ITGI™ Enables
ISO/IEC 38500:2008 Adoption

ISO/IEC 38500：2008 への適合を ITGI™は可能とする

ISO/IEC 38500:2008への適合をITGIは可能にする

ITGI Enables IS0/IEC 38500:2008 Adoption

IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help executives and IT professionals ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly managed, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfill their IT governance responsibilities and help IT professionals deliver value-adding services.

IT ガバナンス協会®

ITガバナンス協会(ITGI™)(www.itgi.org)は、非営利であり、独立した調査研究機関として、IT資産のガバナンスに関する国際的な問題を経のガイダンスを提供するものである。ITGIは非営利の会員組織であるISACAによって1998年に設立され、企業の役員やITの専門家が、企業目標に整合させて、ITが価値を生み出しリスクを軽減し、IT資源が適切にマネジメントされ、そしてITの成果が測定されるようにすることを支援するものである。ITGIは*Control Objectives for Information and related Technology* (COBIT®)とVal IT™を開発し、独自の調査とケーススタディを提供することで、企業のリーダー及び取締役会が、彼らのITガバナンスにおける責任を果たすことを支援し、ITの専門家には付加価値のあるサービスを提供することを支援している。

Disclaimer

ITGI has designed and created this publication, titled *ITGITM Enables IS0/IEC 38500:2008 Adoption* (the 'Work'), primarily as an educational resource. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information procedure or test, control professionals should apply their own professional judgment to the specific control circumstances presented by the particular systems or information technology (IT) environment.

免責事項

ITGIは、本書「ISO/IEC 38500:2009への適合をITGIは可能とする」を主として教育を目的として設計し出版した。ITGIは、本書のどのような使用であれ、その成果の成功を保証するものではない。本書は、すべての適切な手続やテストを含むものではなく、また、合理的に同じ結果を導く、本書に記載されていない手続およびテストを除外するものでもない。本書を使用するコントロールの専門家は、その特定の手続およびテストの妥当性は、対象とするシステムまたはIT環境における特定の統制の状況について十分に考慮し、自身の専門家としての判断を下すべきである。

Reservation of Rights

著作権等

Quality of the Translation

This Work is translated into Japanese from the Work by ITGI Japan with the permission of the IT Governance Institute. ITGI Japan assumes sole responsibility for the accuracy and faithfulness of the translation. For the formal Japanese translation of ISO related word, please refer to the document from "Japanese Standards Association"

本著作物の翻訳品質について

この著作物は、IT Governance Instituteの許諾の下、日本ITガバナンス協会（ITGI Japan)が、原著を英語から日本語に翻訳したものです。ITGI Japanは著作物の翻訳の正確さについてのみ、その責任を有します。**なお、ISOで使用されている英語の正式日本語訳については、日本規格協会から出版されるものをご利用下さい。**

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

Acknowledgements

ITGI wishes to recognize:

Researcher
Gary Hardy, CGEIT, IT Winners, South Africa

Expert Reviewers
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA
Tony Hayes, FCPA, Queensland Government, Australia
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium
Vatsaraman Venkatakrishnan, CISA, CISM, CGEIT, ACA, Emirates Airlines, UAE

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President
George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President
Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President
Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President
Frank Yam, CISA, CIA, CCP, CFE, CFSA, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Sushil Chatterji, Edutech Enterprises, Singapore
Kyung-Tae Hwang, CISA, Dongguk University, Korea
John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA
Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Accenture Technology Services, France
Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico
Robert E. Stroud, CA Inc., USA
John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

ITGI Affiliates and Sponsors
American Institute of Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systemes d'Information
Institute of Management Accountants Inc.

ITGI Affiliates and Sponsors *(cont.)*
ISACA
ISACA chapters
ITGI Japan
Norwich University
Socitm Performance Management Group
Solvay Brussels School of Economics and Management
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
BWise B.V.
CA Inc.
Consult2Comply
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corp.
TruArx Inc.
Wolcott Group LLC
World Pass IT Solutions

翻訳チーム

翻訳
梶本　政利（ITGI Japan）

翻訳運営チーム　日本ITガバナンス協会（ITGI Japan）翻訳委員会
委員長　松原　榮一
委員　梶本　政利
委員　木村　章展
委員　中村　努
委員　吉丸　成人

Introduction

IT 投資からより価値を生み出し、より増大するIT 関連の多様なリスクをマネジメントすることに対するニーズはこれまでに無いほど高まっている。

1998年にISACA[1]は情報及び関連技術(IT)の利用を企業がガバナンスする手法を改善する必要を識別し、そして画期的な行動を取った。これによりITガバナンス協会(ITGI)を設立し、企業のガバナンスにおけるこのキー領域における調査を進めガイダンスとなるものを開発した。ITGI (www.itgi.org)は企業におけるITの利用に関する、評価、管理、モニタリングについて国際的な思考とガイダンスを発展させるものを確立した。

ITGIはISOが"ISO/IEC 385000:2008 情報技術におけるコーポレイトガバナンス"を公開したことを歓迎するものである。これによってこの話題の重要性をグローバルに認識し、その採用を正式なものとする必要性が認定された。情報及び技術が我々の周囲全体に存在し、ビジネス及び一般生活のどの局面においても重要である時に、同時に、IT投資からより多くの価値を生み出す必要性、そして、IT関連のリスクの種類が増大していることをマネジメントすることの必要性が、かつて無いほど増大している。規制の増大はまた、役員たちの中において、うまくコントロールされたIT環境の重要性と、法的、規制上、及び契約上の義務に従う必要性についての認識を高めた。効果的なITに関する企業のガバナンスは、結果として業績と外的要求への遵守を改善するものとなる。

IT に関する効果的な企業ガバナンスはパフォーマンスの改善に役立ち、外部要件への遵守に役立つ

国際標準はガバナンスをより進んだものへと発展させる基礎を提供するものであるとITGIは信じている。特にそれが、最小から最大の、全ての組織において適用可能であり、組織の目的や設計には依存しないからである。しかしながら、効果的な適用においては、その標準はより多くの導入支援を必要とするものである。ITGIの成果群は全ての規模の企業に合せることが出来る方法で支援を提供できるものである。

[1] ISACAは 1969 年に設立されて、現在 86,000 人以上の会員を 160 を超える国々に抱えている。ISACAはITガバナンス、コントロール、セキュリティ、及びアシュアランスにおける世界的なリーダーであると認識されている。ISACAは国際的なカンファレンスの実施、ISACA Journalの発行、および国際的な情報システム監査とコントロールの基準を開発している。また、3 つの国際的に尊敬される資格認定を行なっている。それは公認情報システム監査人(CISA)，公認情報セキュリティマネジャー(CISM)、Certified in the Governance of Enterprise IT(CGEIT)である。

ITGIの特有のプロフェッショナルアプローチ

COBITとVal ITのフレームワークを中心にすえたITGIのガイダンスは企業の役員とマネジャーが、企業におけるITの利用をどのように方向付けて監督したら良いのかについて、より良い理解をするために役立つ。

ISACAは1990年代の初期に監査人が、ITコントロールと有効性について評価するために彼ら独自のチェックリストを持ち、ビジネスマネジャーやITの実務家が使っているものとは異なる言語で話をしていることを認識した。このコミュニケーションギャップの橋渡しをするために、ビジネスマネジャーのためにITコントロールのフレームワークとしてCOBITが生み出され、ITマネジャーと監査人が基づく汎用のITプロセスの一式として生み出されたのである。COBITはITの専門家とビジネスマネジメントの両方に意味のあるものである。

ITガバナンス、コントロール、セキュリティ及びアシュアランスの専門家で構成されるISACAの特有の会員制度と、数百のグローバルエキスパート達の実務経験を元にして、ITGIは産業界をリードするガイダンスとなるものを、COBITフレームワークを元にして生み出した。その中には最近公開したVal ITフレームワークがある。これは、世界中の数千の企業にとって、ITガバナンスの原則を理解し実務に適用する際の、共通言語とアプローチを提供するものである。非営利組織としてITGIは幅広い成果を生み出してきた。いずれも特定の技術、ベンダー、及び商業製品とは独立したものであり、このガイダンスも無償で入手することが出来るようにしてある。これは企業の取締役会、執行責任者、役員およびマネジメントの人々が、組織構成、業務プロセス及びツールを導入して、重要なIT関連の要求を管理し、最も重要なIT活動をモニタリングし評価し、情報に基づく意思決定を行なうことを助けるものとなる。

企業は情報システムとそれらのシステムによって生み出された情報を信頼できることについて確信が持てることが必要である。彼らはIT投資からポジティブな利益を期待できることが必要である。ITGIのガイダンスはCOBITとVal ITフレームワークを中心に位置付けて、企業の役員やマネジャーが企業のITの利用をいかに管理しマネジメントするのか、およびITプロバイダーから期待すべき良好な業務の標準についてより良い理解をすることを可能とするものである。

ITGIが提供しているITガバナンスに関する全ての成果物についての説明は本書の最後につけてある。

ISO/IEC 38500標準の利益

ISO/IEC 38500は多くの理由によって有益なものである。

- リスクが内在し、十分な投資が必要であることためにITガバナンスの重要性を強調している
- 企業のITのガバナンスの土台を支えるものとして適切な標準を使用することを企業に奨励している
- 6つの基礎的原則のフレームワークを役員に提供し、それぞれの企業のITの利用における評価、管理、及びモニタリングの際に使用させるものとしている。
  これらの原則に従うことによって役員がリスクとITの利用によってもたらされる機会をバランスさせることを奨励するものである。これは最小から最大の、そして目的と組織構造の設計やオーナーシップとは無関係に、全ての企業に適用できるものである。
- 企業の適切なITのガバナンスによって、役員は容認可能なITの利用に関係する責務（規制、法律、慣習法、契約）への適合を保証すること、及びIT利用がその企業の業績にポジティブに貢献していることを保証することが支援されることを明確にしている
- 不適切なITシステムが役員をますます広範囲の法律を遵守していないリスクにさらされ得ることを明確にしている

標準を導入すること及び取締役会で確立された方向付けに対応することは、ITGIから出されている追加的なガイダンスで支援される。

どのようにITGIはこの標準を支援するか

以下にCOBIT, Val ITと関連するガイダンスが、どのようにこの標準の原則の適用と導入アプローチを支援するのかについてまとめている。より多くの情報を得るために、この文書の最後に現在得られる成果物とウェブのリンクのリストがまとめられている。この新しい標準、“ISO/IEC 38500:2008 － 情報技術のコーポレイトガバナンス”は6つのキーとなる原則に基づいている。各原則の実務的な導入はその下に説明されて、ITGIのガイダンスがいかにして良い実践を実現するかを追加してある。

この標準の原則[2]

原則1：責任

適切なガバナンス組織構造、役割と責任が、上級役員から付与されている必要がある。これにより、重要な意思決定とタスクについての明確なオーナシップと説明責任が与えられるものである。

実際上に意味すること:ビジネス（顧客）とIT（プロバイダー）はポジティブで信頼関係に基づく効果的なコミュニケーションを活用し、立証された透明性のある責任と説明責任に関して、透明性が立証されたパートナーシップモデルで協同すべきである。より大きな企業においてはIT経営委員会（しばしばIT戦略委員会と呼ばれる）が、取締役会に代わって活動し、取締役のひとりが委員長を務め、その企業におけるITの利用における評価、管理およびモニタリング、及び最重要なIT問題について取締役会にアドバイスを与えることについて非常に効果的な機構となる。中小規模の企業の役員の場合はより単純化された命令系統とより短いコミュニケーション・パスが、ITの活動を方向付けする際に、より直接的なアプローチを取るために必要である。全ての場合において、適切なガバナンスの組織構造、役割と責任が上級役員から権限付与されることが必要であり、それによって重要な意思決定とタスクに対する明確なオーナーシップと説明責任が割り当てられる。これにはキーとなるサードパーティのITサービスプロバイダーとの関係も含まれるべきである。

どのようにITGIのガイダンスは良好な実践を可能にするのか:

- 「取締役会のためのITガバナンスの手引き」と「*Unlocking Value: An Executive Primer on the Critical Role of IT Governance, 2nd Edition*」の出版物がビジネスとIT機能におけるITガバナンスに対する役割と責任について、インハウスであれアウトソースであれ、そのガイダンスを提供しており、そして効果的なIT経営（戦略）委員会の設立方法を解説している
- COBITとVal ITフレームワークにはRACI[3]チャートが入っており、取締役会メンバー及びIT関連のプロセスと活動に関する全てのキーとなるマネジメント層の、役割と責任の例を示している。
- “IT Governance Implementation Guide: Using COBIT and Val It, 2nd Edition”では、ITガバナンスの導入及び拡張時において関わる利害関係者及び他に関与する者の責任を説明している。
- COBITの“モニタリングと評価（ME）”プロセスで、ITガバナンスとITのパフォーマンスに関するモニタリングと評価に関する役員の役割が記述され、そこではゴールと目標を達成するための汎用的な手法と関連する測定指標が示されている。ME4の“ITガバナンスのモニター及び評価”は特にITガバナンス活動の監視に焦点を当てている。

---

[2] この節で議論している6つの原則の定義については、ISO/IEC 38500:208標準を参照のこと、この標準書はANSI(25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, http://webstore.ansi.org)やその他の認可されたところから購入することが出来る。

[3] RACIチャートは、その仕事について、責任を持つ人、説明責任のある人、相談を受ける人、情報を与えられる人を説明したものである。

原則2：戦略

ゴールは戦略目標を支援して価値を生み出すことであり、同時に取締役会のリスクテイクの志向に関して伴うリスクを考慮するものである。

実際上に意味すること：ITの戦略計画策定は複雑であり、緻密な調整を必要とする。その調整は企業全体にわたり、ビジネス単位およびITの戦略計画間で行なわれる。それはまた、望まれる利益を最も達成する可能性のある計画に優先順位をつけ、資源を効果的に配分するために、不可欠なものである。
ハイレベルのゴールは実行可能な戦術計画に翻訳される必要がある、それは失敗と不意の事象の発生を最小化することを保証するものでなければならない。
ゴールは戦略目標を支えて価値を提供するために、それに伴うリスクを取締役会のリスクテイキング指向に配慮して、考慮したものである。一方、トップダウン方式で計画をカスケードダウンすることが重要である。それらの計画はまた柔軟であり、ビジネス要求とIT機会の急速な変化にも追随して適用可能であることが重要である。

なおその上に、IT能力の存在もしくは不在がビジネス戦略を可能としたり、もしくは障害となったりし得る。それ故に、IT戦略計画の策定では、IT能力について透明性をもたせ適切に計画することが含まれているべきである。これには現状のIT基盤と人的資源についての能力の評価が含まれるべきである。その評価では将来のビジネス要求への対応と、将来において競争優位を可能とし、それと/もしくはコストの最適化を可能とする技術開発についての検討が含まれる。IT資源には多くの外部の製品ベンダーやサービスプロバイダーとの関係、ビジネスを支援する重要な役割を演じるであろう一部の人材も含まれる。
戦略資源調達のガバナンスはこのように、役員レベルの指揮命令と方向付けを必要とする非常に重要な戦略計画策定活動である。

どのようにITGIのガイダンスは良好な実践を可能にするのか：

- 「取締役会のためのITガバナンスの手引き」と「*Unlocking Value: An Executive Primer on the Critical Role of IT Governance, 2nd Edition*」の出版物で、どのようにしてIT役員（戦略）委員会が効果的な戦略計画策定を企業全体にわたる戦略計画策定と整合させて行なうのか、そしてどのようにビジネスとITマネジメントが協働して、うまく成果を達成するかについて説明している。
- Val ITではIT投資マネジメントについての特別のガイダンスを提供し、そして（特に、インベストマネジメント（IM）ドメインで）どのように、戦略目標がどのようにして適切なビジネスケース（実行計画）によって支えられるのかについてのガイダンスを提供している。
- COBITの“計画と組織（PO）”ドメインで、内部及び外部のIT資源の効果的な計画策定と組織化に必要なプロセスを説明している。これには戦略策定、技術及びアーキテクチャーの計画策定、組織計画策定、投資計画策定、リスクマネジメント、品質管理、及びプロジェクトマネジメントが含まれている。ビジネスとITのゴールの整合についても説明されており、汎用的な事例によってどのようにしてそれらが全てのIT関連プロセスに対する戦略目標を支えるのかについて、産業界全体にわたる調査結果に基づいて示している。
- “Identifying and Aligning Business Goals and IT Goals”では、ビジネスゴール、ITゴール及びITプロセス間のカスケードダウンの関係をよりよく理解することを提供している。これでは堅実で有力な17の汎用的なビジネスゴールと18の汎用的なITゴールのリストを提供し、異なる分野間で検証され優先順位付けされている。その両方の間の結合情報と共に、ビジネスゴールからITゴールへの汎用的なカスケードダウンを構築する際の良い基礎を提供している。最も重要なビジネスとITのゴールの有力なリストは、異なる分野間で特定され、各分野と地理的な場所の違いによるさらなる分析で、興味ある差異を特定した。それにより実務との関連性が増大し、特定の分野で活動している企業にとって、彼らがビジネス/ITゴールの良い組み合わせを特定するための手助けとなるものとして、これらのリストを使用しようと欲するものとなった。
- “*Understanding How Business Goals Drive IT Goals*”は“*Identifying and Aligning Business Goals and IT Goals*”という調査レポート完全版の内容を要約した白書である。

原則3：取得

導入とは単なる技術的な問題だけではなく、むしろ組織変革、ビジネスプロセスの変更、教育及び変革を可能にさせることの組み合わさったものである。

実際上に意味すること：ITソリューションはビジネスプロセスを支えるために存在する。それ故に、ITソリューションを分離して考えたり、ただの‘技術’プロジェクトもしくはサービスであるというように考えたりすることのないように注意しなければならない。他方で、技術アーキテクチャーの不適切な選択、現在の適切な技術アーキテクチャーの維持の失敗、もしくはスキルのある人材の欠如は、プロジェクトを失敗させ得るし、ビジネス活動の継続不能や、そのビジネスへの価値の減少という結果になり得る。IT資源の取得は、より広範囲のITが可能とするビジネス変革の一部として検討されなければならない。取得された技術はまた、既存のそして計画されたビジネスプロセスとIT基盤と共に維持され運用されなければならない。
導入もまた単なる技術の問題ではなく、むしろ組織変革、ビジネスプロセスの見直し、及び変革に関する訓練と実現との組み合わせである。それ故に、ITプロジェクトはより広範囲の企業全体の変革プログラムの一部として着手されるべきであり、その変革プログラムには、成果の成功を保証するために役立つために要求される全ての範囲の活動を満足させる、その他のプロジェクトも包含されるものでなければならない。

どのようにITGIのガイダンスは良好な実践を可能にするのか：

- IMドメインにおいて、Val ITではITが可能にするビジネスへの投資のガバナンスとマネジメントに関するガイダンスを提供している。この投資はそのビジネスの全ライフサイクル（取得、導入、運用及び廃止）にわたるものである。ポートフォリオマネジメント（PM）のドメインでは、そのような投資における効果的なポートフォリオとプログラムマネジメントをいかにして適用するかを述べており、それによって便益がもたらされ、コストが最適化されることを保証するために役立つものとなる。
- COBITのPOドメインでは導入計画策定のガイダンスを提供しており、それには投資計画策定、リスクマネジメント、プログラム及びプロジェクト計画策定、品質計画策定が含まれている。
- COBITの取得と導入（AI）ドメインでは、ITソリューションの取得と導入に必要なプロセス、要求定義をカバーすること、導入可能なソリューションを特定すること、文書化を準備させること、及び新システムを稼動させるためのユーザー及び運用を訓練し動作可能とすることについてのガイドラインが提供されている。加えて、そのソリューションがテストされ適切にコントロールされて、変更がビジネス及びIT環境に適用されることを保証するために役立つガイダンスが提供されている。
- MEドメインでは、どのように役員が取得プロセス、及び取得が適切にマネジメントされて実行されたことを保証するために役立つ内部統制のモニタリングと評価が、いかにしてできるかについてのガイダンスを提供している。

原則4：パフォーマンス

2つの重要なガバナンスの成功要因とは、利害関係者によるゴールの承認と、役員とマネジャーがゴール達成に対する説明責任を引き受けることである。

実際上に意味すること：効果的なパフォーマンス測定は2つのキー側面に依存する。それはパフォーマンスゴールの明確な定義と、ゴール達成をモニターするための効果的な評価尺度である。またパフォーマンス測定プロセスには、パフォーマンスが矛盾なくそして信頼されるモニタリングがされていることを保証することに役立つことが要求される。ゴールがトップダウンで設定され、ハイレベルで承認されたビジネスゴールと整合し、そして評価尺度がボトムアップで確立され、全てのレベルにおけるゴールの達成がマネジメントの各層でモニタリングされることを可能とする方法で整合していることで、効果的なガバナンスが達成される。ガバナンスの2つの重要成功要因とは、利害関係者によって承認されていることと、ゴールの達成に対する説明責任が役員とマネジメント層で引き受けられていることである。ITは複雑で技術的なテーマである。このため、ゴール、評価尺度とパフォーマンスの報告が利害関係者にとって意味のある言語で表現されて透明性を達成することが重要であり、これによって適切な行動が取られることになる。

どのようにITGIのガイダンスは良好な実践を可能にするのか:

- COBITとVAL ITのフレームワークではIT関連の全ての範囲について汎用的なゴールと評価尺度の例を提供し、それがどのようにビジネスゴールと関連するのかを説明することで、企業が自身の特定の利用に適用できるようにしている。
- COBITではマネジメント層にIT目標をビジネス目標と整合させる上でのガイダンスを提供し、これらの目標のパフォーマンスゴールと評価尺度を用いて、どのようにモニタリングするのかを記述している。

2つのCOBITのキープロセスで明確なガイダンスを提供している

- PO1“IT戦略計画の策定”はゴールの設定にフォーカスをあてている
- サービス提供とサポート(DS)1“サービスレベルの定義と管理”は、適切なサービスとサービス目標の定義、及びサービスレベル・アグリーメントにそれらを記述することにフォーカスをあてている

プロセスME1“IT成果のモニタリングと評価”で、COBITではこの活動に対する上級マネジメントの責任についてのガイダンスを提供している。

COBITでは、ITガバナンスそのものについてのモニタリングのガイダンスを、ME4“ITガバナンスのモニタリングと評価”で提供している。

- Val ITではIT投資のパフォーマンスのモニタリングについての明確なガイダンスと事例を提供している。これはビジネスケース(ビジネス実行計画)から便益の実現に至るまでの、その全経済サイクルにわたるものである。
- “IT統制の保証ガイド:COBITを利用して”ではIT統制の保証の専門家が、どのようにしてITパフォーマンスに関して役員に公平なIT統制の保証を提供できるのかについて説明している。

原則5:適合性

ITが可能とする変革、それにはITガバナンスそのものも含まれ、通常は重大な文化的及び行動上の変革を企業の中だけでなく、同様に顧客やビジネスパートナーにももたらすことを要する。

実際上に意味すること:インターネットと高度技術によって可能にされた、今日のグローバル市場において、企業はますます数を増す法的及び規制要件を遵守する必要がある。近年の企業スキャンダルや財務的な破綻によって、証券取引所において、より厳しい法律と規制の存在とその効果についての認識の高まりが存在する。
利害関係者は、企業が法律と規制を遵守し、経営環境において良いコーポレイトガバナンスに適合していることについて、よりいっそうの保証を求めている。加えて、ITが企業間における切れ目の無いビジネスプロセスを可能としているため、プライバシー、秘密保持、知的財産及びセキュリティのような領域における、重要なIT関連の要件が契約に含まれていることの保証に役立つ必要性がますます増大している。

役員は、外部要件への準拠の保証を、コストのかかる後づけとしてよりも、戦略的な計画策定の一部で扱うことが必要である。彼らはまた、トップにおいて士気を高め、マネジメント層とスタッフが従うべきポリシーと手続きを確立して、企業のゴールが実現され、リスクが最小化され、そして法令順守が達成されることを保証する必要がある。トップマネジメントはパフォーマンスと適合性の間の適切なバランスを決定し、パフォーマンスのゴールが法令順守を危うくしたり、逆に、適合性の体制が適切であって過度にビジネスの遂行を制限したりすることが無いことを保証するものでなければならない。

どのようにITGIのガイダンスは良好な実践を可能にするのか:

- COBITのコントロール目標とコントロールプラクティスで、企業における適切なコントロー

ル環境の実現とITコントロールの適切性を評価するための基礎を提供している。成熟度モデルによってマネジメント層がITプロセスの能力を評価しベンチマークを行なうことが出来るようにしている。

- COBITのプロセス、PO1 “IT戦略計画の策定”は、IT計画と、ガバナンス要件を含めたビジネス目標全体との間の整合性があることを保証することに役立つ。
- COBITのプロセス、ME2 “ITコントロールのモニタリングと評価”は、法令順守要件に合致するために、コントロールが適切かどうかを、役員が評価するために役立つ。
- COBITのプロセス、ME3 “外部要件への準拠の保証”は、外部の準拠すべき要件が特定され、役員が準拠性の方針を定め、ITの準拠性自体がモニタリングされ、評価され、企業要件への全体的な適合性の一部として報告されることを保証するために役立つ。
- “IT統制の保証ガイド：COBITを利用して”では、どのようにして監査人が独立性を持った保証を、内部ポリシー遵守と支持に対して与えられるかを説明している。この内部ポリシーは組織内の命令や外部の法的、規制、もしくは契約要件から派生するものである。これによって、タイムリーな方法で責任あるプロセスオーナーによって、どの遵守のギャップへの処置も全て修正活動が行われたことを確認することが出来るものである。
- 適合性はまた投資の意思決定も含む。Val IT、特にバリューガバナンス（VG）1と3、PM1と4、投資マネジメント（IM）4を通じて、適合性の価値とリスク及び非適合性のコストにおける適合性バランスに関する投資の保証を行なっている。

原則6：人間行動

プライバシーや不正のような問題は個人に関する増大する懸念事項である。そして、人々が利用するITを彼らが信頼しようとするならば、これら及びその他のリスクはマネジメントされなければならない。

実際上に意味すること：どのようなITが可能とする変革にも、ITガバナンス自身も含み、その導入は、通常大きな文化的及び行動上の重要な変革が必要である。それは企業の中でも、そして顧客やビジネスパートナーでも同じである。これはスタッフの間に恐れや誤解を生み出し得る。このため導入は慎重にマネジメントされる必要があり、これにより人々がポジティブに従事するようにとどまるようにする。役員はゴールについて明確にコミュニケーションしなければならず、提案された変革をポジティブにサポートしているように見られるようにしなければならない。人々の訓練とスキル向上は変革のキー側面である。とりわけ技術が急速に変動する正確の場合には重要である。人々は企業の中の全てのレベルにおいてITによる影響を受ける、利害関係者として、マネージャー及び利用者として、もしくはIT関連のサービスやソリューションをビジネスに提供するスペシャリストとして影響を受ける。その企業を超えて、ITは顧客及びビジネスパートナーに影響を与え、そしてセルフサービスおよび自動化された企業間取引を国々の間でそして国境を越えてますます可能とする。ITが可能としたビジネスプロセスが新しい便益と機会をもたらす一方で、ますます増大するリスクをもたらす。プライバシーや不正行為のような問題は個人個人にとって増大する関心事となっており、これら及び他のリスクは、彼らの利用するITシステムを人々が信頼するようにマネジメントされなければならない。情報システムは手作業の手続きを自動化することによって、劇的な影響を仕事の遂行に与えうる。

どのようにITGIのガイダンスは良好な実践を可能にするのか：
Val ITとCOBITの7つのプロセスが人間行動に関係する要件についてのガイダンスを提供している。

- Val ITの第6章、「職務上の説明責任と責任」で、投資のガバナンスに関係して要求される変革とITが可能とした変革そのものについて理解する必要を強調している。
- COBITのプロセス、PO4 “ITの組織と関係の定義”では、ITの組織と関連するプロセスをどのように構築し、全てのレベルのスタッフの要望と要求に合致させることを適切に維持するのかに説明している。
- COBITのプロセス、PO6“マネジメントの意図と指針の周知”では、ゴールと目標が明確に周知されて、働く文化がリスクとコントロールに対する正しい心構えを促進することを保

証することにフォーカスをあてている。
- COBITのプロセス、PO7“IT人材の管理”では、個人のパフォーマンスをどのように企業のゴールに整合させるべきなのか、ITスペシャリストのスキルをどのように維持すべきなのか、そして役割と責任をどのように定義すべきなのかについて説明している。
- COBITのプロセス、AI2“アプリケーションソフトウェアの調達と保守”は、人間の操作と利用の要件に合致するアプリケーションの設計を保証することに役立つ。
- COBITのプロセス、AI4“運用と利用を可能にする”は、利用者がシステムを効果的に利用できるようにすることを保証することに役立つ。
- COBITのプロセス、DS7“利用者の教育と研修”では、利用者研修のニーズがどのように特定することが出来るのか、そしてそれに応じて、ITシステムの効果的な利用を保証することについて説明している。
- COBITのプロセス、ME2“内部統制のモニタリングと評価”は、役員が、内部統制のモニタリングと、特に、人間のパフォーマンスを監督レビューによってモニタリングすることを可能としている。

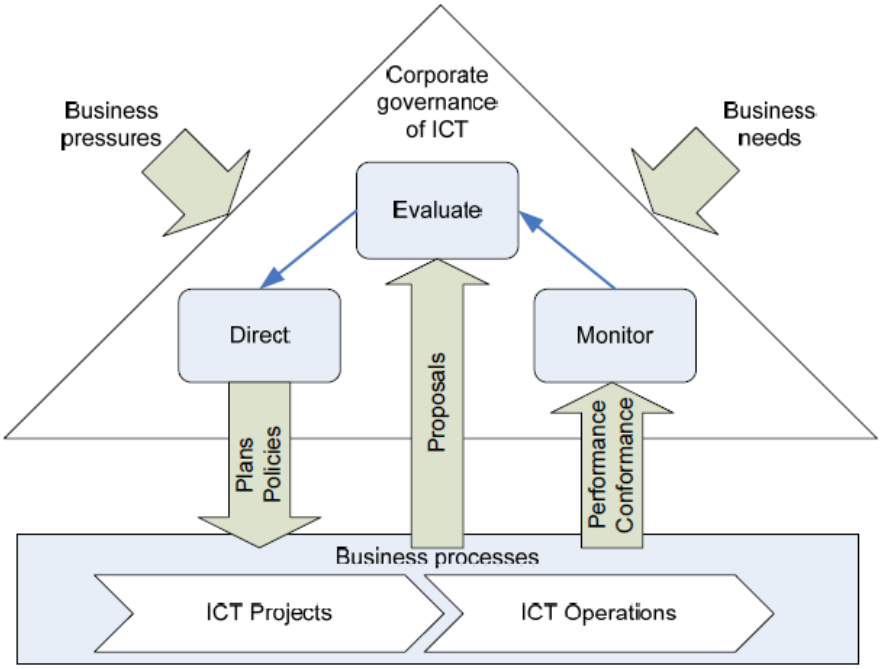
加えて、ISACAでは3つの資格認定をITガバナンスにおけるキーとなる役割を遂行する専門家に対して提供している。
- Certified in the Governance of Enterprise IT™（CGEIT™）
- 公認情報システム監査人™（CISA®）
- 公認情報セキュリティマネジャー®（CISM®）

これらの資格認定者は以上のような役割に関する能力と経験の両方を有すること証明している。

標準の適用

COBITに記述された良いプラクティスは、良いITコントロールへの共通のアプローチである。これらはビジネス及びITのマネジャー者によって導入され、監査人によって同じ基盤に基づいて保証される。

図1：ITコーポレイトガバナンスのモデル



出典：©ISO。 この図はISO/IEC38500：2008から国際標準機構（ISO）に代わって米国国立標準協会（ANSI）の許可を得て、再編集したものである。この図のいかなる部分もどのような形態で複写もしくは複製してはならず、電子的な検索システムやその他、もしくはインターネット、公的なネットワーク、衛星もしくはその他によって利用できるようにすることも出来ない。それらのためにはANSIもしくは他の権限のある組織の書面による了承が必要である。
- この標準のコピーはANSI、もしくは他の公認された販売者から購入することが出来る。ANSI：25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, http://webstore.ansi.org

この図は、ISACA/ITGI本部がANSIの許可を得て再編集したものであり、日本語版は日本規格協会から出版される文献の図を参照していただきたい。

ISO/IEC 38500では、役員が図1に示された3つのタスクを通じてITをガバナンスすべきであることを推奨している。
- 評価
- 方向付け
- モニタリング

実際上に意味すること:
効果的なITガバナンスの導入アプローチは、以下によってより容易になり最も効果的になる:
- 認められたコーポレイトガバナンスの標準と実践と整合している
- その企業のガバナンスのアプローチと整合している
- 企業におけるITに関連する活動の全ての側面を網羅している
- 全ての利害関係者によって理解されて適用可能な原則と目標に基づいている

入手可能な包括的なフレームワーク、標準, 及び実践の参照と、それらの適用と利用(文化、要求及び能力への適用)は、的確かつ効率的に適切にITガバナンス構築アプローチを支援することが出来る。

どのようにITGIのガイダンスは良好な実践を可能にするのか:
以下のITGIの資料が、ISO/IEC 38500で勧告された3つの主タスクを支援する。

評価:
- "取締役会のためのITガバナンスの手引き 第2版"と、"Unlocking Value: An Executive Primer on the Critical Role of IT Governance"の出版物で、取締役会がITガバナンスに関してすべきこと、何を網羅するか、どのような質問をするのか、そしてどのようにしてベストプラクティスと自社を比較するのかが記述されている。
- COBITとVal ITは、ITのコントロールとマネジメント活動との整合性の適切さを評価する基礎を提供し、マネジメント層がITプロセスの能力を評価しベンチマークを行なうことを可能としている。
- "ITガバナンスの導入ガイド:COBITとVal ITを利用して、第2版"の「ニーズの特定とソリューションの予測フェーズ」では、ビジネスニーズと重要なITプロセスにおけるITの評価にどのようにフォーカスするのか、それから良い実践とのギャップ分析のどのように実行するのかについて説明を行なっている。
- "COBIT Quickstart™ 第2版"では、より小規模の企業、もしくは大企業が事前に定義した基準に基づいて彼らのITのコントロールとガバナンスを評価しようと望んだときのガイダンスを提供している。
- "Enterprise Value: Governance of IT Investments, Getting Started With Value Management"は、より良いIT投資のマネジメントのためのトリガーを特定し、ビジネスニーズを評価するために役立つ。
- "Enterprise Value: Governance of IT Investments, The Business Case"は、ITガバナンスを改善するためのビジネスケース(実施計画)を策定するために役立つ。
- "IT統制の保証ガイド:COBIT®を利用して"は、アシュアランスの専門家に独立評価におけるマネジメント及び監査とレビューを実行する際の手法とテストの事例を提供している。

方向付け:

- “取締役会のためのITガバナンスの手引き 第2版”と、“Unlocking Value: An Executive Primer on the Critical Role of IT Governance”の出版物では、取締役会がITガバナンスに関して何をなし得るのかを記述し、どのようにしてそれを達成するのかについて説明している。
- COBITとVal ITでは導入のガイダンスをコントロール目標とキーマネジメントプラクティスの形で提供しており、これらは(一般的に認められた国際標準とベストプラクティスに基づいており)良いITガバナンスを可能とするものとして検討されるべきものである。
- “ITガバナンスの導入ガイド:COBITとVal ITを利用して、第2版”の「ソリューションの計画とソリューションの導入フェーズ」では、ITガバナンスの改善の設計を、どのように優先順位付け、計画し、設計するのかについて説明している。
- “COBIT® Quickstart™ 第2版”では、より小規模企業におけるコントロール、もしくはより大規模企業が良いITガバナンスに向けての最初のステップを踏み出そうと考える場合の、推奨されるベースラインを提供している。
- セキュリティが改善を必要としているキー分野である企業に対しては、“COBIT Security Baseline™ 2nd Edition”でキーITセキュリティコントロールの導入を管理するための分かりやすいガイダンスを提供しており、これによってITセキュリティの標準であるISO/IEC 27002との整合を取ることが出来る。

モニタリング:

- “取締役会のためのITガバナンスの手引き 第2版”と、“Unlocking Value: An Executive Primer on the Critical Role of IT Governance”の出版物では、効果的にITに関する企業のガバナンスをモニタリングするためにすべきことを述べている。
- COBITではITのモニタリングと評価のために推奨されるITプロセス(MEドメイン)の形でガイダンスを提供しており、これにはパフォーマンスの即敵、内部統制の有効性、外部要件の遵守、及び全般的な効果的ガバナンスの達成が網羅されている。
- COBITとVal ITには、ビジネスのゴールと目標との整合を取るための効果的なモニタリングプロセスを確立するための支援をするために、ゴールと測定指標の例が含まれている。
- “ITガバナンスの導入ガイド:COBITとVal ITを利用して、第2版”の「ソリューションの運用開始フェーズ」において、ITガバナンスを通常のビジネス運用にどのように組み込むのか、ITガバナンスの改善がうまくいっているかどうかをどのようにモニタリングし評価するのかを説明している。
- “IT統制の保証ガイド:COBIT®を利用して”では、アシュアランスの専門家にパフォーマンスと適合性についての独立した意見のマネジメントの提供、監査とレビューを実施するための手法とテスト事例を提供している。

いかにしてITGIの成果物がISO/IEC 38500の採用を支援するか

図2ではITGIの成果物がどのようにISO/IEC 38500の採用を支援するかを示している。

図2:ITGIの成果物とISO/IECとの関係

COBITはデファクト・スタンダードのコントロールモデルとして世界中で導入が進んでいる。

Val ITはITGIのガイダンスをITが可能とする投資の領域へと拡張するために導入された。

Val ITとCOBITのフレームワークの組み合わせによって効果的なITガバナンスを実現するための分かりやすい基礎が提供されている。

図2: ITGIの成果物とISO/IEC 38500の関係									
ITGIの成果物	ISO/IEC 38500の領域								
	責任	戦略	取得	パフォーマンス	適合性	人間行動	評価	方向付け	モニタリング
取締役会のためのITガバナンスの手引き 第2版	✓	✓				✓	✓	✓	✓
Unlocking Value: An Executive Primer on the Critical Role of IT Governance	✓	✓				✓	✓	✓	✓
COBIT®	✓	✓	✓	✓	✓	✓	✓	✓	✓
VAL IT™	✓	✓	✓	✓	✓	✓	✓	✓	✓
IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition							✓	✓	✓
IT統制の保証ガイド:COBITを利用して				✓	✓		✓		✓
COBIT® Quickstart™, 2nd Edition							✓	✓	
Enterprise Value: Governance of IT Investment. Getting Started With Value Management							✓		
COBIT® Security Baseline™, 2nd Edition	✓						✓	✓	
Enterprise Value: Governance of IT Investment, The Business Case			✓	✓			✓	✓	✓

COBITの中の良いプラクティスは良いITコントロールのへの共通のアプローチである。これらは、ビジネス及びITのマネジャーたちによって導入され、そして監査人によって同じ基礎の元に評価が行なわれる。何年も掛けて、COBITは無償で入手できるフレームワークとして開発され、現在はデファクト・スタンダードのコントロールのモデルとして世界中でますます適用されることが増加している。それは効果的なITガバナンスとマネジメントの導入、及びそれを証明するモデルとしてである。

最近、Val ITがITGIのガイダンスをITが可能とする投資の領域の領域へと拡張するものとして導入された。Val ITとCOBITの組み合わせは、企業のIT関連活動全体の効果的なガバナンス構成を確立するための、包括的な基礎を提供するものである。

COBITフレームワーク、Version 4.0もしくはそれ以降には以下の全てが含まれる。

- フレームワーク：COBITで、どのようにITガバナンスのマネジメントとコントロール目標、及び良いプラクティスをITドメインとプロセスで構成しているか、およびそれらとビジネス要求へのリンクを説明している。
- プロセス記述：ITが責任を持つ最初から最後までの領域をカバーしている34のプロセスを包含している
- コントロール目標： ITプロセスのマネジメント目標の汎用的なベストプラクティスを提供している
- マネジメントガイドライン：責任を割り当てることとパフォーマンス測定に役立つツールを提示している
- 成熟度モデル：ありうる現在及び将来状態を記述するITプロセスのプロファイルを提供している

その最初から、年毎にCOBITのコアとなるコンテンツは進化を続け、そして多くのCOBITを基礎とする関連文献も増大した。以下はCOBITから誕生した文献である。

- “Unlocking Value: An Executive Primer on the Critical Role of IT Governance” － 役員に何故ITガバナンスが重要であり、企業にどのようにしたら付加価値を生み出すかについての理解を深める手助けとなる
- 「取締役会のためのITガバナンスの手引き 第2版」 － 役員がITガバナンスのコンセプトをよりよく理解し、何が問題であり、最良の結果を生み出すためにどうするのかを理解するに役立つ。
- “COBIT Online®” － 利用者がCOBITをカスタマイズして自社版を作成することを可能としており、そしてそれを保存して、望むように扱えるようにしている。これにはオンラインで、リアルタイムの調査、FAQ、ベンチマーキング、及び経験や質問に関するディスカッション機能が提供されている。
- “COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition” － コントロール目標を適用する際に、避けるべきリスクと、得るべき価値についてのガイダンスを提供し、そのコントロール目標をどのように導入するかの解説を提供している。
- 「IT統制の保証ガイド：COBITを利用して」 － IT統制を保証する各種の活動を支援するためにCOBITがどのように使えるのかについてのガイダンスを提供し、全てのCOBITのITプロセスとコントロール目標に関して推奨できるテストステップを提供している。また、COBIT 4.1のコントロール目標についての自己評価を実施するためにも有用である。
- 「サーベインズ・オクスリー法（企業改革法）遵守のためのIT統制目標 － 財務報告に係る内部統制の設計と導入におけるIT の役割について（第2 版）」 － COBITのコントロール目標に基づいて、どのようにIT環境に対する法令順守の保証を行うのかについてのガイダンスを提供している。
- 「『バーゼルIIのためのIT統制目標』コンプライアンスのためのガバナンスとリスクの管理の重要性」 － ITに関連するオペレーショナルリスクについて、銀行に対するガイダンスを提供している。
- “IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition” － COBIT及びVal IT、および支援ツールキットを利用して、ITガバナンスを導入するための汎用的なロードマップとなるものを提供している。
- “COBIT® Quickstart™, 2nd Edition” － より規模の小さい企業、および大企業の最初のステップとしてのコントロールの基本的な事項を提供している。
- “COBIT® Security Baseline™, 2nd Edition” － 企業に情報セキュリティを導入する際の不可欠なステップに焦点を当てている。
- “COBIT Mappings” 現在、www.isaca.org/downloadsに掲載されているものは下記のものである。

– *Aligning COBIT® 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit*
– *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*

- *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
- *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
- *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
- *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
- *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
- *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
- *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*

・「情報セキュリティガバナンス – 取締役会と役員に対するガイダンス 第2版」 ― 情報セキュリティをビジネスの言葉で提供し、セキュリティ関連の問題を明らかにする手助けとなる、ツールと技術を収容している。

Val ITは、Val ITフレームワークに関する出版物、及び今後の関連成果物及び活動を記述するための、包括的な擁護である。

現在のVal IT関連の出版物が以下のものである。

・“Enterprise Value: Governance of IT Investments, Getting Started With Value Management” ― この出版物はビジネスとITの役員及び組織のリーダーに対して、バリューマネジメントのプロジェクトを開始する際に容易に参考と出来るガイドを提供している。
・“Enterprise Value: Governance of IT Investments―The Val IT Framework 2.0” ― COBITのフレームワークに基づき、ITが可能とした投資から、どのように企業が最適の価値を引き出すことが出来るのかを説明している。これは以下のものから構成されている。
- 3つのプロセス ― バリューガバナンス、ポートフォリオマネジメント、そしてインベストメントマネジメント
- ITのキーマネジメントプラクティス ― 望ましい結果、もしくは特定の活動の目的の達成にポジティブに影響を与える不可欠なマネジメントプラクティス

COBIT、VAL IT及び関連成果物、ケーススタディ、教育機会、ニュースレター、及び他のフレームワーク特定の、全てのそして最新の情報は、www.itgi.org, www.isaca.orag/cobit, www.isaca.org/valitにアクセスしてください。

