
- **Tumbuh kedewasaan dan konsekuen penerimaan kerangka dianggap baik, seperti C OBI T, IT Infrastructure Library (ITIL), seri ISO 27000 tentang standar yang berhubungan dengan keamanan informasi, ISO 9001: 2000 *Sistem-Persyaratan Manajemen Mutu,* Capability Maturity Model Integrasi (CMMI), Proyek di Terkendali Lingkungan 2 (PRINCE2) dan *Sebuah Panduan untuk PMBOK (* PMBOK)**
- Kebutuhan perusahaan untuk menilai bagaimana mereka melakukan terhadap standar yang berlaku umum dan rekan-rekan mereka (benchmarking)

Siapa

Sebuah kerangka tata kelola dan pengendalian kebutuhan untuk melayani berbagai pemangku kepentingan internal dan eksternal, yang masing-masing memiliki kebutuhan khusus:

- Pemangku kepentingan dalam perusahaan yang memiliki kepentingan dalam menghasilkan nilai dari investasi TI:
  - Mereka yang membuat keputusan investasi
  - Mereka yang memutuskan tentang persyaratan
  - Mereka yang menggunakan layanan TI
- stakeholder internal dan eksternal yang menyediakan layanan TI:
  - Mereka yang mengelola organisasi TI dan proses
  - Mereka yang mengembangkan kemampuan
  - Mereka yang mengoperasikan layanan
- stakeholder internal dan eksternal yang memiliki tanggung jawab kontrol / risiko:
  - Mereka yang keamanan, privasi dan / atau tanggung jawab risiko
  - Fungsi-fungsi kepatuhan melakukan
  - Mereka membutuhkan atau menyediakan jasa asuransi

Apa

Untuk memenuhi persyaratan yang tercantum dalam bagian sebelumnya, kerangka kerja untuk tata kelola TI dan kontrol harus:

- Memberikan fokus bisnis untuk memungkinkan keselarasan antara bisnis dan TI tujuan
- Membangun orientasi proses untuk menentukan ruang lingkup dan luasnya cakupan, dengan struktur didefinisikan memungkinkan navigasi yang mudah dari konten

- Secara umum dapat diterima dengan menjadi konsisten dengan diterima IT praktek yang baik dan standar dan independen dari teknologi tertentu
- Menyediakan bahasa yang sama dengan satu set istilah dan definisi yang secara umum dipahami oleh semua pemangku kepentingan
- Membantu memenuhi persyaratan peraturan dengan menjadi konsisten dengan standar tata kelola perusahaan yang berlaku umum (misalnya, COSO) dan mengontrol diharapkan oleh regulator dan auditor eksternal

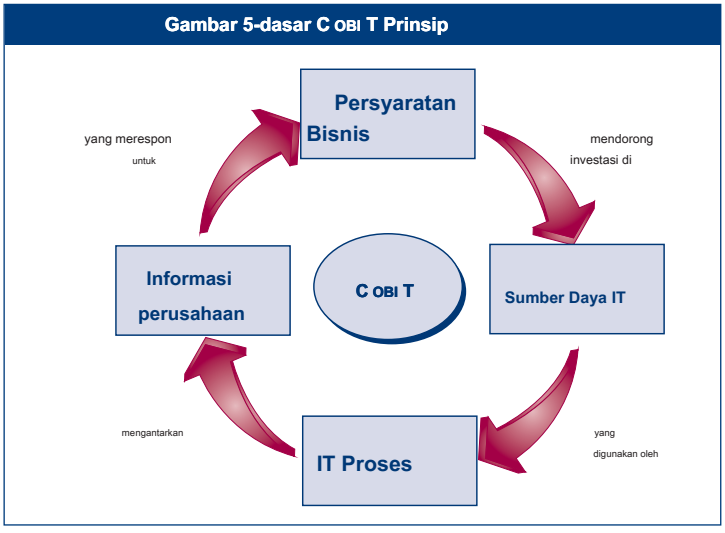
CARA C OBI T MEMENUHI KEBUTUHAN

Menanggapi kebutuhan dijelaskan pada bagian sebelumnya, C OBI T kerangka diciptakan dengan karakteristik utama menjadi bisnis yang berfokus, proses-berorientasi, kontrol berbasis dan pengukuran-driven.

Bisnis yang berfokus

orientasi bisnis adalah tema utama C OBI T. Hal ini dirancang tidak hanya untuk dipekerjakan oleh penyedia layanan TI, pengguna dan auditor, tetapi juga, dan yang lebih penting, untuk memberikan bimbingan yang komprehensif untuk manajemen dan proses bisnis pemilik.

Gambar 5-dasar C OBI T Prinsip



C OBI T kerangka kerja didasarkan pada prinsip berikut (Angka 5):

Untuk memberikan informasi bahwa perusahaan membutuhkan untuk mencapai tujuannya, perusahaan perlu untuk berinvestasi dalam dan mengelola dan mengendalikan sumber daya TI menggunakan satu set terstruktur proses untuk memberikan layanan yang memberikan informasi perusahaan yang diperlukan.

Mengelola dan mengendalikan informasi adalah jantung dari C OBI Kerangka T dan membantu memastikan keselarasan dengan kebutuhan bisnis.

C OBI KRITERIA INFORMASI T'S

Untuk memenuhi tujuan bisnis, informasi perlu memenuhi kriteria kontrol tertentu, yang C OBI T sebut sebagai kebutuhan bisnis untuk informasi. Berdasarkan kualitas yang lebih luas, persyaratan fidusia dan keamanan, tujuh, tentu tumpang tindih, kriteria informasi yang berbeda didefinisikan sebagai berikut:

- **Efektivitas** penawaran dengan informasi yang relevan dan berkaitan dengan proses bisnis serta yang disampaikan pada waktu yang tepat, benar, konsisten dan dapat digunakan.
- **Efisiensi** menyangkut penyediaan informasi melalui optimal (paling produktif dan ekonomis) penggunaan sumber daya.
- **kerahasiaan** menyangkut perlindungan informasi sensitif dari pengungkapan yang tidak sah.

- **Integritas** berkaitan dengan akurasi dan kelengkapan informasi serta validitasnya sesuai dengan nilai-nilai bisnis dan harapan.

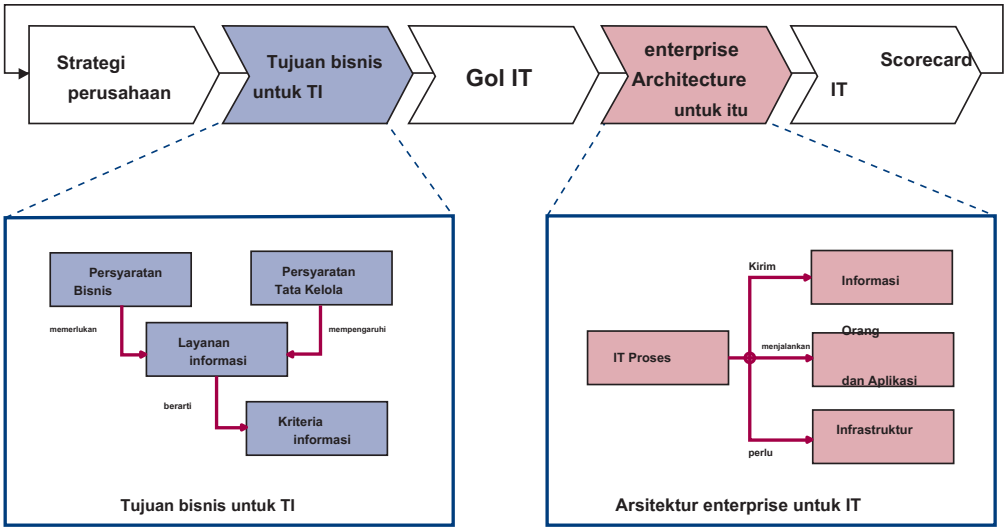
- **Tersedianya** berkaitan dengan informasi yang tersedia ketika dibutuhkan oleh proses bisnis sekarang dan di masa depan. Hal ini juga menyangkut pengamanan sumber daya yang diperlukan dan kemampuan yang terkait.
- **Pemenuhan** penawaran dengan mematuhi undang-undang, peraturan dan pengaturan kontrak yang proses bisnis tunduk, yaitu, dikenakan eksternal kriteria bisnis serta kebijakan internal.
- **Keandalan** berkaitan dengan penyediaan informasi yang tepat bagi manajemen untuk mengoperasikan entitas dan latihan fidusia dan pemerintahan tanggung jawabnya.

TUJUAN BISNIS DAN TUJUAN IT

Sementara kriteria informasi menyediakan metode umum untuk mendefinisikan kebutuhan bisnis, mendefinisikan satu set bisnis generik dan tujuan TI menyediakan bisnis terkait dan lebih halus dasar untuk membangun kebutuhan bisnis dan mengembangkan metrik yang memungkinkan pengukuran terhadap tujuan-tujuan tersebut. Setiap perusahaan menggunakan IT untuk memungkinkan inisiatif bisnis, dan ini dapat direpresentasikan sebagai tujuan bisnis untuk TI. Lampiran I menyediakan matriks tujuan bisnis generik dan tujuan TI dan menunjukkan bagaimana mereka memetakan dengan kriteria informasi. Contoh-contoh generik dapat digunakan sebagai panduan untuk menentukan bisnis yang spesifik persyaratan, tujuan dan metrik untuk perusahaan.

Jika TI adalah untuk berhasil memberikan layanan untuk mendukung strategi perusahaan itu, harus ada kepemilikan yang jelas dan arah persyaratan oleh bisnis (pelanggan) dan pemahaman yang jelas tentang apa yang perlu disampaikan, dan bagaimana, dengan IT (penyedia).
Gambar 6 menggambarkan bagaimana strategi perusahaan harus diterjemahkan oleh bisnis menjadi tujuan yang terkait dengan inisiatif IT-enabled (tujuan bisnis untuk TI). Tujuan-tujuan ini harus mengarah pada definisi yang jelas tentang tujuan TI sendiri (tujuan TI), yang pada gilirannya menentukan sumber daya TI dan kemampuan (arsitektur enterprise untuk IT) yang diperlukan untuk berhasil melaksanakan IT bagian dari strategi perusahaan.[1]

Gambar 6-Mendefinisikan Tujuan IT dan Enterprise Architecture untuk IT



Setelah gol selaras sudah ditetapkan, mereka perlu dipantau untuk memastikan bahwa pengiriman harapan pertandingan yang sebenarnya. Hal ini dicapai dengan metrik yang berasal dari tujuan dan ditangkap di sebuah scorecard IT.

Bagi pelanggan untuk memahami tujuan IT dan IT scorecard, semua tujuan dan metrik terkait harus dinyatakan dalam istilah bisnis yang berarti kepada pelanggan. Ini, dikombinasikan dengan keselarasan efektif dari hirarki tujuan, akan memastikan bahwa bisnis dapat mengkonfirmasi bahwa TI cenderung mendukung tujuan perusahaan.

Lampiran I, Tabel Menghubungkan Tujuan dan Proses, memberikan pandangan global bagaimana generik tujuan bisnis berhubungan dengan IT tujuan, proses TI dan kriteria informasi. Tabel membantu menunjukkan ruang lingkup C OBI T dan hubungan bisnis secara keseluruhan antara C OBI T dan perusahaan driver. Sebagai angka 6 menggambarkan, driver ini berasal dari bisnis dan dari lapisan pemerintahan dari perusahaan, mantan lebih fokus pada fungsi dan kecepatan pengiriman, yang terakhir lebih pada efisiensi biaya, laba atas investasi (ROI) dan kepatuhan.

[1] Perlu dicatat bahwa definisi dan implementasi arsitektur enterprise untuk IT juga akan menciptakan gol IT internal yang berkontribusi, tetapi tidak langsung berasal dari, tujuan bisnis.

SUMBER IT

Organisasi TI memberikan terhadap tujuan ini dengan satu set yang jelas dari proses yang menggunakan keterampilan orang dan infrastruktur teknologi untuk menjalankan aplikasi bisnis otomatis sementara memanfaatkan informasi bisnis. Sumber daya ini, bersama-sama dengan proses, merupakan suatu arsitektur enterprise untuk IT, seperti yang ditunjukkan pada **Angka 6.**

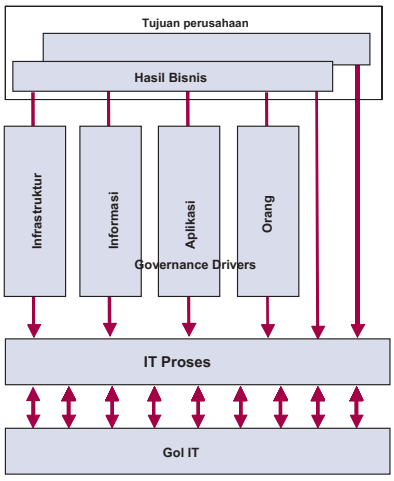
Untuk menanggapi kebutuhan bisnis untuk TI, perusahaan perlu untuk berinvestasi dalam sumber daya yang diperlukan untuk membuat kemampuan teknis yang memadai (misalnya, perencanaan sumber daya perusahaan [ERP] sistem) untuk mendukung kemampuan bisnis (misalnya, menerapkan supply chain) yang dihasilkan dalam hasil yang diinginkan (misalnya, peningkatan penjualan dan keuntungan finansial).

Sumber daya TI diidentifikasi di C OBI T dapat didefinisikan sebagai berikut:

- **Aplikasi** adalah sistem pengguna otomatis dan manual prosedur yang memproses informasi.
- **Informasi** adalah data, dalam segala bentuknya, input, diproses dan output oleh sistem informasi dalam bentuk apapun yang digunakan oleh bisnis.
- **Infrastruktur** adalah teknologi dan fasilitas (yaitu, hardware, sistem operasi, sistem manajemen database, jaringan, multimedia, dan lingkungan yang rumah dan mendukung mereka) yang memungkinkan pengolahan aplikasi.
- **Orang-orang** adalah personil yang dibutuhkan untuk merencanakan, mengatur, memperoleh, melaksanakan, menyampaikan, dukungan, memantau dan mengevaluasi sistem informasi dan layanan. Mereka mungkin internal, outsourcing atau kontrak seperti yang diperlukan.

Gambar 7 merangkum bagaimana tujuan bisnis untuk TI mempengaruhi bagaimana sumber daya TI perlu dikelola oleh proses IT untuk menyampaikan TI gol.

Gambar 7-Mengelola Sumber Daya IT untuk Memberikan IT Goals



Berorientasi proses

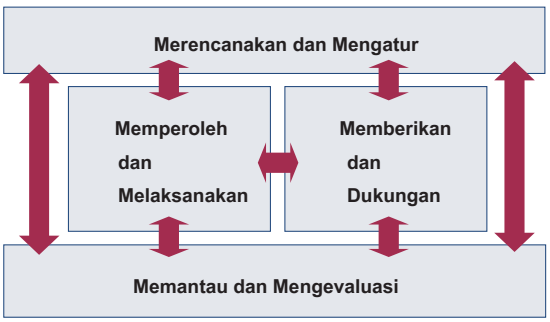
C OBI T mendefinisikan kegiatan IT dalam model proses generik dalam waktu empat domain. Domain ini adalah Rencana dan Mengatur, Memperoleh dan Melaksanakan, Memberikan dan Dukungan, dan Monitor dan Evaluasi. Domain peta ke TI daerah tanggung jawab tradisional rencana, membangun, menjalankan dan memantau.

C OBI T kerangka menyediakan model proses referensi dan bahasa umum untuk semua orang dalam suatu perusahaan untuk melihat dan mengelola kegiatan IT. Menggabungkan model operasional dan bahasa umum untuk semua bagian dari bisnis yang terlibat dalam IT adalah salah satu langkah yang paling penting dan awal menuju pemerintahan yang baik. Hal ini juga menyediakan kerangka kerja untuk mengukur dan memantau kinerja IT, berkomunikasi dengan penyedia layanan dan mengintegrasikan praktek manajemen terbaik. Sebuah model proses mendorong kepemilikan proses, memungkinkan tanggung jawab dan akuntabilitas untuk didefinisikan.

Untuk mengatur IT secara efektif, penting untuk menghargai kegiatan dan risiko dalam IT yang perlu dikelola. Mereka biasanya memerintahkan ke dalam domain tanggung jawab merencanakan, membangun, menjalankan dan memantau. Dalam C OBI T kerangka, domain ini, seperti yang ditunjukkan pada **Angka 8,** disebut:

- **Merencanakan dan Mengatur (PO)** arah-Menyediakan pengiriman solusi (AI) dan pelayanan (DS)
- **Memperoleh dan Melaksanakan (AI)** -Menyediakan solusi dan melewati mereka akan berubah menjadi layanan
- **Memberikan dan Dukungan (DS)** -Receives solusi dan membuat mereka dapat digunakan untuk pengguna akhir
- **Memantau dan Evaluasi (ME)** -Monitors semua proses untuk memastikan bahwa arah disediakan diikuti

Gambar 8-Empat saling berhubungan Domain C OBI T



RENCANA DAN BERORGANISASI (PO)

Domain ini mencakup strategi dan taktik, dan menyangkut identifikasi cara TI terbaik dapat memberikan kontribusi pada pencapaian bisnis tujuan. Realisasi dari visi strategis perlu direncanakan, dikomunikasikan dan dikelola untuk perspektif yang berbeda. Sebuah organisasi yang tepat serta infrastruktur teknologi harus diletakkan di tempat. domain ini biasanya membahas pertanyaan-pertanyaan manajemen berikut:

- Apakah IT dan strategi bisnis selaras?
- Adalah perusahaan mencapai penggunaan optimal dari sumber daya?
- Apakah setiap orang dalam organisasi memahami tujuan TI?
- Apakah IT risiko dipahami dan dikelola?
- Apakah kualitas sistem TI yang sesuai untuk kebutuhan bisnis?

AKUISISI DAN MELAKSANAKAN (AI)

Untuk mewujudkan strategi TI, solusi TI perlu diidentifikasi, dikembangkan atau diperoleh, serta diimplementasikan dan diintegrasikan ke dalam proses bisnis. Selain itu, perubahan dan pemeliharaan sistem yang ada ditutupi oleh domain ini untuk memastikan solusi terus memenuhi tujuan bisnis. domain ini biasanya membahas pertanyaan-pertanyaan manajemen berikut:

- Apakah proyek baru cenderung memberikan solusi yang memenuhi kebutuhan bisnis?
- Apakah proyek baru kemungkinan akan dikirimkan tepat waktu dan sesuai anggaran?
- Akan sistem baru bekerja dengan baik ketika diimplementasikan?
- Akan perubahan dilakukan tanpa mengganggu operasi bisnis saat ini?

MEMBERIKAN DAN DUKUNGAN (DS)

Domain ini berkaitan dengan pengiriman aktual dari layanan yang dibutuhkan, yang meliputi pelayanan, pengelolaan keamanan dan kontinuitas, dukungan layanan untuk pengguna, dan pengelolaan data dan fasilitas operasional. Ini biasanya membahas pertanyaan-pertanyaan manajemen berikut:

- Apakah layanan TI yang disampaikan sejalan dengan prioritas bisnis?
- Apakah biaya TI dioptimalkan?
- Apakah tenaga kerja dapat menggunakan sistem IT produktif dan aman?
- Memadai kerahasiaan, integritas dan ketersediaan di tempat untuk keamanan informasi?

MONITOR DAN EVALUASI (ME)

Semua proses TI perlu dinilai secara berkala dari waktu ke waktu untuk kualitas dan kepatuhan mereka dengan persyaratan kontrol. domain ini membahas manajemen kinerja, pemantauan pengendalian internal, kepatuhan terhadap peraturan dan tata kelola. Ini biasanya membahas pertanyaan-pertanyaan manajemen berikut:

- Apakah IT yang kinerja diukur untuk mendeteksi masalah sebelum terlambat?
- Apakah manajemen memastikan bahwa pengendalian internal yang efektif dan efisien?
- Dapat IT kinerja dihubungkan kembali ke tujuan bisnis?
- Memadai kerahasiaan, integritas dan ketersediaan kontrol di tempat untuk keamanan informasi?

Di empat domain tersebut, C OBI T telah mengidentifikasi 34 proses TI yang umumnya digunakan (lihat angka 22 untuk daftar lengkap). Sementara sebagian besar perusahaan telah menyelenggarakan program, membangun, menjalankan dan memantau tanggung jawab untuk IT, dan sebagian besar memiliki proses kunci yang sama, beberapa akan memiliki struktur proses yang sama atau menerapkan semua 34 C OBI proses T. C OBI T menyediakan daftar lengkap proses yang dapat digunakan untuk memverifikasi kelengkapan kegiatan dan tanggung jawab; Namun, mereka tidak perlu semua berlaku, dan, bahkan lebih, mereka dapat dikombinasikan seperti yang dipersyaratkan oleh masing-masing perusahaan.

Untuk setiap 34 proses ini, link dibuat untuk tujuan bisnis dan TI yang didukung. Informasi tentang bagaimana tujuan dapat diukur, apa kegiatan kunci dan point utama yang, dan siapa yang bertanggung jawab untuk mereka juga disediakan.

Kontrol berbasis

C OBI T mendefinisikan tujuan pengendalian untuk semua 34 proses, serta proses menyeluruh dan kontrol aplikasi.

PROSES PERLU KONTROL

Kontrol didefinisikan sebagai kebijakan, prosedur, praktek dan struktur organisasi yang dirancang untuk memberikan keyakinan memadai bahwa tujuan bisnis akan dicapai dan acara yang tidak diinginkan akan dicegah atau dideteksi dan dikoreksi.

tujuan pengendalian TI memberikan satu set lengkap persyaratan tingkat tinggi untuk dipertimbangkan oleh manajemen untuk kontrol yang efektif dari setiap proses TI. Mereka:

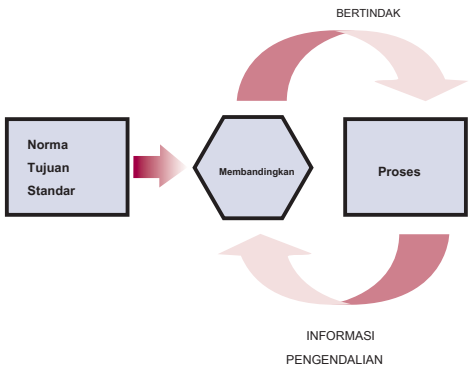
- Apakah laporan tindakan manajerial untuk meningkatkan nilai atau mengurangi risiko
- Terdiri dari kebijakan, prosedur, praktek dan struktur organisasi
- Dirancang untuk memberikan keyakinan memadai bahwa tujuan bisnis akan dicapai dan acara yang tidak diinginkan akan dicegah atau dideteksi dan dikoreksi

manajemen perusahaan perlu membuat pilihan relatif terhadap tujuan pengendalian ini dengan:

- Memilih orang-orang yang berlaku
- Memutus mereka yang akan dilaksanakan
- Memilih bagaimana menerapkan mereka (frekuensi, span, otomatisasi, dll)
- Menerima risiko tidak menerapkan mereka yang mungkin berlaku

Bimbingan dapat diperoleh dari model kontrol standar ditampilkan di **Angka 9.**
Ini mengikuti prinsip-prinsip jelas dalam analogi ini: Ketika suhu kamar (standar) untuk sistem pemanas (proses) diatur, sistem akan terus memeriksa (bandingkan) suhu ruang ambien (kontrol informasi) dan akan sinyal (tindakan) sistem pemanas untuk memberikan lebih atau kurang panas.

Gambar 9-Control Model



manajemen operasional menggunakan proses untuk mengatur dan mengelola kegiatan IT yang sedang berlangsung. C OBI T menyediakan model proses generik yang mewakili semua proses biasanya ditemukan dalam fungsi IT, menyediakan model referensi umum dipahami operasional TI dan bisnis manajer. Untuk mencapai pemerintahan yang efektif, kontrol harus dilaksanakan oleh manajer operasional dalam kerangka kontrol ditetapkan untuk semua proses IT. Sejak C OBI tujuan pengendalian TI T yang diselenggarakan oleh proses IT, kerangka memberikan link yang jelas antara persyaratan tata kelola TI, proses TI dan kontrol TI.

Masing-masing dari C OBI proses IT T memiliki deskripsi proses dan sejumlah tujuan pengendalian. Secara keseluruhan, mereka adalah karakteristik proses yang dikelola dengan baik.

Tujuan pengendalian diidentifikasi oleh dua karakter referensi domain (PO, AI, DS dan ME) ditambah sejumlah proses dan sejumlah tujuan kontrol. Selain tujuan kontrol, masing-masing C OBI Proses T memiliki persyaratan kontrol generik yang diidentifikasi oleh PCN, untuk nomor kontrol proses. Mereka harus dipertimbangkan bersama-sama dengan tujuan kontrol proses untuk memiliki pandangan lengkap persyaratan kontrol.

Tujuan Proses PC1 dan Tujuan

Mendefinisikan dan berkomunikasi spesifik, terukur, dapat ditindaklanjuti, realistis, berorientasi pada hasil yang tepat waktu tujuan (SMARRT) proses dan tujuan untuk pelaksanaan yang efektif dari setiap proses TI dan. Memastikan bahwa mereka terkait dengan tujuan bisnis dan didukung oleh metrik yang sesuai.

Kepemilikan Proses PC2

Menetapkan pemilik untuk setiap proses IT, dan jelas mendefinisikan peran dan tanggung jawab dari pemilik proses. Termasuk, misalnya, tanggung jawab untuk desain proses, interaksi dengan proses lainnya, akuntabilitas untuk hasil akhir, pengukuran kinerja proses dan identifikasi peluang perbaikan.

Proses PC3 Repeatability

Desain dan membangun setiap proses IT utama seperti bahwa itu adalah berulang dan konsisten menghasilkan hasil yang diharapkan. Menyediakan untuk urutan logis tapi fleksibel dan scalable kegiatan yang akan mengarah pada hasil yang diinginkan dan cukup gesit untuk menangani pengecualian dan keadaan darurat. Menggunakan proses yang konsisten, di mana mungkin, dan penjahit hanya ketika tidak dapat dihindari.

Peran dan Tanggung Jawab PC4

Mendefinisikan kegiatan kunci dan kiriman akhir proses. Menetapkan dan mengkomunikasikan peran dan tanggung jawab ambigu untuk pelaksanaan yang efektif dan efisien dari kegiatan utama dan dokumentasi mereka serta akuntabilitas untuk kiriman proses akhir.

PC5 Kebijakan, Rencana dan Prosedur

Mendefinisikan dan mengkomunikasikan bagaimana semua kebijakan, rencana dan prosedur yang mendorong proses IT didokumentasikan, Ulasan, dipelihara, disetujui, disimpan, dikomunikasikan dan digunakan untuk pelatihan. Menetapkan tanggung jawab untuk setiap kegiatan dan, pada waktu yang tepat, meninjau apakah mereka dieksekusi dengan benar. Memastikan bahwa kebijakan, rencana dan prosedur dapat diakses, benar, dipahami dan up to date.

PC6 Peningkatan Kinerja Proses

Mengidentifikasi satu set metrik yang memberikan wawasan ke dalam hasil dan kinerja proses. Menetapkan target yang mencerminkan pada tujuan proses dan indikator kinerja yang memungkinkan pencapaian tujuan proses. Mendefinisikan bagaimana data yang akan diperoleh. Bandingkan pengukuran sebenarnya untuk target dan mengambil tindakan atas penyimpangan, di mana diperlukan. Menyelaraskan metrik, target dan metode dengan TI pendekatan pemantauan kinerja secara keseluruhan.

kontrol yang efektif mengurangi risiko, meningkatkan kemungkinan pengiriman nilai dan meningkatkan efisiensi karena akan ada lebih sedikit kesalahan dan pendekatan manajemen yang lebih konsisten.

Selain itu, C OBI T memberikan contoh untuk setiap proses yang ilustratif, tapi tidak preskriptif atau lengkap, dari:

- input dan output generik
- Kegiatan dan bimbingan pada peran dan tanggung jawab dalam, Akuntabel, Dikonsultasikan dan Informed (RACI) grafik Bertanggung Jawab
- kegiatan utama tujuan (hal yang paling penting untuk dilakukan)
- metrik

Selain menghargai apa yang diperlukan kontrol, pemilik proses perlu memahami masukan apa yang mereka butuhkan dari orang lain dan apa yang orang lain butuhkan dari proses mereka. C OBI T menyediakan contoh generik input kunci dan output untuk setiap proses, termasuk persyaratan TI eksternal. Ada beberapa output yang input ke semua proses lainnya, ditandai sebagai 'SEMUA' di tabel output, tetapi mereka tidak disebutkan sebagai masukan dalam semua proses, dan biasanya mencakup standar kualitas dan persyaratan metrik, kerangka proses IT, peran didokumentasikan dan tanggung jawab, kerangka kontrol TI perusahaan, kebijakan TI, dan peran personil dan tanggung jawab.

Memahami peran dan tanggung jawab untuk setiap proses adalah kunci untuk pemerintahan yang efektif. C OBI T menyediakan grafik RACI untuk setiap proses. Akuntabel berarti 'uang berhenti here'-ini adalah orang yang memberikan arahan dan kewenangan suatu kegiatan. Tanggung jawab tersebut diberikan untuk orang yang mendapat tugas dilakukan. Dua peran lain (dikonsultasikan dan memberitahu) memastikan bahwa setiap orang yang perlu terlibat dan mendukung proses.

BISNIS DAN IT KONTROL

Sistem perusahaan itu kontrol internal dampak TI pada tiga tingkatan:

- Pada tingkat manajemen eksekutif, tujuan bisnis ditetapkan, kebijakan ditetapkan dan keputusan dibuat tentang bagaimana untuk menyebarkan dan mengelola sumber daya perusahaan untuk menjalankan strategi perusahaan. Pendekatan secara keseluruhan untuk tata kelola dan kontrol didirikan oleh dewan dan dikomunikasikan di seluruh perusahaan. Lingkungan pengendalian TI diarahkan oleh ini tingkat atas set tujuan dan kebijakan.

- Pada tingkat proses bisnis, kontrol diterapkan untuk kegiatan bisnis tertentu. Kebanyakan proses bisnis yang otomatis dan terintegrasi dengan sistem aplikasi IT, sehingga banyak dari kontrol pada tingkat ini yang otomatis juga. Kontrol ini dikenal sebagai kontrol aplikasi. Namun, beberapa kontrol dalam proses bisnis tetap sebagai prosedur manual, seperti otorisasi untuk transaksi, pemisahan tugas dan rekonsiliasi manual. Oleh karena itu, kontrol pada tingkat proses bisnis adalah kombinasi dari kontrol manual dioperasikan oleh bisnis dan bisnis dan aplikasi otomatis kontrol. Kedua adalah tanggung jawab bisnis untuk mendefinisikan dan mengelola, meskipun kontrol aplikasi membutuhkan fungsi IT untuk mendukung desain dan pengembangan mereka.

- Untuk mendukung proses bisnis, TI menyediakan layanan TI, biasanya dalam layanan bersama untuk banyak proses bisnis, karena banyak pembangunan dan operasional proses IT disediakan untuk seluruh perusahaan, dan banyak dari infrastruktur TI disediakan sebagai layanan umum (misalnya, jaringan, database, sistem operasi dan penyimpanan). Yang diterapkan untuk semua kegiatan layanan TI kontrol dikenal sebagai IT kontrol umum. Keandalan operasi ini kontrol umum diperlukan untuk ketergantungan untuk ditempatkan di kontrol aplikasi. Sebagai contoh, manajemen perubahan yang buruk bisa membahayakan (sengaja atau sengaja) keandalan pemeriksaan integritas otomatis.

IT KONTROL UMUM DAN KONTROL APLIKASI

kontrol umum adalah kontrol tertanam dalam proses TI dan layanan. Contoh termasuk:

- pengembangan sistem
- perubahan manajemen
- Keamanan
- operasi komputer

Kontrol tertanam dalam aplikasi proses bisnis yang sering disebut sebagai kontrol aplikasi. Contoh termasuk:

- Kelengkapan
- Ketepatan
- Keabsahan
- Otorisasi
- Pemisahan tugas

C OBI T mengasumsikan desain dan implementasi pengendalian aplikasi otomatis menjadi tanggung jawab IT, tercakup dalam Acquire dan Melaksanakan domain, berdasarkan kebutuhan bisnis didefinisikan dengan menggunakan C OBI Kriteria informasi T, seperti yang ditunjukkan pada **Angka 10.**

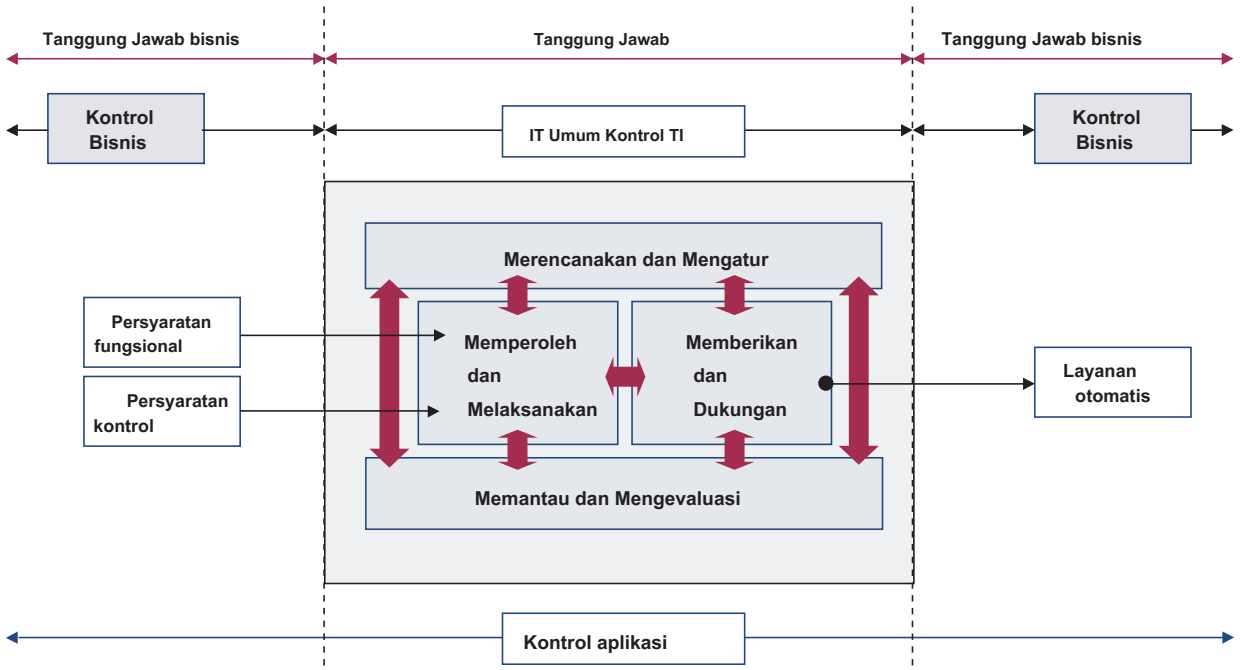
Operasional pengelolaan dan pengendalian tanggung jawab untuk kontrol aplikasi tidak dengan IT, tapi dengan pemilik proses bisnis.

Oleh karena itu, tanggung jawab untuk kontrol aplikasi yang end-to-end tanggung jawab bersama antara bisnis dan TI, tetapi sifat dari perubahan tanggung jawab sebagai berikut:

- bisnis bertanggung jawab untuk benar:
  - Mendefinisikan kebutuhan fungsional dan kontrol
  - Gunakan layanan otomatis
- IT bertanggung jawab untuk:
  - Mengotomatisasi dan melaksanakan bisnis fungsional dan kontrol persyaratan
  - Membangun kontrol untuk menjaga integritas kontrol aplikasi

Oleh karena itu, C OBI proses IT T menutupi umum mengontrol IT, tetapi hanya aspek-aspek pengembangan kontrol aplikasi; tanggung jawab untuk definisi dan penggunaan operasional dengan bisnis.

Gambar 10-Batas Bisnis, Umum dan Kontrol Aplikasi



Daftar berikut menyediakan satu set direkomendasikan tujuan pengendalian aplikasi. Mereka diidentifikasi oleh ACN, untuk nomor kontrol aplikasi.

AC1 Sumber Persiapan Data dan Otorisasi

Memastikan bahwa sumber dokumen yang disiapkan oleh petugas yang berwenang dan berkualitas mengikuti prosedur yang ditetapkan, dengan memperhitungkan pembagian tugas yang memadai mengenai originasi dan persetujuan dokumen-dokumen ini. Kesalahan dan kelalaian dapat diminimalkan melalui desain form input yang baik. Mendeteksi kesalahan dan penyimpangan sehingga mereka dapat dilaporkan dan diperbaiki.

Pengumpulan Data AC2 Sumber dan Masuk

Menetapkan bahwa input data dilakukan pada waktu yang tepat oleh staf yang berwenang dan berkualitas. Koreksi dan resubmission data yang keliru masukan harus dilakukan tanpa mengorbankan tingkat otorisasi transaksi asli. Apabila diperlukan untuk rekonstruksi, mempertahankan dokumen sumber asli untuk jumlah waktu yang tepat.

AC3 Akurasi, Kelengkapan dan Keaslian Cek

Memastikan bahwa transaksi yang akurat, lengkap dan valid. Memvalidasi data yang masukan, dan mengedit atau mengirim kembali untuk koreksi sebagai dekat dengan titik originasi mungkin.

AC4 Pengolahan Integritas dan Validitas

Menjaga integritas dan validitas data sepanjang siklus pengolahan. Deteksi transaksi yang keliru tidak mengganggu proses transaksi yang sah.

AC5 Keluaran Ulasan, Rekonsiliasi dan Penanganan Kesalahan

Menetapkan prosedur dan tanggung jawab terkait untuk memastikan output yang ditangani dengan cara yang berwenang, dikirim ke penerima yang tepat, dan dilindungi selama transmisi; verifikasi, deteksi dan koreksi akurasi output terjadi; dan bahwa informasi yang diberikan dalam output digunakan.

AC6 Transaksi Otentikasi dan Integritas

Sebelum melewati data transaksi antara aplikasi internal dan bisnis / fungsi operasional (di atau di luar perusahaan), memeriksa untuk tepat menangani, keaslian asal dan integritas konten. Menjaga keaslian dan integritas selama transmisi atau transportasi.