GOVERNANCE INSTITUTE™

COBIT®

3rd Edition

マネジメントガイドライン

2000年 7月

ITガバナンス協会 編
松尾 明 監訳
情報システムコントロール協会（ISACA）東京支部 翻訳

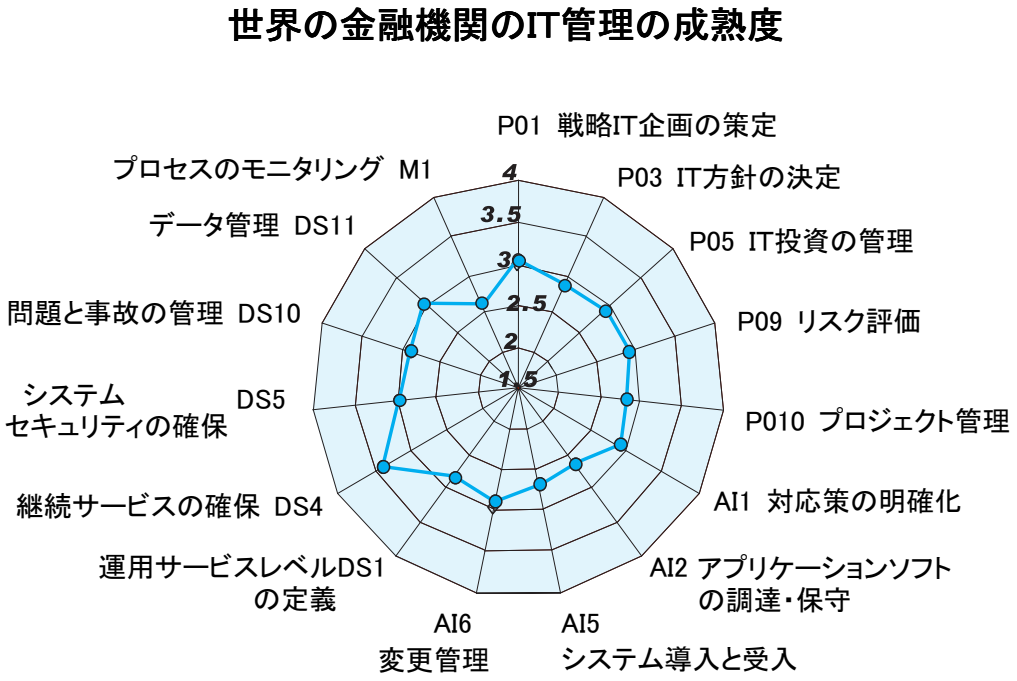
COBITのミッション

ビジネス管理者，システム監査人が日々利用する国際的に一般に公正妥当と認められる権威ある最新のITのコントロール目標を研究，開発，出版，啓蒙する

日本語監訳者のまえがき

世界の IT ガバナンスのデファクトになりつつある COBIT 第３版のマネジメントガイドラインの翻訳がやっと完成しました。このガイドラインは 2000 年の夏に出され，バランススコアカードと成熟度等を取り入れた先進的なものであり，IT 投資の戦略，戦術，管理を行なう経営者，CIO，CTO，IT コーデイネータ，システム監査，システム保証等の関係者にとってはバイブル的な役割を果たすものになってきています。

例えば，2001 年にベンチマークを行い以下のようなレーザーチャートを公開しています。経営者は自己評価の結果と他社のベンチマークを比較することによって IT のマネージメントの方向性を判断する際に貴重な情報を入手することができます。



1993 年にパリでの COBIT 方針委員会の会議でフレームワークの作成にたずさわり，目標，プロセス，資源からなるキューブ（オブジェクト）に知識を整理する方針を提案し採択されたのが昨日のように思い出されます。1996 年の第１版，1998 年の第２版まで委員として関わりましたが，今回第３版の翻訳の監訳にあたり内容をみて，それ以降よくここまで世界の知恵を集めて育ってきたと感動しています。2003 年には簡易版やオンライン版などさらに使いやすいツールが出される予定になっています。また，目標ガイド，監査ガイド等（第２版）は，ISACA 東京支部のホームページに会員向けに公開されています。ぜひ，皆様の IT ガバナンスにご活用ください。

2003 年 4 月

松尾　明

MANAGEMENT GUIDELINES

COBIT 第 3 版マネージメントガイドラインの出版に寄せて

日本では，2002 年にインターネット世帯普及率が 50%を超え，2003 年中には ADSL などの常時接続世帯数が 1,000 万となることが予想されており，ネットワーク社会が実現しつつあります。一方，金融や航空では，利用者を巻き込んだ大規模な情報システムのトラブルや SQL Slammer ウイルスによる広域のトラブルなど新しい問題が相継いで起きています。このような環境の中で，システム監査や情報セキュリティに注目が集まっています。2002 年には，ISO/IEC17799:2000 の JIS 化，ISMS 制度の発足および 2003 年の情報セキュリティ監査制度の発足など，情報セキュリティ分野では大きく環境が変わりました。この中で，COBIT は，1996 年の初版の発行以来，専門家の中ではデファクト的な存在としてリファーされ，翻訳が待たれていました。今回，出版されました COBIT 第 3 版マネージメントガイドラインは，企業や組織の中で，IT をコントロールしていくための管理者向けのガイドラインです。COBIT は IT のコントロール・オブジェクティブを中心として，今回のガイドラインと監査基準の 3 部作で構成されています。この COBIT 第 3 版マネージメントガイドラインは，企業や組織の IT 戦略，IT 管理，IT ガバナンスなど，さまざまな場面を想定しており，IT 分野の多くの方のお役に立てるものと思います。

ISACA 東京支部会長
原田　要之助

目　次

Information Systems Audit and Control Foundation
IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: research@isaca.org
Web sites: www.ITgovernance.org
www.isaca.org

MANAGEMENT GUIDELINES

COBIT STEERING COMMITTEE

Erik Guldentops, S.W.I.F.T. sc, Belgium
John Lainhart, PricewaterhouseCoopers, USA
Eddy Schuermans, PricewaterhouseCoopers, Belgium
John Beveridge, State Auditor's Office, Massachusetts, USA
Michael Donahue, PricewaterhouseCoopers, USA
Gary Hardy, Arthur Andersen, United Kingdom
Ronald Saull, Great-West and Investors Group, Canada
Mark Stanley, Sun America Inc., USA

EXPERT PANEL

William Malik, Gartner Group, USA
Jayant Ahuja, PricewaterhouseCoopers, USA
Floris Ampe, PricewaterhouseCoopers, Belgium
Mauro Eidi Villola Assano, BBA Creditanstalt, Brazil
Gary Austin, U.S. General Accounting Office, USA
Efrim J. Boritz, Ph.D, University of Waterloo, Canada
Paul Bull, KPMG, USA
Peter De Koninck, S.W.I.F.T. sc, USA
Ken Devansky, PricewaterhouseCoopers, USA
John Dubiel, Gartner Group, USA
Chris Frost, PricewaterhouseCoopers, United Kingdom
Christopher Fox, PricewaterhouseCoopers, USA
Nils Kandelin, George Mason University, USA
Werner Lippuner, Ernst & Young, USA
Stuart Macgregor, South African Breweries, South Africa
Mario Micallef, National Australia Bank, Australia
Pratapraj Oak, Fidelity Investments, USA
Daniel F. Ramos, SAFE Consulting Group, Argentina
Debra Reddish, PricewaterhouseCoopers, USA
Robert J. Reimer, PricewaterhouseCoopers, Canada
Gregory Robertson, Northrop Grumman, USA
Susana Sharp, U.S. House of Representatives, USA.
Craig Silverthorne, U.S. House of Representatives, USA
Gustavo A. Solis, Grupo Cynthus, Mexico
William Spernow, Gartner Group, USA
Mike Taylor, City of Dallas, USA
Elia Fernandez Torres, Grupo Cynthus, Mexico
Wim Van Grembergen Ph.D., UFSIA, Belgium
Winifred Whelan, PricewaterhouseCoopers, USA
Marc Wise, PricewaterhouseCoopers, USA
Roberta J. Witty, Gartner Group, USA

RESEARCH AND DEVELOPMENT SUPPORTED AND SPONSORED BY

SPECIAL THANKS to the National Capital Area Chapter for its contributions to the COBIT Management Guidelines.

SPECIAL THANKS to the members of the Board of the Information Systems Audit and Control Association and Trustees of the Information Systems Audit and Control Foundation, headed by International President Paul Williams, for their continuing and unwavering support of COBIT.

池下　秀樹	神久　治郎
石上　武志	高橋　孝治
石倉　朝之	瀧口　詠子
岩田　悦之	永井　道人
浦澤　俊雄	長尾　慎一郎
遠藤　潔	中島　貴
加藤　浩幸	中野　孝哉
金井　洋一	西垣　智裕
鹿又　洋美	野根　俊和
上川　眞一	林　　一雅
木村　章展	蓮見　孝
黒住　友香子	羽場　進
古磯　仁明	日笠　剛治
五井　孝	深田　睦子
康　理恵	深町　克実
小林　正和	藤原　学
小松　博明	古川　研吾
齋藤　英喜	前田　信男
坂下　真由美	三浦　英樹
坂本　祐輝	柳原　俊郎
佐藤　真奈	山内　重樹
猿渡　良太郎	吉田　覚
清水　惠子	龍崎　則久

（敬称略，五十音順）

Translated into Japanese from the English language version of COBIT®: ***Govemance, Control and Audit for Information and Related Technology 3rd*** Edition, Management Guide with the permission of the IT Governance Institute and the Information Systems Audit and Control Foundation. The Tokyo Chapter of the Information Systems Audit and Control Association assumes sole responsibility for the accuracy and faithfulness of the translation.

COBIT3 マネジメントガイドの英語版の日本語への翻訳は IT ガバナンス協会および情報システムコントロール財団の承諾のもとに行われた。ISCA 東京支部がその翻訳の正確性と正当性に責任を持つものである。

COBIT ® Disclaimer

情報システムコントロール財団，IT ガバナンス協会およびスポンサーは，本 COBIT マネジメントガイドラインを主としてコントロール専門家の研修用資源としてデザイン，制作，出版するものであり，これを利用することによって必ず成果が出ることを保証するものでない。

エグゼクティブ サマリー

組織が必要とする情報を提供するための情報テクノロジを，どのようにしたらうまくコントロールすることができるか。どのようにさまざまなリスクを管理し，極めて依存度の高まっているインフラの安全性を維持できるのか？ このような経営戦略レベルの幅広い問いかけは経営者が直面している多くの課題と同様に，次のような典型的な質問に分けることができる。

- **重要な課題／問題は何か。**
- **対応策は何か。**
- **それはどのような内容か。**
- **うまく動くだろうか。**
- **どのようにすればよいのか。**

このような課題を取り扱うための方法論を「COBIT フレームワーク」は提供している。COBIT は「Control Objectives for Information and related Technology」の略称であり，IT ガバナンス協会が作成し普及を図っている情報テクノロジを管理するためのオープンスタンダード(公開標準)である。このフレームワークでは，上位レベルからプロセスをコントロールするアプローチの対象として，34 の情報テクノロジ(IT)プロセスを明らかにするとともに，34 の IT プロセスを評価するための 318 の詳細なコントロール目標および監査ガイドラインを明らかにしている。 このフレームワークは，優れた IT セキュリティおよびコントロール手続を行うための一般に適用可能で広く認知された標準を提供することによって，おのおのの組織において適切なレベルの IT セキュリティおよびコントロールを決定しモニタリングする任にあるマネジメントのニーズに応えるものである。

IT ガバナンス協会は，世界中の業界専門家，アナリストおよび大学の研究者と共同して行った最先端の研究に基づき，このフレームワークの充実を図った。この結果 COBIT マネジメントガイドラインが完成し，成熟度モデル，主要成功要因(CSF)，重要目標達成指標(KGI)および重要成果達成指標(KPI)が盛り込まれた。また，IT を測定できる形で管理したいというマネジメントのニーズに応えて，COBIT の 34 の IT プロセス毎に組織の IT 環境を評価・測定するツールを提供することによって，従来よりもかなり改善されたフレームワークになった。

IT やネットワークの分野は技術革新が激しく，そのため IT 関連のリスクをもっと適切に管理することが強く求められている。 事業の中核となるビジネスプロセスを支援していくためには，どうしても電子情報および IT システムに頼らざるを得ない。ビジネスを成功させるために，組織全体に広がっている複雑なテクノロジをより適切に管理し，ビジネスニーズに迅速かつ安全に応える必要がある。 加えて規制面では，より厳しい情報管理を行うことが義務付けられ始めている。情報システムの事故や電子的な不正事件が明るみに出ることが多くなるにつれ，この傾向に拍車がかかっている。IT 関連のリスクマネジメントは今や，企業が行うコントロール活動(エンタプライズ・ガバナンス)のかぎとなる重要な要素であることが理解され始めている。

企業のコントロール活動(エンタプライズ・ガバナンス)において IT とそのプロセスにおけるリスクと効果のバランスをとりながら，付加価値を高め企業目標を達成するうえで，

MANAGEMENT GUIDELINES

IT ガバナンスは，ますます重要性が高まっている。IT ガバナンスは，さまざまな企業プロセスに対して効率的・効果的で計測可能な改善を保証し，企業コントロール活動を成功させるために必要不可欠である。IT ガバナンスによって，IT プロセス・IT 資源および情報は企業戦略と目標に関連付けられることになる。 さらに，IT にかかわる計画と組織，調達と導入，サービス提供とサポート，そしてモニタリングにかかわるベストプラクティスを統合化することによって，情報テクノロジが経営目標と整合性が取れるようになる。このように，IT ガバナンスによって企業の情報活用の面での優位性を高めることができ，企業は利益を最大化し，ビジネス機会を利用して，競争上優位に立つことが可能になる。

グローバル経済の e エコノミー化が進展し，IT の相互連結や IT の利用範囲がますます広がるにつれて，リスクマネジメント全体が，特定のマネジメント手続に依存するようになっている。複雑な環境の中で，経営者は，リスクとコントロールに関して困難な決定を，迅速にそして適切に行うため，要約されたタイムリな情報を常に求めている。 下の表はいくつかの経営者の伝統的な問いかけに対して，その答えを得るために利用できる経営者のための情報ツールキットを示したものである。

経営者の問いかけ

責任あるマネージャが「船を正しい方向に運航させる」ためにはどのようにすればよいか？	DASHBOARD ダッシュボード
最も多くの利害関係者が満足しうる結果を達成するにはどうすればよいか？	SCORECARDS スコアカード
企業環境の動向と展開に対してどのようにタイムリに組織を適合させていくのか？	BENCHMARKING ベンチマーキング

ただし，ダッシュボードには“指標”が，スコアカードにはスコアを測定する“評価尺度”が必要であるし，ベンチマーキングには比較のための“物差し”が必要となる。これらを情報管理のために提供することが，「COBIT マネジメントガイドライン」の開発の主要な目的である。

自社の IT システムの状況を理解し，どのようなセキュリティとコントロールを備える必要があるか判断することは，すべての組織に基本的に必要とされることである。必要とされるコントロールレベルを理解することもその判断を下すこともいずれも簡単な課題ではない。自社のレベルを客観的に把握することは容易ではない。 何を，どのようにして計測すべきなのか？ 組織が現在どのレベルにあるかを測定する必要性に加えて，IT セキュリティおよびコントロールの分野では間断のない改善が重要であるし，この改善をモニタするための管理ツールが必要である。また適切なレベルは何かを決めることも同じように難しい。 企業ならびに公的機関の上級管理者は，情報インフラのコントロールとセキュリテ

ィを改善するための支出に際して，他社事例を検討することをしばしば要求される。全員が時折以下のように自問しているはずであり，これに異議を唱える人はほとんどいないだろう。

「どこまで投資すべきか？，コストに見合う効果が得られるだろうか？」

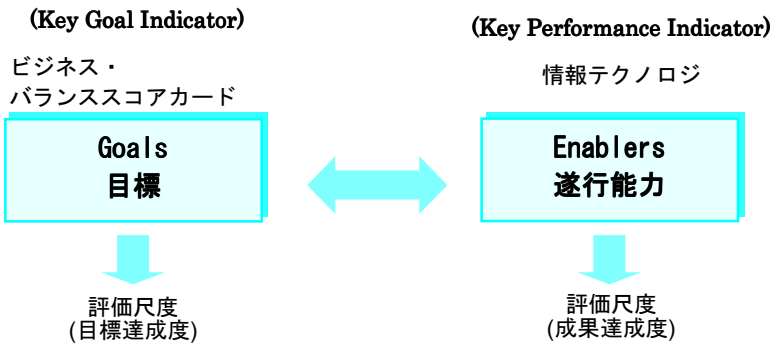
その答えを「COBIT マネジメントガイドライン」 は提供する。このガイドラインは汎用的で実践的なことを特徴としており，以下のような上級管理者の関心に応えることを目的として作成されている。

- 成果評価尺度…よい成果を表す指標は何か？
- IT コントロールのプロフィール…どれが重要か？　コントロールのための主要成功要因(CSF)は何か？
- 認知…目的が達成できなかった場合のリスクは何か？
- ベンチマーキング…他社はどうしているか？　どのように測定し，比較するのか？

適切な IT セキュリティとコントロールのレベルの決定とモニタリングの要請に対しては，次のように対応している。

- IT コントロール実務についてのベンチマーキング**(成熟度モデルとして掲載)**
- IT プロセスの目標達成度や成果達成度を評価するための**成果達成度指標**
- IT プロセスをうまくコントロールするための**主要成功要因**(CSF)

このマネジメントガイドラインは，現行の「COBIT フレームワーク，コントロール目標 および監査ガイドライン」と整合性を取って作成されている。 さらに，成果管理に焦点を当てやすくするために，「ビジネス・バランススコアカード 」(脚注 1)の原則を用いた。これによって，プロセスの成果を明確に測定するための重要目標達成指標(KGI)や，プロセスを作動させる遂行能力(Enablers)を計測してプロセス性能の良し悪しを評価するための成果達成指標(KPI)を定義することが容易にできる。今日の情報サービスに依存した環境では，IT がビジネスの主要な遂行能力(Enablers)になってきている。 このため企業目標と IT との整合性を取ることは非常に重要であり，図式化すると次のようになる。



1 “The Balanced Business Scorecard – Measurements that Drive Performance,” Robert S. Kaplan and David P. Norton, Harvard Business Review, January-February 1992

これらの評価尺度を，以下のような簡単な質問に言い換えることによって，マネジメントが自社 IT 組織をモニタリングするときの助けになる。

1. **経営者は何に関心を持っているか？**
   企業ニーズの満されていることを確認する

2. **どこでそれを測定できるか？**
   ビジネス・バランススコアカード上における KGI で測定できる（KGI はビジネスプロセスの目標達成度を表す）。

3. **IT 管理者は何に関心を持っているか？**
   IT プロセスが，ビジネスニーズを満たすように，企業に対してタイムリに適切な情報を提供していること。これは企業にとっての主要成功要因(CSF)である。

4. **どこでそれを測定できるか？**
   IT バランススコアカード上における KGI で測定できるる。この KGI は IT の目標達成度を表しており，情報が適切な形で提供されていることを示す（有効性，効率性，機密性，万全性(インテグリティ)，可用性，遵守性および信頼性)。

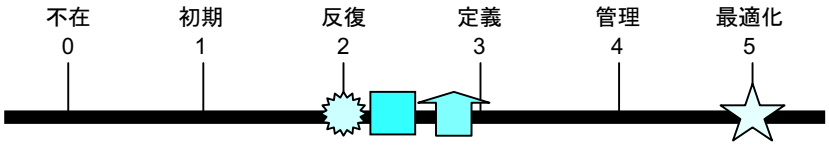
5. **他に測定する必要があるものは？**
   IT プロセスの KPI を測定する必要があると判断された複数の CSF が，ビジネスプロセスの目標達成に積極的な影響を与えていること。

成熟度モデル

IT プロセスを管理するための成熟度モデルは，今回初めて作成されたものであり， 自社組織を，「コントロール不在」から「コントロール最適化」まで(0 から 5 まで)の 6 レベクでスコアリングする方法を採用した。 この方法は，ソフトウェア工学研究所 がソフトウェア開発能力の成熟度(脚注 2)のために定義した成熟度モデルに基づいている。COBIT の 34 の IT プロセス用に作成された 1 から 5 の成熟度レベルに合わせて，マネジメントは自社組織のレベルを測ることができる。

- **組織の現状…組織の現在のポジション**
- **業界(の中の最優秀企業)の現状…比較**
- **国際基準の現状…追加比較**
- **改善に関する組織の戦略…組織が目指すあるべきポジション**

2 “Capital Maturity Model for Software,” Version 1.1 Technical Report CMU/SEI-93-TR-024, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, February 1993



凡例

現行

国際標準ガイドライン

業界ベストプラクティス

目標

凡例

0：不在 ------管理プロセスは全くない
1：初期 ------管理プロセスは場当たり的で組織的ではない
2：反復 ------管理プロセスが標準的なパターンに従うようになる
3：定義 ------管理プロセスは文書化され、周知されている
4：管理 ------管理プロセスはモニタリングされ、評価測定されている
5：最適化 ---管理プロセスは、ベストプラクティスに従っており、また自動化されている

主要成功要因(CSF)

主要成功要因(CSF)は，マネジメントがITプロセスのコントロールを達成するための最も重要な事項あるいは行動を表している。CSFはマネジメント指向の導入ガイドラインであるとともに，戦略面，技術面，組織面，あるいは手続の面で最も重要な事項でなければならない。

重要目標達成指標(KGI)

重要目標達成指標(KGI)は，ITプロセスがその業務要件を達成したかどうかを事後的に経営者に示す評価尺度を定める。通常，次のような情報規準の用語を用いて表される。

- ビジネスニーズを支援するために必要な情報の可用性
- 万全性(インテグリティ)の欠如および機密性に関するリスク
- プロセスとオペレーションのコスト - 効率性
- 信頼性，有効性および遵守性の確認

重要成果達成指標(KPI)

重要成果達成指標(KPI)は，ビジネス目標を達成できるように，ITプロセスがいかに有効に機能しているかを評価するための評価尺度を定める。ビジネス目標が達成される可能性があるかないかを示す先行指標であるとともに，能力，手続およびスキルに関する優れた指標でもある。

「マネジメントガイドライン」では，CSF，KGIおよびKPIについては簡潔に，焦点を絞って記述されており，「COBIT フレームワーク」(付録Ⅱ参照)で提示されている上位レベルのコントロールのガイドラインを補足する構成となっている。ITがビジネス上必要とする情報を提供することによって，ビジネスを遂行させていることを示している。

要約すると，「マネジメントガイドライン」は，マネジメントのために企業の情報，プロ

セス，テクノロジの管理レベルを維持する以下のような，実践的で汎用的なガイドラインを定めることに焦点を当てて作成されている。

- **成熟度モデル**…戦略的な意思決定をベンチマークによって他と比較ができる。
- **CSF**…IT プロセスを適切にコントロールすることができるようにする。
- **KGI**…IT プロセス全体の目標達成状況をモニタリングすることができる。
- **KPI**…個々の IT プロセスの成果達成状況をモニタリングすることができる。

電子商取引およびテクノロジへの依存がますます高まる時代においては，組織はより高いレベルのセキュリティおよびコントロールを達成していることを示さなければならない。すべての組織が自己の成果(パフォーマンス)を認識し，その達成状況を評価しなくてはならない。ベンチマーキングや競合相手，自社の企業戦略と照らして達成レベルを測定することは，IT セキュリティおよびコントロールのレベルを他と競争できるレベルまで引き上げるための一つの方法である。「COBIT マネジメントガイドライン」は，成熟度モデル，実務的な主要成功要因および成果評価指標などを示すことによって，実践的な指針を経営者に提供することによって以下の永遠に繰り返される質問に答えるものである。

「わが社の目標達成を支援する IT に対する適切なコントロールのレベルはどのようなものだろうか？」

フレームワーク

1. 成熟度モデル

企業や公的機関の上級マネジメントは，情報インフラストラクチャのコントロールに必要な資源の投下を行う際に，ビジネスケース（その効果の説明）を検討することを求められることが多い。きっと全員が以下のように自問しているはずであり，これに異議を唱える人はほとんどいないだろう。

「どこまで投資すべきか，コストに見合う効果が得られるだろうか？」

この疑問に答えるために，さらに，密接に関連した次の問いかけがよくなされる。

「国際標準と言われているものにはどのようなものがあるのだろうか？　国際標準から見て，わが社はどのように位置付けられるのだろうか？」
「他社の動向は？　他社に比べてわが社は進んでいるのか，それとも遅れているのか？」
「業界のベストプラクティスとはどのようなものか？　わが社は大きく遅れているのか，それとも大差ないのだろうか？」
「外部と比較して，わが社は情報資産を保護するために『合理的な』保護策を講じているといえるだろうか？」

このような問いかけに対してこれまで有意義な回答をすることが難しかったのは，評価に必要なツールが提供されていなかったためである。

IT 管理者は，業務効率化のノウハウを知るため，ベンチマーキングや自己評価用のツール類に絶えず目を光らせている。最初から COBIT のプロセスとプロセス管理のためのコントロール目標を使えば，コントロール目標に対するベンチマークはとてもやりやすくなるはずである。そして COBIT は次のような三つのニーズに応えることができる。

(1) 組織の現状を把握するための相対的な評価指標が欲しい。
(2) 効率的な目標設定の方法を知りたい。
(3) 目標に対する進捗度を計るためのツールが欲しい。

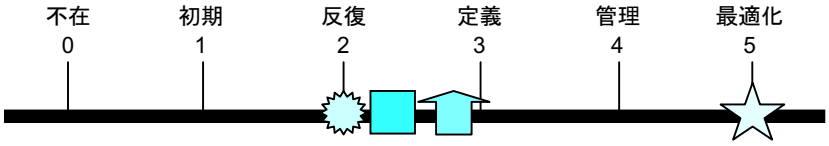
COBIT フレームワークでは，全体で 34 の IT プロセスが定義されている(付録Ⅱ参照)。おのおののプロセスには，プロセス全体のコントロール目標の内容説明が一つあり，さらに詳細なコントロール目標が 3 から 30 設定されている。プロセスオーナは，簡単な自己評価を行った場合でも第三者によるレビュー結果を参照する場合でも，コントロール目標の達成レベルを判断することができるはずである。マネジメントは，自社の属する業界や環境と比較し，または国際標準および規制の展開(将来の実現の可能性)分野と比較したりして，これらの状況をふまえたうえで判断したいと考えるであろう。経営者に対する要旨報告で，その判断結果を簡単に利用できるようにするために，図表を用いたプレゼンテーション手法を提供する必要がある。そして，その結果は将来計画のシナリオ作りに役立つであろう。

IT プロセスを管理するための成熟度モデルへのアプローチでは，「不在」から「最適化

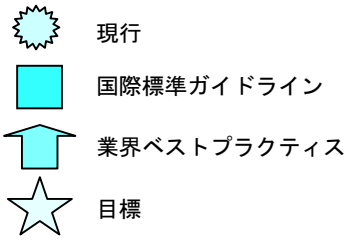
されている」(0 から 5 まで)の 6 レベルでスコアリングする方法を採用している。この方法はソフトウェア工学研究所(SEI)がソフトウェア開発能力の成熟度を測るために定義した成熟度モデルに基づいている。どんなモデルでも，その尺度はあまり細かすぎないほうがよい。使いにくいものになったり，精密な正当化しえないものを提示する恐れがあるからである。

逆に，あいまいにならない程度のいくつかの条件に基づいて設定される，成熟度レベルに絞り込む必要がある。COBIT の 34 の IT プロセス用に開発された 1 から 5 までのレベルを用いて，マネジメントは次の項目に関してスコアリングすることができる。

- 組織の現状……組織の現在のポジションの把握
- 業界(業界最大手)の現状……業界内のベストプラクティスとの比較
- 国際標準のガイドラインの現状……国際標準との比較
- 改善に関する組織の戦略……組織が目指すポジションの把握



凡例



凡例

0：不在 ----- 管理プロセスは全くない
1：初期 ----- 管理プロセスは場当たり的で組織的ではない
2：反復 ----- 管理プロセスが標準的なパターンに従うようになる
3：定義 ----- 管理プロセスは文書化され、周知されている
4：管理 ----- 管理プロセスはモニタリングされ、評価測定されている
5：最適化 -- 管理プロセスは、ベストプラクティスに従っており、また自動化されている

34 の IT プロセスには，それぞれ「0」から「5」までの段階的な評価尺度が作成されている。評価尺度のもととなっているのは，次のような「不在」から「最適化されている」までの一般的な定義を述べた「一般成熟度モデル」である。

一般成熟度モデル
0：不在 コントロールが存在しない状態。識別できるコントロールプロセスが全くない。それらの課題があることすら認識されていない **1：初期状態** コントロールとしては初期の状態。課題があること，検討が必要であることは認識されている証はある。標準化されたプロセスはないが，その代わりに個々の担当者ベースあるいは「ケースバイケース」で適用されるその場対応型のアプローチがある。

マネジメントを志向した全体的なアプローチは整備されていない。

2：再現性あり

コントロールに再現性がある状態。同じ仕事をしているいろいろな人々によってよく似た手続がとられる段階にまで，プロセスが進歩している。標準化された手続を研修する教育訓練や手続の周知徹底に関する正規の手続は定められておらず，実行責任は個々の担当者に委ねられている。個々の担当者の知識に依存する度合いが高く，そのためにミスが起きやすい。

3：定義されている

コントロールの定義されたプロセスがある状態。手続が標準化され，文書化され，そして研修を通して周知されている。しかしながら，このようなプロセスに従うかどうかは個々の担当者に委ねられ，プロセスからの逸脱行為が検出される可能性は低い。手続自体は改善されたものではなく，既存の手続をそのまま採用している。

4：管理されている

コントロールが管理されている状態。手続に対する遵守状況をモニタリングし評価すること，プロセスが効果的に機能していないと思われる場合には，アクションを取ることが可能である。プロセスは，常時改善されており，グッドプラクティスといえるレベルに達している。自動化やツールの活用は，限定された範囲で部分的に実施されているだけである。

5：最適化されている

コントロールが最適化されている状態。絶間ない改善，他社との成熟度ベンチマーキングの結果，プロセスがベストプラクティスのレベルにまで高められている。IT の利用方法は，ワークフローを自動化する統合的レベルに達しており，品質と有効性を改善するツールを提供するとともに，企業の環境適応力の迅速化に貢献している。

CobiT は IT 管理者を対象にした一般的なフレームワークであり，その評価尺度は実用的かつ合理的で分かりやすいものである必要がある。しかしながら，IT 管理プロセスにおけるリスクと適切なコントロールに関する事項は，本来，主観的で厳格さに欠ける面があるため，ソフトウェア工学向けの成熟度モデルほど，機械工学的なアプローチは必要ではない。

成熟度モデルの強みは，経営者による自己評価が比較的簡単に行える点，成果を改善する必要がある場合に，その改善課題の発見が比較的容易な点にある。プロセスが全く存在しないということもありうるので，評価尺度には 0 から 5 までが存在する。0 から 5 までの評価尺度は，プロセスが「不在の状態」から「コントロールが最適化された状態」までどのように発展していくかを表す，単純な成熟度評価尺度を基礎にしている。ここでいうプロセスは管理プロセスを指し，その成熟度や能力の向上は，リスクマネジメントや効率性の向上と同じ意味になる。

成熟度モデルは，管理プロセスがどの程度発展しているかを測る一つの方法である。本来あるべきレベルは，前述のようにビジネスニーズによって異なる。評価尺度は一つの実務的な例であり，ある管理プロセスにおける成熟度レベルに応じた典型的な体系が示されている。COBIT フレームワークの中の情報規準(付録 II 参照)を利用することによって，手続の現状調査を行う際に，正しい管理の側面に焦点を絞ることが確認できるようになる。例えば，計画立案や組織化は有効性，効率性といった管理目標に焦点を絞ることになる。これに対して，システムセキュリティの保証は機密性と万全性(インテグリティ)の管理が目標となる。

成熟度モデルの物差しは，IT 専門家が管理者に対してどこに IT 管理上の欠点があるかを説明するのに役立ち，また組織のコントロール手続とベストプラクティスを比較することによって，達成すべき目標を設定するのに役立つ。適切な成熟度レベルは，企業の経営目標および事業環境によって異なる。特にコントロールの成熟度レベルは，IT に対する企業の依存度，IT 技術の使い勝手，そして特に情報の価値によって異なってくる。

セキュリティやコントロールを改善する場合に，組織として戦略上見落としてはならないポイントに，公表されている国際標準や業界のベストプラクティスの調査がある。今日の最先端のレベルは明日の期待された成果レベルになり得る。それゆえに組織がいずれ将来どのレベルを目指すべきか決めるために有意義なものである。

成熟度モデルは一般成熟度モデル(上記参照)からスタートし，各レベルに対して，以下の領域における手続や原則が徐々に追加されてゆく。

- リスクとコントロールに関する課題の理解と認識
- 課題解決に必要な研修とコミュニケーション
- 導入されているプロセスと手続
- プロセスをより効果的，効率的にするための手法や自動化への取組み
- 社内の方針，法律，規制の遵守状況
- 利用されている専門的技術のタイプと範囲

次の表は，異なる領域別にそれぞれのレベルで適用される業務を示している。これが，一般成熟度モデルとともに多くの IT プロセスに適用可能な成熟度モデルとなる。

	理解と認識	研修とコミュニケーション	プロセスと手続	技法と自動化	遵守状況	専門的技術
1	認知	課題に対する散発的なコミュニケーション	プロセスや手続に対する，その場対応型のアプローチ			
2	自覚	全社的な課題およびニーズについてのコミュニケーション	まだ直感的なプロセスであるが，類似性，共通性があるものが現れてくる	共通ツールの出現	個別の課題に対する一貫性のないモニタリング	

	理解と認識	研修とコミュニケーション	プロセスと手続	技法と自動化	遵守状況	専門的技術
3	行動の必要性に対する理解	インフォーマルな研修によって，個々の担当者の取組みを支援している	手続が定められ，標準化，文書化がされており，よりよい事例の共有化が始まっている	ツールが標準化され，現在利用できる実務に使われ制度化されている	一貫性のないモニタリングが行われているが，客観的な尺度が導入され始めている。バランススコアカードは時々利用されているが，原因分析は未熟である	ビジネスプロセスにIT スペシャリストが関与している
4	すべての要件についての理解	正式な研修によって，管理されたプログラムが提供されている	プロセスオーナおよび実行責任者が設定されていて，プロセスは健全かつ完全である。社内のベストプラクティスが適用されている	成熟した技法が使われており，標準ツールが制度化されている。また，限定的だがテクノロジを戦術的に利用している	いくつかの分野ではバランススコアカードが利用されており，例外事項が検出されている。また，原因分析は標準化された方法で行われている	社内のすべての主要な分野における専門家が関与している
5	さらに上を目指した前向きな理解	社外のベストプラクティスや最先端の概念を取り込むような研修およびコミュニケーションが実施されている	社外のベストプラクティスが適用されている	洗練された技法が広く利用されており，テクノロジの最適利用が広くなされている	バランススコアカードがグローバルに利用されており，例外事項は一貫した方法で検出，処理されている。また，原因分析は常時行われている	社外のエキスパートや業界のリーダに依頼し，指導を受けている

成熟度モデルを要約すると，以下のとおりである。

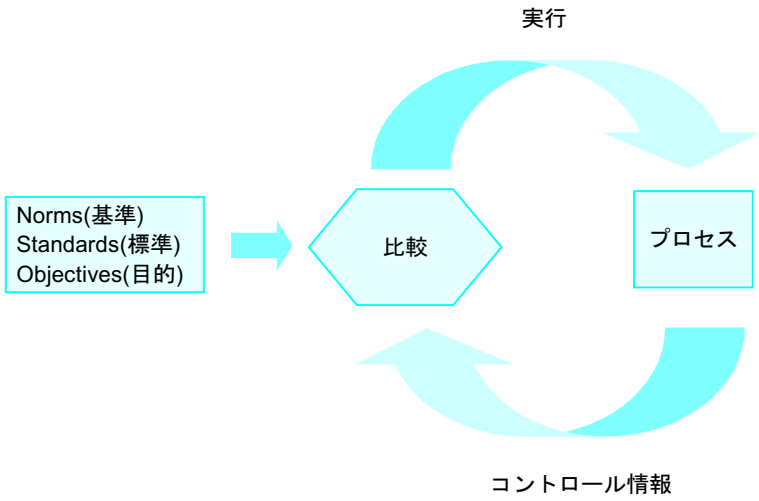
- さまざまな成熟度レベルにおけるビジネス上のニーズとその実現の方向性に言及している。
- 実際に他と比較する場合に役立つツールである。
- 簡単に違いを見つけることができるツールである。
- IT ガバナンス，セキュリティおよびコントロールに関連する，企業の「プロフィール」とみなすことができる。
- IT ガバナンス，セキュリティおよびコントロールの成熟度について，「現状」と「あるべき姿」をマッピングするのに役立つ。
- 選択したレベルを達成するために何をすべきかを決定する，ギャップ分析に適している。
- 下のレベルとの間に極端に差があるようなレベルを設けることは，できる限り避けている。
- 主要成功要因(CSF)の適用を加速化させる。
- 特定の業界に特化したものではなく，いつでも該当するものになるとは限らない。ビジネスのタイプによってどれが適切かの判断を要する。

2. 主要成功要因(CSF)

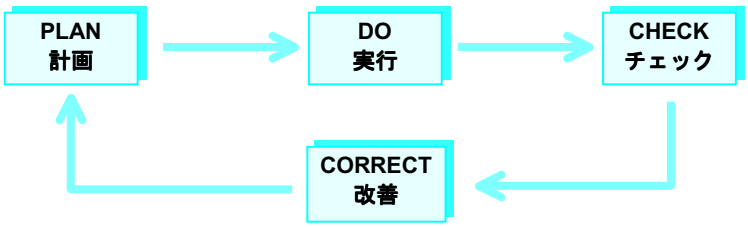
主要成功要因(CSF)は，経営者が IT およびそのプロセスにかかわるコントロールを導入する際の手引きを提供するものである。CSF は IT プロセスの目標達成に不可欠な最重要事項であり，戦略，技術，組織，プロセスあるいは手続などの要素を併せ持った行動指標である。CSF は通常，いろいろな能力やスキルと関係するが，簡潔で焦点が絞り込まれ行動に直結すると同時に，検討中のプロセスにおいて最も重要な経営資源に的を絞ったものでなければならない。

次の標準コントロールモデルを(理解の)手引きとしていただきたい。このモデルは，室温(コントロール情報)を常時チェックして(比較)，もっと熱を供給するように信号を送る(行動)暖房システム(プロセス)で室温(標準)を設定する場合と同じような，周知の原則に従って構成されている。このモデルと原則によって，何を標準とするのか，標準の設定者は誰か，誰がコントロールするのか，それに従って行動する人は誰かなどのすべてのプロセスに共通する，いくつもの CSF が明らかになる。それ以外にも以下のようなものがある。

- 定義され明文化されたプロセス
- 定義され明文化された方針
- 明確な説明責任
- 経営者の強力な支援／責任関与(コミットメント)
- 社内外の関係者との適切なコミュニケーション
- 一貫した評価手続



このようなコントロールの原則は異なったレベルで，すなわち戦略レベル，戦術レベル，管理レベルにおいて必要とされていることに留意する必要がある。互いに論理的に連続している計画・実行・チェック・改善という 4 活動が常に各レベルで存在する。各レベル間でのフィードバックとコントロールのメカニズムは当然検討されるべきである。例えば，戦略レベルの「実行」は戦術レベルの「計画」のもとになり，管理レベルの「チェック」は戦術レベルの「チェック」に統合される。

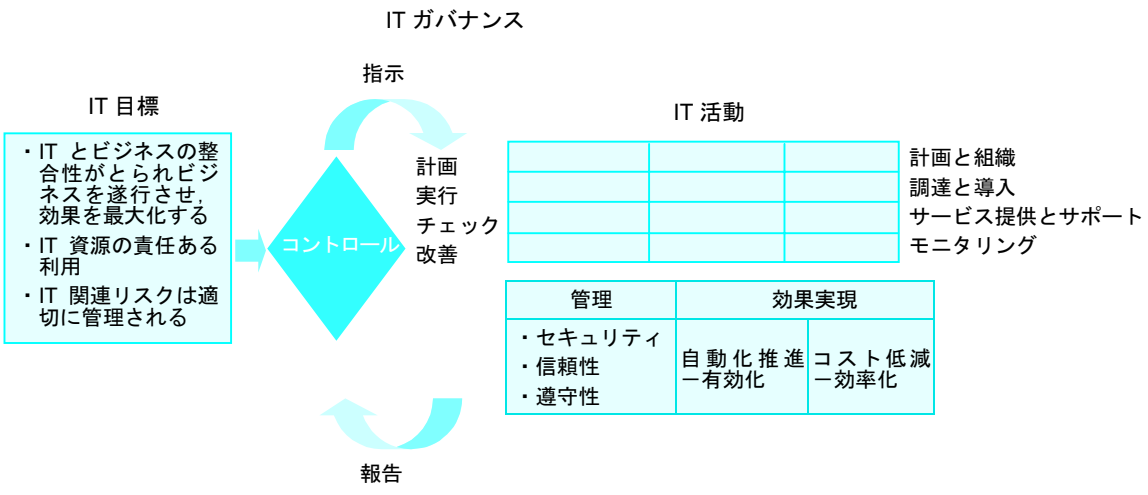


「IT ガバナンスフレームワーク」のコントロール目標やモニタリングガイドラインを熟読すれば，CSF 策定のためのより深い理解ができる。IT ガバナンスの実行責任は経営者や株主にある。IT ガバナンスは，経営目標の達成を保証するコントロールシステムである。IT ガバナンスでは通常，いくつかのシンプルな基準(norm)に照らして報告された業績をレビューし，組織の IT の方向付けをするが，この基準(norm)では次の事項が必要となっている。

- IT とビジネスとの整合性が取られていること
- IT がビジネスの成功要因になっており，かつ利益を最大化していること
- IT 資源が責任を持って利用されていること
- IT 関連リスクが適切に管理されていること

標準コントロールモデルにおいては，チームリーダはマネージャに報告するとともにマネージャから指示を受け，またマネージャは幹部役員に報告を上げ，幹部役員は取締役会に報告するというように，通常異なるマネジメント層にまたがることになる。目標からの乖離を示す報告には，実施すべき行動の提案も通常含まれる。

次の図は，IT ガバナンスの観点から IT 目標と IT 活動の相互作用を概念的に示したものである。IT 活動は，計画・実行・チェック・改善という一般的な管理活動とともに描かれている。「COBIT コントロールフレームワーク」(付録Ⅱ参照)ができたことから，今後情報テクノロジを表す場合，①計画と組織，②調達と導入，③サービス提供とサポート，④モニタリングという COBIT の 4 領域を用いる。



標準コントロールモデルとITガバナンスフレームワークから，ITプロセスの大半に共通する，次のような多くのCSFを導き出すことができる。

IT全般への適用

- ITプロセスが定義され，IT戦略や企業目標との整合性が取られている。
- プロセスの利用者や利用者の期待が明確にされている。
- プロセスは計測可能であり，必要な資源は適切に管理されている。
- 必要な資質を備えたスタッフ(研修，情報／知識の伝承，モラルなども含めた)が確保でき，スキルの調達(採用，引き止め(継続雇用)，再教育などによる)ができる。
- ITの成果には，顧客満足度を織り込み，プロセスの有効性および将来性について財務的な観点から測定評価される。IT管理者の報酬は，これらの評価に基づいて支給される。
- 継続的に品質改善努力が行われる。

大部分のITプロセスへの適用

- すべてのプロセスの利害関係者(利用者，マネジメントなど)は，ITのリスクと重要性の両面およびITが生み出すビジネスチャンスを認識し，強いコミットメントと支援を行っている。
- 企業目標やコントロール目標は，全員に周知(コミュニケーション)され規範として理解されている。いろいろなプロセスをどのように導入し，目標をどのようにモニタリングするか，そして誰にプロセス成果の説明責任があるか，周知されている。
- 全員が目標を目指して活動しており，利用者，内部プロセス，意思決定の結果についての正確な情報が共有化されている。
- 部門を越えた協力，チームワーク，間断のないプロセス改善が奨励されるような企業文化が確立されている。
- 主要なプロセスは統合化され整合性が取られている。例：変更管理，障害管理，構成管理
- コントロール手続の目的は，資源を効率的で最適な方法で使用し，プロセスの有効性を改善することである。

ITガバナンスへの適用

- コントロール手続の目的は，内部管理上の透明性を高め，煩雑さを軽減するとともに，学習を促進し，柔軟性と拡張性を高め，かつ不正・誤謬を防止する点にある。
- 以下のコントロールの健全な監督を可能にする実務手続の適用。
  コントロール環境と文化：行動規範：標準手続としてのリスク評価：自己評価：確立された基準に従った正式な遵守性手続：コントロールの弱点やリスクのモニタリングやフォローアップ。
- ITガバナンスが認識され定義され，その活動が企業全体のガバナンスプロセスの中に統合されている。そのプロセスを通じてIT戦略，リスクマネジメントのフレームワーク，コントロールシステム，セキュリティ方針についても，その方向性が明ら

かにされている。

- IT ガバナンスによって，主要な IT プロセス，実行責任，必要資源や能力を意識した上で，企業変革や品質向上などの重要性の高い IT プロジェクトに注力することができる。
- 監査委員会が設立され，独立した監査人を選任・監督する。また監査委員会は IT 監査計画を推進し，監査結果や第三者の意見をレビューする。

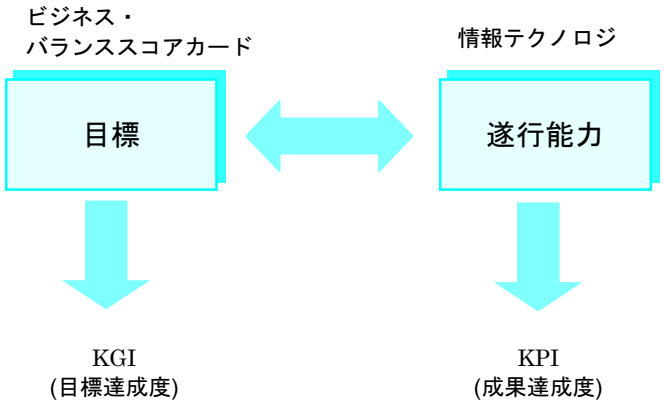
CSF を要約すると以下のとおりである。

- IT プロセスやプロセスを支援する環境に焦点を当てた重要な遂行能力である。
- 理想的な成功を得るために必要となるある事柄や条件，あるいは理想的な成功を得るために推奨される特定活動である。
- プロセスが成功する確率を向上させるために実施すべき最も重要な事柄である。
- 外部から観察できる ― 通常測定できる ― 組織やプロセスの特徴である。
- 特質として，戦略，技術，組織，手続のいずれかに属する。
- 能力やスキルを獲得，維持し，普及させることに焦点が当てられている。
- プロセスの観点で表現されればよく，必ずしもビジネスの観点で表現される必要はない。

3. KGI(重要目標達成指標)

KGI はプロセスの最終目標を意味しており，達成されるべき「何か」を評価するための尺度である。目標の達成に向けて動くプロセスの状況を表す計測可能な指標であり，数値目標として定義されることがしばしばある。

これに対して，次のセクションで取り挙げる KPI(重要成果達成指標)は，そのプロセスが「いかに良好に」実行されているかを評価するための尺度である。この KGI と KPI の関係は，バランススコアカードの考え方を使って次のように図式化することができる。バランススコアカードにも，最終目標の成果を計測するための評価尺度，そして最終目標の達成を可能にする遂行能力に関連した成果の評価尺度が必要とされている。このような関係においては，IT がビジネスの主要な遂行能力であることを念頭においておく必要がある。

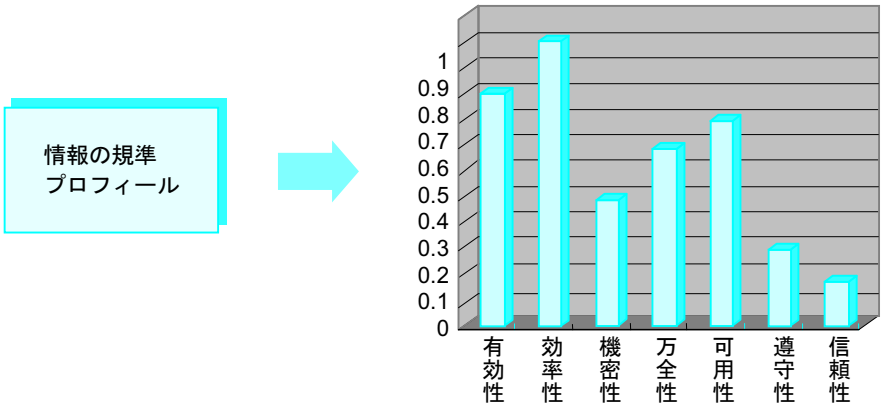


ITは，ビジネスの主要な遂行能力の一つとして，独自のスコアカードを持つことになる。遂行能力であるがゆえに，その評価尺度が目標に対する成果達成指標になる。すなわち，企業目標を達成するために必要な指示ができるように，いかに良好に遂行能力が発揮されているかということである。また，ビジネスの業績評価尺度が，ITにおいては最終目標の評価尺度になること(すなわち，バランススコアカードが次々と下のレベルに落とし込まれていくこと)に注目すべきである（付録Ⅲ参照）。

しかし，企業目標とIT目標の評価尺度をどのように関連付けるのだろうか。「COBIT フレームワーク」では，ITの目標は企業目標を達成するためにビジネス上必要となる情報の規準としている。IT目標は通常，次のような言葉で表現される。

- システムとサービスの可用性
- 万全性(インテグリティ)の欠如と機密リスク
- プロセス，オペレーションに関わるコスト効率
- 信頼性，有効性および遵守性の確認

つまり，ITの最終目標は，このような情報の規準に従ってビジネスに必要な情報を提供することであるということができる。この情報の規準は，「マネジメントガイドライン」に記載されているが，その中では各プロセスにおける重要度が，最も重要なものか，次に重要なものかに分けて示されている。実務的には，各企業の情報の規準のプロフィールは，より個別的なものになっていると考えられる。



上記の情報の規準の中のそれぞれの重要度は，各ビジネスの機能と企業を取り巻く環境によって定まる。前図は一例に過ぎない。組織は，自社のビジネスにとって，情報の規準の構成要素がどれほど重要なのかを個々に判断しなければならない。また情報の規準のプロフィールは，リスクに対する企業の見解を表している。しかしながら，情報の規準の重要性も，各プロセスに異なった目標が設定されると変化することもある点に注意する必要がある。いずれにせよ，IT組織の最終目標は，情報の規準のプロフィールを踏まえたうえで，企業目標を達成するために必要な情報を提供することである。

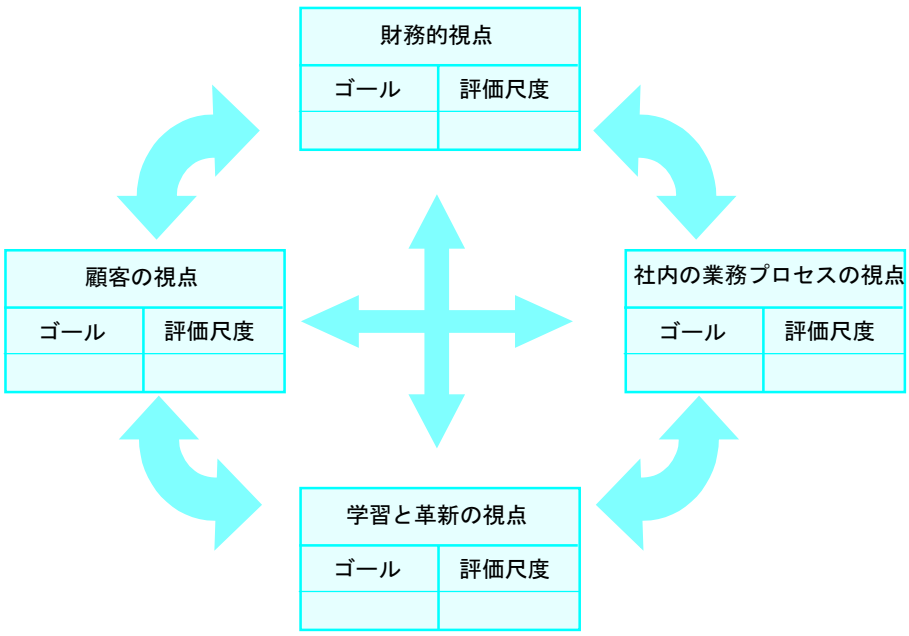
相対的に情報の規準の重要性が高い場合は，COBITが提供するベストプラクティス，具

体的には，「COBIT フレームワーク」(付録 II 参照)での考慮点“コントロール目標”，あるいは，“マネジメントガイドライン”の中の主要成功要因も含めた広範なリストから選択する必要があるかもしれない。

目標および目標に対する成果達成指標をよりよく理解するために，バランススコアカードの次の四つの視点を考慮した。

- **財務**…株主はどのように判断しているか (すなわち，予算に対しての実績は)？
- **顧客**…顧客はどのように判断しているか (顧客満足度，納期どおりの配送，サービスの価値などについては)？
- **社内の業務プロセス**…我々は自社をどう判断しているか (すなわち，業務指針と品質は)？
- **学習／改革**…我々は自らの価値を高め，新たな価値を創造していくことを継続できるのか (すなわち，従業員の知識や技術インフラは)？

IT にとっての KGI は，ビジネスから生まれるものであり，バランススコアカードの財務と顧客の視点で必要な評価尺度を規定するのが通常であり，次の図で表されている。KPI は，次の節で説明するように，バランススコアカードの他の二つの視点(社内の業務プロセスと改革)に焦点を合わせたものである。財務面の成果や顧客満足度は，達成されるべき企業目標の典型的な評価尺度であり，事後に測定されるものである。これに対して，卓越した業務プロセスや学習と改革の能力は，組織の健全性を示すバロメータであり，これを見れば目標が達成できるかどうか，事前に予測することができる。



KGI は，実績が確定して初めて分かる後追いの指標であり，それに対して，事前に成功するかどうかの兆候を示す先行指標となるのが KPI である。KPI は，目標未達時の影響といった言葉を用いて，否定的に表現されることもある。「COBIT 監査ガイドライン」の「リスクの実証」のセクションでは，IT プロセスが適切にコントロールされていない場合に生

じる不具合について 34 の各 IT プロセス別に事例を掲載している。

KGI は抽象的，あいまいであってはならず，数値あるいはパーセンテージで示される必要がある。また，情報や技術が組織の使命と戦略の実現に貢献していることが分かるものでなければならない。企業目標は個々の企業によって異なるため，KGI も可用性を向上させる，コストの低減を図るというように，向かうべき方向性が分かる形で作成されることが多い。実際には，経営者は，過去の業績や将来の目標を考慮に入れて，達成すべき特定の目標値を設定しなければならない。

前述のポイントを整理するために，通常，すべての IT プロセスに適用できる汎用的な KGI を次に挙げる。

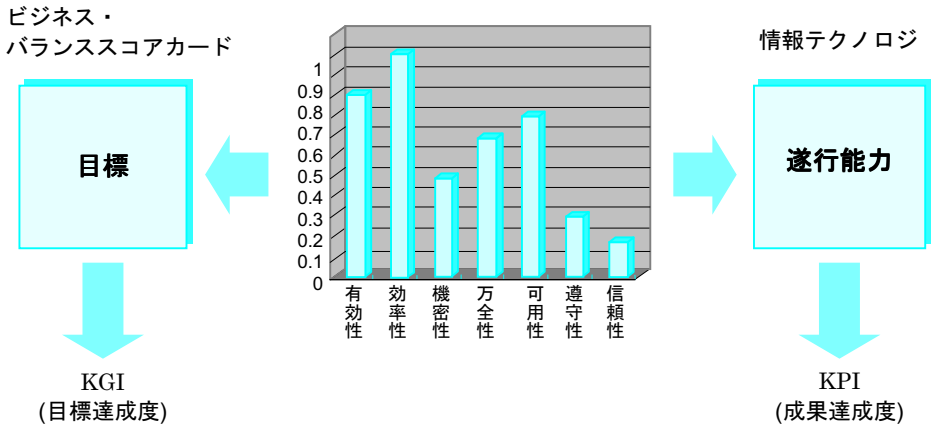
- 目標とする投資効果を達成すること，またはビジネス価値の増大に伴って得られる利益の目標をクリアすること
- 成果(パフォーマンス)管理を強化すること
- IT リスクを低減すること
- 生産性を改善すること
- サプライチェーンを統合化すること
- 業務プロセスを標準化すること
- サービス提供(売上)を増大させること
- 新規顧客を開拓し，既存顧客の満足度を向上させること
- サービス提供のための新しいチャネルを生み出すこと
- 通信ネットワーク，コンピュータ，情報提供の仕組みがビジネスニーズに合った形でサービス提供されていること，またそれらが利用可能な時間と休止時間
- IT プロセスに対する顧客の要求と期待を予算，納期ともに満足させること
- 顧客の人数と顧客一人当たりの平均コスト
- 業界標準の遵守

KGI を要約すると以下のとおりである。

- IT プロセスの最終目標を表すものである。すなわち，達成すべき「何か」を測るための評価尺度であったり，目標値そのものであったりする。
- IT プロセスの成果を記述するものであるから，後追いの指標であり，事後にならないと分からない。
- IT プロセスの結果をそのまま反映する直接的な指標である。一方，サービスを受けるビジネスの側から見れば，提供されたサービスの価値を表す間接的な指標となる。
- IT プロセスの目標が未達に終わった場合の影響度について記述されることもある。
- バランススコアカードの財務と顧客の視点に焦点を合わせている。
- IT 志向になってはいるが，まずビジネスありきである。
- 可能な限り正確で，事後に検証ができる客観的なことばで表現される。
- 個々の IT プロセスにとって最も重要な情報規準に焦点が合わせられている。

4. KPI(重要成果達成指標)

KPI は，ある IT プロセスがビジネスニーズを満たしているかどうか知るために，その IT プロセスの推進能力の成果(パフォーマンス)をモニタリングする際にマネジメントが用いることができる指標である。バランススコアカードの原則によれば，KPI と KGI の関係は次のとおりである。



KPI は，IT プロセスに必要不可欠な成果(パフォーマンス)を把握することができる簡潔・明確な指標である。また，KPI によって IT プロセスが，目標達成に向けてどの程度良好に機能しているか判断することができる。KGI が「何を達成するか」に焦点を合わせているのに対し，KPI は「いかに達成するか」に重点を置いている。KPI はしばしば CSF(重要成功要因)の指標になるため，継続的なモニタリングと対応を行えば，IT プロセスを改善するチャンスが生まれる。このような改善は，IT プロセスの成果にプラスの影響を与えることから，KPI と IT プロセスの KGI の間には原因結果関係がある。

KPI として複合化した指標を使うことが望ましい場合がある(KGI についてもまれにある)。例えば，IT 組織の健全性を表す指標として，IT スタッフの仕事への注力度，モラル，職務満足度を合わせて指標化することがある。また，ある計画の質を測るために，作成時期の適時性，内容の完全性，作成手続の手順化を合わせて一つの指標とすることもある。

KGI がビジネスの必要性に基づいて設定されるのに対し，KPI は IT プロセスを志向している。したがって，KPI によって，IT プロセスや組織が必要なリソースにどのような影響を与え，またそれらをどのように管理しているか判断することができる。KGI と同様に，KPI はしばしば数値やパーセンテージで表示される。KPI の良し悪しは，プロセス目標達成の成否が見分けられるかどうか，またプロセス改善に有用かどうかを判断することによって，厳しく評価することができる。

次に，すべての IT プロセスに一般的に適用できる汎用的な KPI を列記する。

共通して適用できるもの

- ライフサイクル時間の短縮(例：開発・運用における)
- 品質の向上とイノベーション
- 高速ネットワークやコンピュータの利用
- サービス提供レベルとレスポンスタイム
- 利害関係者の満足(苦情の調査，苦情の数)
- 新しい技術と顧客サービススキルの研修を受けたスタッフの人数

大部分の IT プロセスで適用できるもの

- IT プロセスの費用効率性の改善(費用と成果物の比較)
- スタッフの生産性(成果物の数)，モラル(調査)
- 発生したエラーの総数

IT ガバナンスに適用できるもの

- ベンチマークによる比較
- ルール違反が報告された件数

KPI を要約すると以下のとおりである。

- IT プロセスがどの程度良好に機能しているかを表す指標である。
- 将来の成功あるいは失敗の可能性を予測する「先行指標」である。
- IT プロセスを志向し，IT のニーズによって生まれるものである。
- バランススコアカードの内部プロセス，学習の次元に焦点を合わせている。
- 正確で客観的な言葉で表現される。
- モニタリングすることによって，IT プロセスの改善に役立つ。
- IT プロセスにとって最も重要な経営資源に焦点を合わせている。

5. 結論

情報テクノロジをうまくコントロールするために，すなわち IT とビジネスの整合性がとられ，組織に必要な情報が IT から提供される状況を生み出すために，この「マネジメントガイドライン」には多くの管理ツールが盛り込まれている。CSF，成熟度モデル，KPI，KGI の間の関係は次のように記述することができる。

「CSF は，成熟度分析を通じて得られる将来目標を踏まえて実施すべき最重要事項であるが，一方 KGI から生み出された企業目標を達成するためには，KPI を使ってモニタリングすることが必要である。」

しかし，このガイドラインは汎用的なものであり，業種を問わず使うことができる反面，特定の業種に固有の事項には対応していない点に注意していただきたい。多くの場合，組織はその置かれている環境に合わせて，このガイドラインをカスタマイズする必要があると思われる。

本ガイドラインに至るまでをたどると，「CobiT フレームワーク」からスタートし，国際標準やガイドラインの取込み，ベストプラクティスの調査を経て，「コントロール目標 Conrol Objectives」が完成した。その後さらに，「コントロール目標」が適切に導入されるかどうかを評価するために，「監査ガイドライン」が開発された。しかしながら，経営者は今，「フレームワーク」と共通点を持った新たなツールを必要としている。それは，情報や情報に関連するテクノロジの現状を自己評価し，それらに対するコントロールの導入や改善を意思決定するためのツールである。

上に示したことが，「マネジメントガイドライン」の主な目的であり，開発に当たっては IT ガバナンス，成果管理，情報セキュリティとコントロールの分野における世界中の専門家から助言いただいた。本ガイドラインには，経営者の次のような疑問を解くのに役立つツールセットが盛り込まれている。

「IT をわが社の企業目標の達成に役立てるためにコントロールする際の，適切なコントロールレベルとはどのようなレベルだろうか？」

Planning and Organisation		計画と組織
P01	Define a Strategic IT Plan	IT 戦略計画の策定
P02	Define the Information Architecture	情報アーキテクチャの定義
P03	Determine Technological Direction	技術指針の決定
P04	Define the IT Organisation and Relationships	IT 組織とそのかかわりの定義
P05	Manage the IT Investment	IT 投資の管理
P06	Communicate Management Aims and Direction	マネジメントの意図と指針の周知
P07	Manage Human Resources	人的資源の管理

P08	Ensure Compliance with External Requirements	外部要求事項の遵守の保証
P09	Assess Risks	リスク評価
P010	Manage Projects	プロジェクト管理
P011	Manage Quality	品質管理
Acquisition and Implementation		**調達と導入**
AI1	Identify Automated Solutions	コンピュータ化対応策の明確化
AI2	Acquire and Maintain Application Software	アプリケーションソフトウェアの調達と保守
AI3	Acquire and Maintain Technology Infrastructure	技術インフラの調達と保守
AI4	Develop and Maintain Procedures	操作，運用手続の作成と維持
AI5	Install and Accredit Systems	システムの導入と受入信認
AI6	Manage Changes	変更管理
Delivery and Support		**サービス提供とサポート**
DS1	Define and Manage Service Levels	サービスレベルの定義と管理
DS2	Manage Third-Party Services	サードパーティのサービスの管理
DS3	Manage Performance and Capacity	成果と能力(キャパシティ)の管理
DS4	Ensure Continuous Service	継続的なサービスの保証
DS5	Ensure Systems Security	システムセキュリティの保証
DS6	Identify and Allocate Costs	コストの捕捉と配賦
DS7	Educate and Train Users	利用者の教育と研修
DS8	Assist and Advise Customers	利用者に対する支援と助言
DS9	Manage the Configuration	構成管理
DS10	Manage Problems and Incidents	問題と事故の管理
DS11	Manage Data	データ管理
DS12	Manage Facilities	設備管理
DS13	Manage Operations	オペレーション管理
Monitoring		**モニタリング**
M1	Monitor the Processes	プロセスのモニタリング
M2	Assess Internal Control Adequacy	内部統制の十分性の評価
M3	Obtain Independent Assurance	独立した第三者の保証の獲得
M4	Provide for Independent Audit	独立監査の実施

次章以降で，34 の COBIT プロセスのそれぞれについて詳細な「マネジメントガイドライン」を提供する。また，ガイドラインの読み方についてのガイダンスは付録 I を参照のこと。

マネジメント
ガイドライン

計画と組織

PO1：IT 戦略計画の策定

情報テクノロジの利用機会と IT に対するビジネス要件の達成を確かなものとするために最適なバランスを確立させることをビジネス目標としている IT プロセスの **IT 戦略計画の策定**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，長期計画の立案につながるように定期的に実施されている戦略企画プロセスによって可能となる。また，これらの長期計画は，明確でかつ具体的な短期目標を設定した業務計画に，定期的に展開されることが望ましい。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その測定・評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 計画立案プロセスにおいてビジネス目標の優先順位付けの仕組みがあり，可能であればビジネスニーズを数値化していること
- 文書化された IT 戦略の策定方法や有効なデータおよび体系的で透明度の高い意思決定プロセスなどにより，マネジメントの投資承認やサポートに関する管理を実現可能にしていること
- IT 戦略計画ではリスクポジションが明確に示されている。例えばリスクの高い最先端の IT を使用するのか，それとも実証済みの IT を使用するのか，またはイノベータとして先頭を走るか，それともフォロアとして追随するのかということである。また同時に，市場投入に掛かる時間とシステムの保有コストやサービス品質といった QCT 間におけるバランスについても言及していること
- 戦略計画の前提条件がすべて検討され，検証されるようになっていること
- 成果を出すために必要なプロセス，サービスおよび機能は定められてはいるが，透明度の高い変更管理プロセスがあって，柔軟に変更ができるようになっていること
- 客観性を高めるため，戦略の実現可能性を第三者がチェックし，また，適切な回数繰返しチェックしていること
- IT 戦略計画を達成するため，具体的な進め方を示したロードマップや移行戦略が作成

されていること

重要目標達成指標(KGI)*4

- 各担当者の実行責任レベルまで詳細展開でき，長期，短期計画に展開され整合が取れている IT やビジネス戦略計画の割合
- 組織が現在保有している IT 能力(capabilities)を明確に理解しているビジネスユニットの割合
- マネジメントの検証によって，ビジネスや IT 戦略目標と実行責任の関連を明確に判定していること
- IT 戦略計画の中に含まれている戦略テクノロジを活用しているビジネスユニットの割合
- ビジネスオーナが計上している IT 予算の割合
- 未了となっている IT プロジェクトのうち，容認でき，合理的な理由のあるものの件数

重要成果達成指標(KPI)*5

- IT 能力(capabilities)評価の最新性(最終評価日からの経過月数)
- IT 戦略計画の老朽度(最終更新日からの経過月数)
- IT 戦略計画立案プロセスに参画したスタッフの満足度
- IT 戦略計画の変更が運営計画に反映されるまでの間のタイムラグ
- 作業負荷の程度，IT スタッフ数に対する参画したビジネスオーナ数の割合，キーとなる参画者の数などに基づいた，IT 戦略計画策定参画者の関与度の指標
- 策定作業の適時性，体系的アプローチの遵守性，および計画の完全性を含む計画の品質指標

PO1 成熟度モデル

情報テクノロジの利用機会と IT に対するビジネス要件の達成を確かなものとするために最適なバランスを確立させることをビジネス目標としている IT プロセスの **IT 戦略計画の策定**におけるコントロール

0：不在

IT 戦略計画は作成されていない。ビジネス目標の達成を支援するために IT 戦略計画が必要であることにマネジメントは気がついていない。

1：初期／その場対応

IT 管理者は IT 戦略計画を策定する必要性を感じているが，体系的な意思決定プロセスはない。IT 戦略計画は，ビジネスニーズに応えるように必要に応じて策定されているため，散発的でしかも一貫していない。IT 戦略計画は IT マネジメントのミーティングで時々検討されるが，経営者のミーティングでは取り挙げられない。ビジネスニーズ，アプリケーションとテクノロジの間の整合性は，その場対応型になっており，全社的戦略によるよりはむしろ，ベンダからの提案によって受動的に決まることが多い。戦略的なリスクポジションは，プロジェクトごとにインフォーマルに決められている。

2：再現性はあるが，直感的

IT 戦略計画を作成するプロセスを IT マネジメントは理解しているが，文書化はしていない。IT 戦略計画は IT マネジメントが作成しており，必要な時だけ経営者と共有するにとどまっている。マネジメントからの要請があった場合に IT 戦略計画の変更がなされるだけで，IT 計画の変更を必要とする IT 開発や新規ビジネス開拓を積極的に把握するようにはなっていない。戦略的意思決定はプロジェクトごとになされ，全社的戦略との整合性がない。主要な戦略的意思決定におけるリスクや利用者における効果については認識されているものの，リスクや効果の定義は，その時々によって異なっている。

3：定められたプロセスがある

IT 戦略計画を策定する時期や方法について方針が定まっている。文書化され，全員に周知されている体系的なアプローチによって，IT 戦略計画の策定がなされている。IT 計画策定プロセスは相応にしっかりしており，適切な計画が確実に策定されるようになっている。しかしながら，このプロセスの導入は各マネージャの判断に任されており，また，このプロセスの妥当性を定期的に検証する手続はない。全社的な IT 戦略には，組織がイノベータとして先頭を走る場合とフォロアとして追随する場合のそれぞれのリスクについても定めている。IT の財務面，技術面，人的資源面の戦略が，新製品や新技術の調達を促進している。

4：管理，測定されている

IT 戦略計画の策定は標準的実務であり，例外が生じた場合には，マネジメントが分かるようになっている。IT 戦略計画の策定は，上級マネジメントレベルに責任がある管理機能として定められている。IT 戦略計画の策定プロセスによって，マネジメントは計画をモニタリングし，計画情報に基づいた意思決定を行い，その有効性を計測することが可能となる。短期・長期両方の IT 計画が策定され，必要に応じて更改され，段階的に社内に浸透している。IT 戦略と全社的な組織戦略は，ビジネスプロセスや価値付加能力(value-added capabilities)を明らかにすることや，ビジネスプロセスリエンジニアリングを通してアプリケーションやテクノロジの利用を増加させることによって，より整合性の取れたものになってきている。システム開発と運用上で必要とされる社内外の資源のバランスをとるために十分に定義されたプロセスがある。業界標準や競合他社に対するベンチマーキングが，徐々に定義されてきている。

5：最適化

IT 戦略計画の策定プロセスは文書化され，実際使用されており，ビジネス目標を設定する際や IT 投資によって実現したビジネス上の価値を識別する際に絶えず配慮されている IT 戦略計画の策定プロセスにおいて，継続的に IT 投資のもたらすリスクと付加価値に関する検討が行われている。事業計画と整合性のとられた IT 戦略計画の策定機能がある。実現可能な長期 IT 計画が策定され，テクノロジの変化やビジネス関連の開発要求を反映して常に改訂されている。短期の IT 計画ではプロジェクトのマイルストーンや成果物が示され，変更の都度，常にモニタされ，更新されている。明確で，信頼性の高い業界標準に対するベンチマーキングのプロセスは適切に定義され，戦略策定プロセスに統合化されている。新しいビジネス能力を作り出し，競争力を高めるために，IT 部門では，新しいテクノロジについての最新の情報を集め，その利用を促進している。

PO2：情報アーキテクチャの定義

情報システムの体系を最適化することをビジネス目標としているITプロセスの**情報アーキテクチャの定義**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**ビジネス情報モデルの策定，および保守を行うことによって，またこの情報の利用を最適化するために適切なシステムが定義されることを保証することによって**，可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
S	機密性
S	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
✔	アプリケーション
	テクノロジ
	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 企業のデータモデルや情報標準を管理するために，必要十分なレベルと権限を備えた全社データ管理機能が確立されていること
- 情報アーキテクチャに関する標準が文書化され，周知され，遵守されていること
- データモデルは誰にとっても単純で理解しやすいものであること
- ビジネスを反映した企業のデータモデルが定義され，情報アーキテクチャ作成を推進させていること
- データのオーナーシップが割り当てられ，受け入れられていること
- データやデータモデルが最新の状態になっていること
- 情報アーキテクチャ，データディクショナリ，アプリケーション，データ構文，データ分類スキームやセキュリティレベルといった，情報システムのインフラに必要な構成要素間の整合性が保証されるように，自動リポジトリが利用されていること
- 情報要求事項をあらかじめ十分に理解していること

重要目標達成指標(KGI)*4

- アプリケーションのより早い開発
- 主要な情報システムの開発時間(Time to market)の短縮

- 機密性，可用性，万全性(インテグリティ)について定められている要求事項の組込み
- データの冗長性の低減
- システムとアプリケーションの相互操作性の向上
- 利用者が自動的に利用可能なデータディクショナリの割合

重要成果達成指標(KPI)*5

- 情報アーキテクチャの開発や保守に割り当てられている IT 予算の割合
- データモデルと整合性を取るために生じたアプリケーションの変更数
- データの分類スキームに記載されている情報インテグリティの要求事項の割合
- データモデルの一貫性の欠如に起因するアプリケーションやシステムの障害件数
- データモデルの一貫性の欠如によって生じた手戻り作業の量
- 情報アーキテクチャが最新でないことに起因するエラーの件数
- 情報アーキテクチャの変更がアプリケーションの変更に反映されるまでのタイムラグ

PO2 成熟度モデル

情報システムの体系を最適化することをビジネス目標としている IT プロセスの**情報アーキテクチャの定義**におけるコントロール

0：不在

組織における情報アーキテクチャの重要性に対する認識はない。また，情報アーキテクチャを策定するのに必要な知識，専門技術，実行責任を持つ部門が社内にはない。

1：初期／その場対応

マネジメントは情報アーキテクチャの必要性を認識しているが，それを開発するための業務プロセスや計画は承認されていない。情報アーキテクチャの構成要素は，バラバラに，その場対応で作成されている。データダイアグラム，ドキュメンテーションやデータ構文ルールなどは部分的に，関連性なく導入されている。しかし，情報についてというよりデータに関する定義となっており，アプリケーションソフトのベンダからの提案に影響を受けている。情報アーキテクチャの必要性を周知させることは，一貫性がなく散発的なものにとどまっている。

2：再現性はあるが，直感的

組織として情報アーキテクチャの重要性に対する認識を持っている。作成プロセスの形ができつつあり，インフォーマルで直感的ながらも，社内でさまざまな担当者が似通った手続をとりつつある。正式な研修はなく，スタッフは経験や技術を繰返し適用することによってスキルを習得している。戦術的な要求から，情報アーキテクチャの構成要素を個人的に作成する必要に迫られている。

3：定められたプロセスがある

情報アーキテクチャの重要性が理解され，承認されている。またその推進責任者が決められ，明確に周知されている。関連する手続，ツールやテクニックは精巧なものではないが，標準化され，文書化され，しかもインフォーマルな研修活動の一部になって

きている。情報アーキテクチャに関する基本的な方針には，戦略的な要件が若干盛り込まれているが，方針や標準，ツールを遵守することは，必ずしも制度化されていない。正式に承認されたデータ管理機能があり，全社標準を設定して情報アーキテクチャの導入や利用法について通達し始めている。全社的に自動化されたデータ管理ツールが導入され始めているが，そのプロセスやルールの定義はデータベースソフトウェアのベンダの提案に基づいて定義しているにすぎない。

4：管理，測定されている

情報アーキテクチャの作成や適用の制度化は，正式に承認された方法やテクニックによって完全にサポートされている。作成プロセスは変化やビジネスニーズにすばやく対応している。アーキテクチャ開発の成果に対する説明責任が強く求められおり，情報アーキテクチャの出来映えが測定されている。正式な研修活動が明確に定められていて，文書化され，しかも一貫して適用されている。自動化された支援ツールは広く利用されているが，まだ全社的には統合化されていない。社内のベストプラクティスが共有され，作成プロセスに取り入れられている。基本的な評価尺度指標が明らかになっており，評価測定システムができている。情報アーキテクチャを定義するプロセスは前向きであり，将来のビジネスニーズに関わることに焦点が当てられている。データ管理組織は，一貫性を確実にするためにすべてのアプリケーション開発に積極的に関与している。自動化されたリポジトリが全面的に導入され，データベース内の情報コンテンツを充実させるために，より複雑なデータモデルが導入されている。経営者向けの情報システムと意志決定支援システムによって，利用することができる情報が増えている。

5：最適化

情報アーキテクチャがあらゆるレベルで一貫して導入されており，そのビジネスに対する貢献度が絶えず強調されている。すべてのビジネスニーズを反映した，健全で即応性の高い情報アーキテクチャを開発，保守するため，IT 要員は必要な専門的能力やスキルを維持している。情報アーキテクチャから提供される情報は一貫して広範囲に利用されている。保守にあたっては，情報アーキテクチャの間断のない改善を含め，業界のベストプラクティスが利用されている。データ・ウェアハウスやデータマイニング技術によって，情報の活用を促す戦略が，明確に定められている。情報アーキテクチャは常に改善されており，業務プロセス，組織やシステムに関するこれまでの枠にとらわれない情報も考慮されている。

PO3：技術指針の決定

ビジネス戦略を推進し実現可能にするために，利用可能な新しいテクノロジを利用することをビジネス目標としている IT プロセスの**技術指針の決定**に関するコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**製品やサービス，デリバリーの仕組みに対してどのようなテクノロジの提供が可能かについて，明確かつ現実的な期待値の設定と管理を行う技術インフラ計画の作成および維持によって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- ビジネスに関連するテクノロジの報告書がビジネスユニットに配布されていること
- テクノロジの変化について，積極的なモニタリングが行われ，それが脅威となるかビジネスチャンスになるか判断している。モニタリングの担当者が明確になっており，また，そのプロセスは検証済みで信頼性のあるリソースを用いて行われるよう定められている。
- モニタリングの結果は上級マネジメントレベルで評価され，対応のためのアクションプランは合意を得たうえで IT インフラ計画に組込まれる。その際，IT 戦略計画との整合性は保たれている。
- 研究，プロトタイプ開発，テスト機構の導入にあたっては，テクノロジの熟達度よりも，ビジネスにおける価値，また，利用上の制約，機会を明らかにすることに重点が置かれる。
- 技術インフラ計画は，テクノロジの活用に関する方針や標準を勘案し，テクノロジの調達計画，要員の研修計画，採用計画に反映されていること
- IT インフラを移行させるためのロードマップや移行戦略があること
- テクノロジの方向性や計画の前提条件が，適切なタイミングで独立的な立場から再評

価されていること
- IT インフラ計画が，緊急時対応の観点から定期的に評価されていること
- テクノロジ開発に関するオープンな情報変換，ベンダやサードパーティとの良好な関係作りを通じて，業界動向の収集が進み，社内での対比とベンチマーキングが行われている。

重要目標達成指標(KGI)*4
- ビジネス戦略と整合性の取れていない技術的なソリューションの数
- 計画どおりに進んでいないテクノロジプロジェクトの割合
- 互換性がないテクノロジやプラットフォームの数
- 維持すべきテクノロジプラットフォームの削減数
- アプリケーションの開発工数の削減と開発期間の短縮
- システムとアプリケーション間の相互操作性の向上

重要成果達成指標(KPI)*5
- 技術インフラや調査研究に費される IT 予算の割合
- 技術インフラの最新性(最終レビュー日からの経過月数)
- テクノロジを活用するチャンスをタイムリに見つけ，分析することによって得られるビジネス部門の満足度
- 技術インフラ計画に含まれる技術ドメインのうち，現状とビジョン，導入までのロードマップといった実行計画まである技術ドメインの比率
- 自社で活用できそうなテクノロジを見つけてから，そのテクノロジをどのように利用するか決定するまでにかかる平均時間

PO3 成熟度モデル

ビジネス戦略を推進し実現可能にするために，利用可能な新しいテクノロジを利用することをビジネス目標としている IT プロセスの**技術指針の決定**に関するコントロール

0：不在

技術インフラ計画の重要性は認識されていない。技術インフラ計画を立案するために必要な知識や専門能力は欠如している。テクノロジの動向を読んで計画を立てることが，資源を効果的に配分するために極めて重要であるという理解が欠けている。

1：初期／その場対応

マネジメントは技術インフラ計画の必要性を認識しているが，計画の作成プロセスや計画そのものは正式に承認されていない。テクノロジの部分的な開発や新しいテクノロジの導入は，その場対応で，ばらばらに実施されている。計画の立案は受動的で，運用面に焦点を当てたアプローチになっている。技術指針は，ハードウェア，システムソフトウェア，アプリケーションソフトウェアのベンダから提案される，矛盾の多いバ

ージョンアップ計画に振り回されている。テクノロジの変更が及ぼす潜在的な影響について，常に情報提供されているわけではない。

2：再現性はあるが，直感的

技術計画の必要性と重要性について，社内において暗黙の了解がある。また，そのことについて周知されている。しかしながら，計画立案は戦略的で，ビジネスニーズを満たすためのテクノロジ活用よりも，技術的な問題に対してテクニカルな解決策を見い出すことに重点が置かれている。技術的な変更の評価は各担当者の独自の判断に任されているが，そのプロセスは似通ったものとなっている。個々の役割や責任についての正式な研修はなく，伝達もされていない。技術インフラの構成要素の開発に必要な標準テクニックや基準ができ上がりつつある。

3：定められたプロセスがある

マネジメントは技術インフラ計画の重要性に気がついている。技術インフラ計画の策定プロセスは妥当性があり，IT 戦略計画と整合性が取られている。技術インフラ計画は明文化され，十分に周知されてはいるが，実施に関しては一貫性がない。技術インフラ指針には，テクノロジの利用について先端を行くのか，それとも追随姿勢をとるのかについて，組織内の認識が示されており，それは，リスク判断と組織戦略に基づいている。キーベンダの選択は，自社の指針とベンダの技術・製品開発の長期計画が合致しているかどうかの判断に基づいて行われる。

4：管理，測定されている

IT スタッフには，技術インフラ計画を策定するために必要な専門的能力とスキルがある。テクノロジ調査のために正式な研修が用意されている。テクノロジの変化や新たなテクノロジの出現によって生じる潜在的なインパクトが考慮され，検証されている。マネジメントは，計画との差異を明らかにし，予期された問題に手を打つことができる。技術インフラ計画の策定と改善を担当する責任者が選任されている。計画策定のプロセスは洗練され，変更に柔軟に対応できる。また，そこには社内のベストプラクティスが導入されている。人的資源の戦略は技術指針と整合性が取られており，IT スタッフがテクノロジの変化に対応できる管理能力を持つことが保証されている。新しい技術を導入するための移行計画が定められている。自社に必要なノウハウやスキルを活用するために，アウトソーシング契約やパートナーシップ契約の締結が推進されている。

5：最適化

新たに出現したテクノロジや進歩の著しいテクノロジをレビューし，業界標準とのベンチマーキングを行う専門の調査部門がある。技術インフラ指針は，ベンダに左右されることはほとんどなく，業界や国際規格やその方向に準じて設定されている。テクノロジの変更によるビジネスへの潜在的な影響について上級マネジメントレベルでレビューされており，その結果に基づいて意思決定が行われることで，情報対応策に効果的な人的および技術的影響をもたらすことができる。技術指針の作成や，変更には経営者による正式な承認が必要である。業界標準の設定機関への参画やベンダの利用者団体への参画は正式に承認されている。組織には，ビジネスニーズを反映した強固な技術インフラ

計画があり，柔軟性が高く，ビジネス環境の変化に適応することができる。また，継続的な改善プロセスがあり，全社で統一的に実施されている。業界のベストプラクティスが，技術指針決定の際に広く取り入れられている。

PO4：IT 組織とそのかかわりの定義

適切な IT サービスを提供することをビジネス目標としている IT プロセスの **IT 組織とそのかかわりの定義**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，人員とスキルを備えた適切な組織で，その役割と実行責任が定義され，周知され，ビジネスとの整合性が保たれること，このことによって，戦略が促進され，効果的な指示や適切なコントロールを行うことが可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- IT 部門は，社内の全階層とその目標と成果を共有していること
- IT はすべての意思決定プロセスに組み込まれるように組織化され，重要なビジネスの意思決定を支援するとともに，全社の自動化ニーズに IT の主眼が置かれていること
- IT 部門の組織体制は，ビジネス機能と整合性が保たれ，ビジネス環境の変化に迅速に対応できるようになっていること
- 責任を持って仕事をすることが奨励され期待されることによって，IT 部門は，個人の発展，成長を促し，さらに，協調体制を高めている
- 指揮命令とコントロールの明確なプロセスがあり，必要に応じて職務分離や専門化，権限付与が行われていること
- IT 部門内にセキュリティ，内部統制，品質管理の各機能が適切に配置され，監督と権限付与のバランスが適切に保たれていること
- IT 部門はリスクや危機的な状況に対応できるよう柔軟な組織となっている。何も問題が発生していないときには職階制の体制をとっているが，緊急事態には各担当者に一時的に権限が付与され，チーム型の体制へと移行する。
- IT サービスのアウトソーシングに対しては強力なマネジメントコントロールが確立されている。明確な方針が存在するとともに，アウトソーシングに掛かるトータルコス

トが認識されている。

- 重要度の高い IT 機能が，組織体制の中で明示的に示され，その役割や責任が明確にされている。

重要目標達成指標(KGI)*4

- IT 部門の質的問題や能力不足のために遅れているビジネスプロジェクトの数
- IT 部門以外で実施されているコアとなる IT 活動で，正式な承認を受けていないものや IT 部門の標準に準拠していないものの数
- IT 部門の支援を受けているビジネスユニットの数
- IT 要員のビジネス指向意識，モラル，業務満足度に関する調査結果
- 直接ビジネス上の利益を生み出す IT プロセスに従事している IT 要員の稼働率

重要成果達成指標(KPI)*5

- 組織改変から経過している年数(組織の再編成や再評価が行われた場合も含む)
- 組織評価時に行われた改善勧告のうち，未実施のままとなっている件数
- 業務部門の組織に組み込まれている IT 部門の機能の割合
- ビジネス目標が，個人の任務や責任にまで直接，落とし込まれている IT ユニットの数
- 文書化された職務記述書がある役職の割合
- ビジネスの方針転換から，IT 部門の組織体制に変更が反映されるまでの平均的なタイムラグ
- 組織体制の中で，その役割や責任が明確にされ，明示的に示されている重要度の高い機能の割合

PO4 成熟度モデル

適切な IT サービスを提供することをビジネス目標としている IT プロセスの **IT 組織とそのかかわりの定義**についてのコントロール

0：不在

IT 部門は効果的に編成されておらず，ビジネス目標の達成を重視していない。

1：初期／その場対応

IT の活動や機能は受動的で，一貫性がない。明確な組織構造がなく，役割や責任はインフォーマルに決定され，明確な責任ラインが存在しない。IT 部門は，全社的な視点から見られることはなく，単なるサポート機能の一つであると思われている。

2：再現性はあるが，直感的

IT 部門の必要性について暗黙の理解はあるが，役割や責任は正式に承認されておらず，制度化もされていない。IT 部門は，戦術的に顧客のニーズに応え，ベンダとの関係を維持するために組織化されているが，その活動には一貫性はない。体系的な組織やベンダ管理の必要性は広く認識されているが，意思決定はまだ主要な担当者の知識とスキルに委ねられている。IT 部門内や対ベンダ間における管理には，共通の技法が用いられるようになってきている。

3：定められたプロセスがある

IT 部門やサードパーティの役割と責任は明確に定められている。IT 部門の組織体制が構築され，また文書化，周知され，IT 戦略と整合性が取られている。また，組織のデザインや内部のコントロール環境が定義されている。運営委員会，内部監査部門，ベンダ管理部門を含む他部門との関連についても一定の形式が定められている。IT 部門の機能は完成されているが，IT に対する関心は，ビジネス上の問題解決のためにテクノロジを活用することよりも，技術的な対応策に集まっている。IT 要員が担当する機能と利用者がいずれ担うべき機能の定義がされている。

4：管理，測定されている

IT 部門は洗練され，積極的に変化に対応するとともに，ビジネスニーズを満たすために必要なすべての役割を担っている。IT マネジメント，プロセスオーナーシップ，説明責任と実行責任が定義され，バランスが保たれている。IT スタッフの人員配置に必要な要件や専門的技術に関わるニーズは充足されている。社内のベストプラクティスが IT 部門内にも導入されている。IT マネジメントは，組織の体制や役割についてあるべき姿を明らかにし，それを実現し，モニタリングしていくために必要なノウハウとスキルを備えている。ビジネス目標や利用者が定義した CSF(主要成功要因)を支援するための重要な測定基準(metrics)は標準化されている。スキルの棚卸リストが，プロジェクトのスタッフ編成や専門家の育成をサポートするのに利用されている。IT 部門内で調達できるスキルやリソースと部門外から調達する必要があるものとのバランスが調整され，制度化されている。

5：最適化

IT 部門の組織体制は，ビジネスニーズを適切に反映しており，個別のテクノロジというより，戦略的なビジネスプロセスに見合ったサービスを提供している。IT 部門の組織はフレキシブルで，順応性がある。利用者やサードパーティとの関係についても定義されている。また，業界のベストプラクティスが導入されている。組織体制を構築し，管理するプロセスは洗練され，適切に運用管理されている。部門内外の広範囲な技術的ノウハウが活用されている。組織の役割や責任の遂行状況のモニタリングにもテクノロジが広く利用されている。さらに，複雑で，分散化した，バーチャルな組織のサポートにも IT の活用が推進されている。そして，適所に継続的な改善プロセスが存在している。

PO5：IT 投資の管理

財務的調達と支出をコントロールすることをビジネス目標としている IT プロセスの **IT 投資の管理**のコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**定期的な投資およびビジネスによって確立，承認された運用予算によって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
	可用性
	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- すべての IT 関連コストが識別され，分類されていること
- 正確なコストの把握を可能にする IT 資産の棚卸リストが，保持されていること
- 正式な投資規準が定められ，プロジェクトのタイプに応じた承認プロセスを経て迅速に意思決定されていること
- IT サービスのデリバリー計画が策定され，運用中の業務や投資，テクノロジのライフサイクル，テクノロジの構成要素の再利用に関する明確な視点が明らかにされていること
- 投資の意思決定プロセスが定められ，短期／長期の影響，組織にまたがる影響，ビジネス的な妥当性，効果の実現可能性，戦略への貢献度，技術アーキテクチャや技術指針などが検討されていること
- 影響度，測定可能な効果，時間的制約や実現可能性に基づいて透明度の高い選択をするために，投資の決定にあたっては，さまざまなオプションや代替案が提示されていること
- IT 予算や投資の金額は，IT 戦略計画や年次計画との整合性が取られていること
- 費用の承認権限が，明確な方法で委譲されていること
- IT 全体に掛かる費用(TCO)の予算が明確にされ説明責任者が決められており，その内容について適時に，厳密に，自動化された方法で検証されていること

- 期待した効果の達成はマネジメントの説明責任であることが明確にされており，分配しているものを除き，その達成状況を検証し報告するプロセスがあること
- 期待した効果を達成し，検証することが，明確にマネジメントの説明責任として位置付けられていること
- 意思決定権限を持つ者が，ライフサイクル全体や起こりうるマイナスの効果も含めて，他のビジネスユニットに与えうるあらゆる影響について考慮していること

重要目標達成指標(KGI)*4

- 投資回収率(ROI)と利用者満足度に基づいて算出する，期待した効果に見合ったもしくはそれを上回った IT 投資の割合
- 組織の支出合計に占める実際の IT 費用の割合，また目標値との比較
- 総収益に占める実際の IT 費用の割合，また目標値との比較
- 提出した IT 予算が満額承認されたビジネスオーナの割合
- 投資の意思決定の遅れや資金不足によるプロジェクトの遅れが無いこと

重要成果達成指標(KPI)*5

- IT 投資と予算に関する標準モデルが使われているプロジェクトの割合
- ビジネスオーナが定められているプロジェクトの割合
- 予算を最後にレビューしてからの経過月数
- 予算からの乖離が生じてから報告がなされるまでのタイムラグ
- 投資評価の結果がプロジェクトファイルに残されている割合
- ビジネスにおける効果が事後に検証されていないプロジェクトの件数
- 承認後に，投資やリソースの競合が明らかになったプロジェクトの件数
- 新しいテクノロジの利用に遅れが生じた事例の件数と，利用までのタイムラグ

PO5 成熟度モデル

財務的調達と支出をコントロールすることをビジネス目標としている IT プロセスの**IT 投資の管理**のコントロール

0：不在

IT 投資を選択し，予算化することの重要性が全く認識されていない。IT 投資やその支出状況を検証し，モニタリングすることも全く行なわれていない。

1：初期／その場対応

IT 投資を管理する必要性は社内で認識されているが，その必要性について十分に周知されているわけではない。IT 投資を選択し予算化する責任者は正式には任命されていない。重要な支出は，個別に申請する必要がある。IT 投資の選択と予算編成は，インフォーマルな資料に基づいて，個別に行われる。IT 投資についてはその場対応で承認がされる。受動的で，運用面を重視した予算決定が行なわれている。

2：再現性はあるが，直感的

IT 投資を選択し予算化することの必要性について暗黙の理解がある。また，社内で周知されている。しかし，これに従うかどうかは，個人の自発性に委ねられている。IT 予算の構成要素を策定するための共通のテクニックが現れてきている。予算決定は，受動的ではあるが，戦略的に行なわれている。投資を決定する際に，技術動向に基づく予測や，生産性やシステムのライフサイクルへの影響についての検討が行なわれるようになってきている。

3：定められたプロセスがある

IT 投資の選択と予算化のプロセスは妥当性があり，ビジネスやテクノロジにおいて主要な課題をカバーしている。投資の選択プロセスやその方針は定義され，文書化され，周知されている。IT 予算は，戦略的な IT 計画やビジネス計画と整合性が保たれている。予算化と IT 投資の選択プロセスは正式に承認され，文書化され，周知されている。また，インフォーマルに自習方式の研修が始まっている。IT 投資の選択と予算化について，正式に承認され始めている。テクノロジの開発や IT 要員の能力や生産性の向上を図るために，人的資源，ハードウェア，システムソフトウェアに対する投資と，アプリケーションソフトウェアへの投資とのバランスが定められ，合意がなされている。

4：管理，測定されている

投資の選択や予算作成の実行責任と説明責任は，特定の個人に割り当てられている。予算との差異は，速やかに把握され，修正されている。IT スタッフには，IT 予算を見積り，適切な IT 投資を提案するために必要な専門的技術と必要なスキルがある。正式なコスト分析が行われており，分析対象には既存システムの運用に掛かる直接費，間接費のほかに，提案されている投資案件に掛かるものも含まれる。これは，システムの所有に必要な総コスト(TCO)の考え方に基づいている。予算編成プロセスは前向きで標準化されたものになっている。開発費や運用費の内容がハードウェア，ソフトウェア費用からシステムインテグレーション費，IT 人件費へシフトしていることが投資計画の中で認識がされている。

5：最適化

投資によってもたらされる効果や利益は，財務面，非財務面両方から算定されている。業界のベストプラクティスを用いて，コストをベンチマークし，投資の有効性を高めるためのアプローチが明らかにされている。テクノロジ開発に関する分析が，投資の選択と予算編成プロセスの中で実施されている。また，必要に応じた継続的な修正プロセスがある。投資の決定に当たっては，新しいテクノロジや製品の導入によるコスト成果の改善点が加味される。資本の投下に関する選択肢が，組織の既存の資本構造の中で，正式な評価方法を用いて公式に分析，評価されている。したがって，予算と実績の差異もあらかじめ織り込まれている。投資の決定にあたっては，投資物件を保持するために長期的に掛かるコストの分析も考慮されている。投資案の決定プロセスでは，テクノロジを活用することによって新たなビジネスチャンスを創造するなど，長期にわたり戦略的な取組みを支援する必要性が認識されている。組織内には，新たなビジネスチャンスの創出や運用効率の向上のために，テクノロジの利用において先行するのか，それとも動向を見極めてからにするのか，投資リスクについての方針があり，周知徹底されている。

PO6：マネジメントの意図と指針の周知

マネジメント目標を利用者に認識させ，理解させることを保証することをビジネス目標としている IT プロセスの**マネジメントの意図と指針の周知**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**ある共通の目的を持つ利用者共同体に対して，確立され，周知されているさまざまな方針によって**可能になる。**さらには，戦略的な選択肢を実務的で，しかも有用な利用者のルールに変えていくための標準が確立される必要がある。**

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
	効率性
	機密性
	万全性
	可用性
S	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 方針を作成する際に，いかに方針を徹底するかが検討され，決められていること
- 必要な時に，方針に対する意識や理解度，遵守状況を評価するための検証プロセスがあること
- 適切に定義され，明確に示されたミッション指示書や方針が整備されていること
- 情報コントロール方針は，全社的な戦略計画と整合性が保たれていること
- マネジメントが，情報コントロール方針を保証するとともに強いコミットメントを示し，方針を周知させ，理解させ，遵守させることの必要性を強く示していること
- マネジメントは自らが模範となって組織をリードしていること
- 方針や手続を実施するための実務的なガイドがあること
- 重要なメッセージを繰返し伝えるために，さまざまな方法によって注意の喚起がされていること
- 情報コントロール方針が最新の状態に更新されていること
- 一貫して適用されている方針策定のためのフレームワークがあり，作成，導入，教育，遵守のためのガイドになっていること

重要目標達成指標(KGI)*4

- ミッション，ビジョン，目標，価値，行動規範を含めて作成され，明文化されている IT 計画や方針の割合
- すべての利害関係者に漏れなく周知されている IT 計画や方針の割合
- 方針や手続について研修を受けている組織の割合
- 定期調査の結果として改善された利用者の認知度
- 情報コントロールを取り扱っている方針や手続の数

重要成果達成指標(KPI)*5

- 方針が承認されてから利用者に周知されるまでのタイムラグ
- 周知の頻度
- 特定の情報コントロール方針について記述された文書が作成された年代(前回の改訂からの経過月数)
- 情報コントロール方針の作成と導入に当てられた予算の割合
- 業務手続が確かに運用されていることを確かめるためにそれと関連付けて考えられている情報コントロール方針の割合

PO6 成熟度モデル

マネジメント目標を利用者に認識させ，理解させることを保証することをビジネス目標としている IT プロセスの**マネジメントの意図と指針の周知**についてのコントロール

0：不在

マネジメントは情報のコントロール環境を積極的には確立していない。一連の方針，手続，標準，遵守すべきプロセスを確立することの必要性が全く認識されていない。

1：初期／その場対応

マネジメントは，情報のコントロール環境に必要な要件の確立においては受動的である。方針，手続，標準は，必要に応じてその都度作成されて伝達されるが，それは主に問題が生じた場合である。作成，周知，遵守すべきプロセスはインフォーマルなもので一貫性がない。

2：再現性はあるが，直感的

マネジメントは，効果的な情報のコントロール環境の必要性やその要件について暗黙に理解している。しかしながら，実務には一定の形式はなく，一貫して文書化されているわけではない。マネジメントはコントロールのための方針，手続，標準の必要性を伝えているが，それらの作成は，個々のマネージャやビジネスエリアの裁量に委ねられている。方針やその他の補助資料は個別の必要に応じて作成されており，全社的な作成のためのフレームワークはない。クオリティの向上は，努力目標に過ぎず，その実現は各マネージャの裁量に委ねられている。また，研修は，要望に応じて個別に実施されている。

3：定められたプロセスがある

マネジメントは，方針や手続，標準を作成するためのフレームワークを含む，完全な

情報のコントロール環境と品質管理の環境を作り，文書化し，周知徹底している。方針の策定プロセスは体系化，維持されており，スタッフに公開されている。また，既存の方針，手続，標準は適切であり，重要事項をカバーしている。マネジメントはITセキュリティの重要性を認識しており，意識付けを行うための教育プログラムを始めている。正式な研修が整備され，情報のコントロール環境を支援できるような体制はあるが，厳密に行われてはいない。コントロール方針や標準を遵守しているかどうか，モニタリングはされているが，一貫性に欠けている。

4：管理，測定されている

マネジメントは内部統制に関する方針を周知させる責任について理解しており，重要な変更に対し，コントロール環境を保つために適切な権限委譲を行う責任を持ち，必要十分な資源の割当てを行っている。品質の向上やITセキュリティに対する意識付けへの前向きな取組みも含めて，積極的な情報のコントロール環境が確立されている。一連の方針，手続，標準が完備され，維持，周知されており，その内容は組織内のベストプラクティスとなっている。導入や導入後の遵守状況をチェックするためのフレームワークが確立されている。

5：最適化

情報のコントロール環境は，戦略的経営のフレームワークやビジョンと整合性が保たれており，レビューが頻繁に行われるとともに，最新のものにアップデートされ，絶えず改善されている。コントロールのガイドやコミュニケーション技法に関しては，組織内外の専門家が活用され，業界のベストプラクティスが確実に取り入れられるようになっている。モニタリング，自己評価，コミュニケーションのプロセスは，組織全体に広がっている。テクノロジが，方針や意識統一のためのナレッジデータベースを維持するため，またコミュニケーションの最適化を図るために活用されており，OAやコンピュータベースの研修ツールが利用されている。

PO7：人的資源の管理

意欲的で有能な人材を獲得して教育を行い，IT プロセスに対する要員の貢献度を最大化することをビジネス目標としている IT プロセスの**人的資源の管理**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**募集，採用，身元調査，給与の支払，教育訓練，表彰，昇進昇格，解雇を行うための適切かつ公正で，透明性の高い要員管理の手続によって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- IT の人的資源管理計画を作成し，維持するためのフレームワークがあること
- マネジメントが，IT の人的資源管理計画の策定を支援し，責任関与(コミットメント)していること
- IT 戦略計画と IT 人的資源管理計画との整合性が保たれていること
- IT の人的資源管理計画を作成するために，十分な能力があり，適切なスキルを備えた人材が配置されていること
- 常時継続的に行われている IT 研修や新人研修に十分なリソースが割り当てられ，IT の人的資源管理計画のニーズを満たしていること
- IT の人的資源継承計画において，特定の担当者への依存度が高い業務を検討し，担当者間で専門技術力のギャップが生じないようにしている
- キャリア開発のためのジョブ・ローテーションが実施されていること

重要目標達成指標(KGI)*4

- IT の人的資源管理計画が策定されてからの経過月(最終更新日からの経過月数)
- 組織における役割を果たすのに必要な能力要件を満たしている IT 要員の割合

- 直接ビジネス上の利益を生み出す IT プロセスに従事している IT 要員の稼働率
- IT 要員の離職率
- 欠員の補充率
- 担当業務を始めてからの平均期間(月数)

重要成果達成指標(KPI)*5

- IT 戦略計画が変更されてから IT の人的資源管理計画が変更されるまでのタイムラグ
- 専門能力の開発計画が策定されている IT 要員の割合
- 成果評価(パフォーマンスレビュー)が文書化され，承認されている IT 要員の割合
- IT 要員 1 人当たりの研修時間の割合
- 相互研修やバックアップ要員の割当てがされている，重要業務担当要員の割合
- IT 要員の不足が原因で，延期またはキャンセルされたプロジェクトの件数
- IT 人的資源管理計画の作成や改善に当てられた人件費の予算比率
- 文書化された職務記述書や採用条件書がある IT 役職の割合

PO7 成熟度モデル

IT プロセスに対する要員の貢献度を最大化することをビジネス目標としている IT プロセスの**人的資源の管理**についてのコントロール

0：不在

組織として IT の人的資源管理とテクノロジ計画プロセスとの整合性を保つことの重要性に全く気がついていない。IT の人的資源管理に対して責任を負う人物もグループも存在しない。

1：初期／その場対応

マネジメントは IT の人的資源を管理する必要性を認識しているが，それに関する正式なプロセスや計画はない。IT の人的資源の管理プロセスはインフォーマルなものにすぎず，IT 要員の採用や管理のアプローチは，受動的で実務中心になっている。急激なビジネスや技術の変化，ますます複雑化する問題の解決には，新しいスキルやそれに見合った能力レベルが必要になってくるということに気づき始めている。

2：再現性はあるが，直感的

IT の人的資源管理の必要性については暗黙に理解されている。IT 要員の採用や管理についてのアプローチは，技術指針や，組織内外の技術スタッフの可用性についてバランスを考慮しているというよりむしろ，特定のプロジェクトからのニーズに対応しているにすぎない。また，新人に対してインフォーマルな研修が行われているが，それは要望に応じて実施されているにすぎない。

3：定められたプロセスがある

IT の人的資源を管理するプロセスが作成されており，IT の人的資源管理計画が定義，文書化されている。IT 要員を採用し管理するための戦略的なアプローチがある。さらに，

IT の人的資源のニーズを満たすように設計された正式な研修計画がある。技術的スキルおよびビジネスマネジメントスキルを高めるためにデザインされたローテーションプログラムも確立されている。

4：管理，測定されている

IT の人的資源管理計画を作成し改善する責任は，必要な専門能力とスキルを持った特定の個人に割り当てられている。そのプロセスは変化に対応できるものとなっている。組織には計画からの乖離を明らかにするための標準化された指標があり，IT 要員の増員や離職率の管理には特に注意が払われている。報酬比較分析が定期的に行われ，給与面において，他の同等の IT 組織と十分競争できることが保証されている。IT の人的資源の管理は，キャリアパスの作成も考慮に入れた，事前対応型のものになっている。

5：最適化

組織には，効果的な IT の人的資源管理計画があり，IT や IT がサポートしているビジネスの要件を満たしている。IT の人的資源の管理はテクノロジ計画に統合され，有効な IT スキルの開発や活用を保証するものとなっている。IT の人的資源の管理を構成する要素には，例えば，報酬，成果評価，業界団体への参加，知識の共有，研修，指導・助言があり，業界のベストプラクティスとの整合性もある。新しいテクノロジ標準や製品が導入される前には，必ず研修プログラムが作成されている。テクノロジの利用によって，データベースにアクセスすることで，簡単にスキルや研修，適性要件情報が得られるようになっており，IT の人的資源の管理プロセスを支援している。IT マネジメント向けに，他部門の上級マネジメントに対して導入されているプログラムと同じようなインセンティブプログラムが制度化されており，IT の成果目標の達成者には報償金が与えられている。

PO8：外部要求事項の遵守の保証

法律，規定，契約上の責務を満たすことをビジネス目標としている IT プロセスの**外部要求事項の遵守の保証**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**外部からの要求事項によって IT が受ける影響を確認して，分析したうえで，要求事項を遵守するために適切な手段を取ることによって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
	効率性
	機密性
	万全性
	可用性
P	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
	テクノロジ
	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 外部からの要求事項の遵守に関する方針や手続が文書化され，周知されていること
- モニタリング機能によって遵守状況がレビューされていること
- 外部からの要求事項を満たすために必要な改善活動のリストが更新されていること
- 外部からの要求事項に関する遵守問題を解決するためのフォローアップのプロセスが明確に定義されていること
- 外部からの要求事項を遵守するためのコストを決定する際に，必要な情報が提供されていること
- 外部からの要求事項の遵守状況をチェックするために，効果的な内部監査が実施されていること

重要目標達成指標(KGI)*4

- 法律，規定または契約上の問題の発生件数
- 法律，規定または契約上の，未解決の問題の平均係争年数
- 和解金や罰金などの遵守違反に掛かるコスト

重要成果達成指標(KPI)*5

- 遵守状況をレビューする頻度
- 遵守状況のレビューで判明した例外事項の件数
- 外部からの要求事項の遵守に関する問題が判明してから解決されるまでに掛かる平均期間

PO8 成熟度モデル

法律，規定，契約上の責務を満たすことをビジネス目標としているITプロセス**外部要求事項の遵守の保証**についてコントロール

0：不在

外部からの要求事項がITに影響を与えるという認識はほとんどなく，規定，法律，契約上の要求事項を遵守することに関するプロセスは全くない。

1：初期／その場対応

組織に影響を与える規定，契約，法律上の遵守事項に対する認識はある。インフォーマルな遵守性を保つためのプロセスがあるが，それは新規プロジェクトで必要が生じた場合，もしくは監査やレビューに対応する上で必要となった場合だけである。

2：再現性はあるが，直感的

外部からの要求事項を遵守する必要があること，またそのことを周知徹底しなければならないことは理解されている。財務規則や，プライバシー法のように遵守することが常に求められるような場合は，個別に遵守手続が作成され，毎年フォローされている。しかし，遵守すべきすべての要求事項が満たされていることを保証する総合的な仕組みはない。したがって，例外事項が発生しやすく，新たな遵守事項に対しては受動的な対応しかできない可能性が高い。個人の知識や責任に大きく依存しており，ミスも発生しやすい。外部からの要求事項や遵守事項に関する研修は，インフォーマルなものである。

3：定められたプロセスがある

規定，契約，法律上の義務の遵守を保証するために，方針，手続，プロセスが作成され，文書化，周知されている。しかし，それらに常に従っているわけではなく，なかには古くなったり，導入しても実務上役に立たないものもある。モニタリングはほとんど行われておらず，処理されないでそのままになっている要求事項もある。組織に影響を与える外部からの法律，規定上の要求事項や定められた遵守プロセスについての研修が実施されている。契約上の責務に関するリスクを最小限にとどめるために，契約書の標準様式や法律上の確認を行うプロセスがある。

4：管理，測定されている

外部要求事項に伴う課題やリスク，および全社レベルでの遵守を保証する必要性について，十分な理解が得られている。正式な研修体系によって，すべてのスタッフが遵守義務を認識することが確保されている。責任体制が明確にされ，プロセスのオーナーシ

ップが理解されている。遵守に関するプロセスには，外部環境のレビューが含まれ，外部要求事項や変更状況を経常的に確認することができる。遵守されていない外部要求事項をモニタし，社内手続を強制化し，訂正行為を起こす組織的なメカニズムがある。遵守されていない課題については，一貫性のある対応策を確立するために，標準化された方法で，その根源原因の分析が行われる。永続的な規定や自動更新サービス契約のような特定のケースについては，標準化された社内のベストプラクティスが活用されている。

5：最適化

外部要求事項の遵守のために，十分に体系化され，効率的に制度化されたプロセスがある。そのプロセスは一つの中央集中機能で担っており，全社にガイドを提供するとともに調整を行っている。該当する外部要求事項の将来動向，予想される変更，新たな対応策の必要性などの広範な知識がある。政界や業界団体との外部検討会へ参画することで，外部要求事項について理解を深めるだけでなく，要求事項への影響力を強めている。外部要求事項の遵守を保証するベストプラクティスが生み出され，遵守に関する例外事項はほとんどなくなっている。中央集中型の全社的な追跡システムがあり，マネジメントがワークフローを文書化し，遵守状況モニタリングプロセスの品質や効率性を評価し，改善することが可能になっている。外部要求事項の自己評価プロセスが導入され，ベストプラクティスのレベルまで改良が進んでいる。遵守についての組織のマネジメントスタイルや文化が強固に確立され，研修が必要なのは，新人社員に対してや重要な変更があった場合だけで十分対応できるようにプロセスが作られている。

PO9：リスク評価

IT の目標を達成するためのマネジメントの意思決定を支援すること，および，複雑さを少なくし，客観性を向上させ，重要な意思決定に関わる要因を明らかにすることで脅威に対処することをビジネス目標としている IT プロセスの**リスク評価**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**一連の規則の機能を取り込み，かつリスクを軽減させるための費用有効性を考慮しながら，組織全体の IT リスクの識別と影響分析に取り組むことによって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
P	機密性
P	万全性
P	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- リスク管理のオーナーシップとマネジメントの説明責任に関する明確な役割や実行責任が決められていること
- リスクの限界や許容範囲を明確に定義するための方針が確立していること
- リスク評価は，脆弱性，脅威，データの価値を総合的に勘案して行われていること
- 構造化されたリスク情報が維持され，かつ事故報告書の情報でさらに養生されていること
- リスク管理の改善事項を明らかにし，合意を得て資金を投下するための責任体制や手続があること
- 理論的脅威よりも現実の脅威に主として評価の焦点が当てられていること
- リスクの識別や低減につながるブレーンストーミングや根本的な原因分析が，定期的に実施されていること
- 客観性を高めるために，第三者によって戦略の実現性のチェックが行われており，それが適切なタイミングで繰り返し実施されていること

重要目標達成指標(KGI)*4

- リスク評価の必要性についての認識度の向上
- 既知のリスクが原因で発生した事故の減少件数
- 十分な軽減措置が図られていると確認されたリスクの増加件数
- リスク評価が完了して，その結果が正式に文書化されている IT プロセスの増加件数
- 費用対効果のリスク評価測定が行われている適切な割合や件数

重要成果達成指標(KPI)*5

- リスク管理のためのミーティングやワークショップの回数
- リスク管理改善プロジェクトの件数
- リスク評価プロセスに対する改善の件数
- リスク管理プロジェクトに割り当てられた資金のレベル
- 公表されたリスクの範囲や方針の更新回数および更新頻度
- リスクモニタリングの結果報告の件数および頻度
- リスク管理手法の研修を受けたスタッフの数

PO9 成熟度モデル

IT の目標を達成するためのマネジメントの意思決定を支援すること，および，複雑さを少なくし，客観性を向上させ，重要な意思決定にかかわる要因を明らかにすることで脅威に対処することをビジネス目標としている IT プロセスの**リスク評価**についてのコントロール

0：不在

プロセスやビジネスの意思決定にかかわるリスク評価は行われていない。セキュリティの脆弱性や開発プロジェクトの不確実性がビジネスに与える影響については考慮されていない。リスク管理が，IT 対応策の調達や IT のサービス提供と関係があると認識されていない。

1：初期／その場対応

法律上，契約上の責任や責務に対する認識はあるが，IT リスクはその場対応で検討されるだけで，一定のリスク管理のプロセスや方針に従ってはいない。個々のプロジェクトが決定した場合に，プロジェクトリスクのインフォーマルな評価が行われている。リスク評価がプロジェクト計画の中で特別に検討されることはなく，特定のプロジェクトマネージャにアサインされることもない。IT 管理者のリスク管理責任については，職務記述書やその他のインフォーマルな方法において明記されていない。セキュリティ，可用性，インテグリティといった具体的な IT 関連リスクは，プロジェクト単位で時折検討されている。マネジメントミーティングにおいて，日々の業務に影響を与える IT 関連のリスクについて検討されることはほとんどない。リスクが検討されている場合にも，リスク軽減策には一貫性がない。

2：再現性はあるが，直感的

IT リスクは検討すべき重要な問題であるという理解が急速に拡がり始めている。いくつかのリスク評価のアプローチはあるが，そのプロセスは未熟であり，開発段階である。リスク評価は，通常リスクの高いものを対象とし，一般に主要なプロジェクトに対してだけ行われている。日々の運用に関するリスク評価は，主として IT マネージャが検討事項として取り上げるかどうかにかかっており，それは問題が発生したときに限られることが多い。IT 管理者は通常，リスク管理に関連する手続や職務記述書を定めていない。

3：定められたプロセスがある

全社的なリスク管理方針によって，リスク評価を行う時期や方法が定められている。リスク評価は明確に定められたプロセスに従って行われ，その内容は文書化され，研修を通して全スタッフが利用することができるようになっている。プロセスに従うかどうか，また研修を受講するかどうかの決定は個人の裁量に委ねられている。リスク評価の方法論は，説得力があって妥当であり，ビジネス上重要なリスクを識別できることを保証している。このプロセスに従うかどうかの決定は IT マネージャ個人に委ねられており，すべてのプロジェクトがリスク評価対象に含まれることを保証する手続や，日々の運用業務のリスクに関する検証が定期的に行われることを保証する手続はない。

4：管理，測定されている

リスク評価は標準手続になっており，手続における例外事項があれば IT 管理者によって通知される。IT リスクの管理は上級マネジメントに責任が委ねられ，明確に定められた管理機能になってきている。リスク評価のプロセスは高度化しており，個々のプロジェクトだけでなく，IT 業務全般についてもリスク評価が定期的に行われている。ネットワークからの脅威の増大や IT 戦略の健全性に影響を与える技術的な動向といった，リスク管理のシナリオに重大な影響を与える可能性のある IT 環境の変化について，マネジメントはアドバイスを受けている。マネジメントはリスクポジションをモニタリングすることが可能であり，意図的にリスクを許容しようとする場合には詳しい情報をもとに意思決定することができる。上級マネジメントや IT 管理者は組織として許容できるリスクのレベルを決定し，リスク／リターン比率に関する標準的な評価指標を持っている。マネジメントは，定期的にリスクを再評価するためのオペレーションリスク管理プロジェクトの予算を組んでいる。また，リスク管理用のデータベースも整備されている。

5：最適化

リスク評価は，全社的に組織化されたプロセスが制度化され，定期的なフォローと適切な管理が行われる段階にまで発展している。リスクに関するブレーン・ストーミングや原因分析が，専門家を伴い，組織の枠を越えて全社的に行われている。リスク管理に関するデータの収集，分析，報告のプロセスは，高度に自動化されている。各分野のリーダによってリスク管理のガイダンスが作成されており，IT 組織は情報交換を目的として同業者団体に参画している。リスク管理が，業務および IT 運用全体の中に完全に統合され，IT サービスを受ける利用者に広く受け入れられ，浸透している。

PO10：プロジェクト管理

優先順位を付け，期限を守り，予算内でサービス提供をすることをビジネス目標としているITプロセスの**プロジェクト管理**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**組織が，業務計画と整合性を取りながらプロジェクトの内容を見極めて優先順位付けを行い，現在着手している各プロジェクトに応じた適切なプロジェクト管理手法を採用し適用することによって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 経験豊富で熟練したプロジェクトマネージャがいること
- 承諾され，標準化されたプログラム管理プロセスがあること
- プロジェクトを上級マネジメントが支援しており，利害関係者(ステークホルダー)やITスタッフが共同してプロジェクトの企画や実施，管理を行なっていること
- 大規模で複雑なプロジェクトを管理する際に，組織やIT機能の能力や限界について認識がされていること
- 全社でプロジェクトリスクの評価方法が定められ実施されていること
- すべてのプロジェクト計画に，明確で跡付けが可能な作業の細分化体系(WBS)，合理的で正確な見積り，スキル要件，追跡課題，品質計画，透明度の高い変更プロセスがあること
- 開発導入チームから運用チームへの引継ぎのプロセスが，適切に管理されていること
- システム開発ライフサイクル(SDLC)の方法論が組織内で定められ，利用されていること

重要目標達成指標(KGI)*4

- 期限，予算内に完了したプロジェクトの増加件数

- 正確なプロジェクトスケジュールや予算情報が利用可能であること
- 繰返し起こる一般的な問題の減少
- プロジェクトリスクをタイムリに見つけること
- プロジェクトによってもたらされるサービス提供に対する組織の満足度の向上
- プロジェクト管理における意思決定のスピードアップ

重要成果達成指標(KPI)*5

- 定められた方法に従って実施されたプロジェクトの増加件数
- 利害関係者(ステークホルダー)がプロジェクトに参画した比率(関与指数)
- プロジェクトチームメンバ１人当たりのプロジェクト管理研修受講日数
- プロジェクトのマイルストーンおよび予算レビューの回数
- プロジェクト終了後にレビューが行われた比率
- プロジェクトマネージャの平均経験年数

PO10 成熟度モデル

優先順位を付け，期限を守り，予算内でサービス提供をすることをビジネス目標としているITプロセスの**プロジェクト管理**についてのコントロール

0：不在

プロジェクト管理手法は使われておらず，誤ったプロジェクト管理や開発プロジェクトの失敗がビジネスに与える影響が検討されていない。

1：初期／その場対応

一般的に，プロジェクトを体系化する必要があることや，管理が行き届かないプロジェクトにはリスクがあることが認識されている。ITにおけるプロジェクト管理手法やアプローチの利用を決定するのは，各ITマネージャである。プロジェクトは一般に，企画が不十分で，組織やビジネス上の利害関係者(ステークホルダー)のビジネス目標や技術指針は含まれていない。一般的に，マネジメントの責任関与(コミットメント)やプロジェクトのオーナーシップが欠如しており，利用者部門のマネジメントや顧客(カスタマ)からの情報提供なしに，重要な決定がなされている。また，ITプロジェクトを企画する際に，顧客や利用者がほとんど参画していない，もしくは全く参画がみられない。ITプロジェクトの中でも明確な組織化がされておらず，役割や責任が定められていない。プロジェクトのスケジュールやマイルストーンも明確にされていない。また，プロジェクトスタッフの時間や費用は記録されておらず，予算との比較もされていない。

2：再現性はあるが，直感的

上級マネジメントは，ITプロジェクトを管理する必要を十分に理解し，周知している。組織は，プロジェクトからプロジェクトへと，一定の技法や方法を反復し，習得している過程にある。ITプロジェクトはインフォーマルながら，ビジネス目標や技術指針を定義し始めている。ITプロジェクト管理への利害関係者(ステークホルダー)の関与は限定されている。プロジェクト管理上のほとんどの局面で利用できるガイドラインが作成されているが，ガイドラインの利用は各プロジェクトマネージャの裁量に委ねられている。

3：定められたプロセスがある

IT プロジェクト管理のプロセスと方法は正式に確立しており，かつ周知されている。IT プロジェクトには，適切なビジネス目標と技術指針が定められている。利害関係者(ステークホルダー)は，IT プロジェクトの管理に関与している。また，IT プロジェクトの組織体制や役割，責任者が定められている。IT プロジェクトでは，マイルストーン，スケジュール，予算，成果達成評価の方法が定められ，更新されている。IT プロジェクトには，システム導入後の正式な手続がある。また，インフォーマルなプロジェクト管理の研修が行われている。品質保証の手続やシステム導入後の作業が定められているが，IT マネージャが幅広く適用しているわけではない。組織内外の資源をバランスよく活用するための方針が定められつつある。

4：管理，測定されている

マネジメントは，プロジェクト完了後に，正式に標準化されたプロジェクトメトリクス(評価尺度)と，“経験則”をレビューする必要がある。プロジェクト管理は，IT 部門内だけでなく，組織全体を通して測定され，評価されている。プロジェクト管理プロセスに成果がみられた場合は，それが正式に認められ，周知され，プロジェクトチームのメンバはそれらすべてを習得すべく研修を受けている。また，リスク管理はプロジェクト管理プロセスの一部として実施されている。利害関係者(ステークホルダー)は，積極的にプロジェクトに参加し，あるいは，プロジェクトをリードしている。プロジェクトマイルストーンはもちろん，マイルストーンごとの成果を評価するための規準も確立されている。プロジェクトの実行前，中途段階，および完成後に，プロジェクトの価値やリスクが測定され，管理される。また，マネジメントによって，IT 部門内にプログラム管理機能が確立されている。IT 固有の目標のためだけというよりはむしろ，組織全体の目標に積極的に取り組むために，プロジェクトが企画され，スタッフの配置や管理が行われている。

5：最適化

ライフサイクル全体を扱う実証済みのプロジェクト管理手法が導入され，制度化されており，全社的な企業文化の中に統合化されている。ベストプラクティスを見つけ，制度化するための経営的な施策(プログラム)が導入されている。上級マネジメントだけでなく，利害関係者(ステークホルダー)も，強力で前向きなプロジェクト支援を行っている。IT 管理者は，プロジェクトにおける役割や責任，スタッフの能力規準が文書化されたプロジェクト組織体系を導入している。長期の IT 資源戦略が定められ，開発や運用のアウトソーシングを支援している。また，施策(プログラム)管理機能を統合した部署があり，プロジェクトの立上げから導入後まで，プロジェクトに関する責任を一貫して担っている。施策管理部門は，ビジネスユニットの管理下にあり，プロジェクトを完成させるために IT 資源の調達や管理を行っている。組織全体でプロジェクトの計画を行うことによって，戦略的な優位性を支えるための利用者および IT 資源の最も効果的な利用が可能になっている。

PO11：品質管理

IT 顧客（カスタマ）の要求事項を満たすことをビジネス目標としている IT プロセスの**品質管理**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，はっきりとした**開発フェーズの下での明確な成果物および明示された責任を規程した品質管理の基準やシステムを企画，導入，維持することによって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
P	万全性
	可用性
	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 明確に定義され，同意された開発プロセスが，品質を保証するために作成されていること
- 品質保証プロセス上の品質管理手続に対する役割として，組織の品質の定義が行われていること
- 品質保証プログラムが測定可能な品質基準をもって適切に定義され，導入されており，また，品質管理プロセスが定められ，資源の割当てがされ，整合性が保たれていること
- 品質管理プロセスと評価尺度(メトリクス)について，継続的な改善活動や定められた知識ベースがあること
- 品質に関する教育と研修プログラムがあること
- 利害関係者(ステークホルダー)が品質保証プログラムに関与していること
- 確かな品質管理の文化が，すべてのマネジメント階層で一貫して浸透していること
- 品質規準は，サードパーティに依頼しているプロセスとプロジェクトに対しても同じように適用することが望ましいという意識があること
- あらゆるサービス提供のプロセスに，適切な品質保証規準を必要としていること
- テストの手法や技法について，IT 部門やエンド利用者部門のスタッフを研修することを重視していること

重要目標達成指標(KGI)*4

- 利害関係者(ステークホルダー)の要求事項を満たしている IT プロセスとプロジェクトの数
- 提供されたサービスに対する顧客満足度の上昇率
- 大幅な修正を行うことなく，正式に品質保証について確認・承認された IT プロセスとプロジェクトの数
- 品質上の欠陥の減少数
- 品質標準に対する準拠性違反の報告件数の減少

重要成果達成指標(KPI)*5

- 品質保証マネジメントの積極的な参画がある IT プロセスとプロジェクトの件数
- 文書化された，品質保証に関するモニタリングやテスト活動の件数
- 品質保証のピアレビューの件数
- ベンチマークされた IT プロセスとプロジェクトの数
- 利害関係者(ステークホルダー)と開発担当者とのミーティングの回数
- 品質管理のための研修の平均日数
- 文書化され，標準化された品質規準のあるプロジェクトの件数

PO11 成熟度モデル

IT 顧客(カスタマ)の要求事項を満たすことをビジネス目標としている IT プロセスの**品質管理**についてのコントロール

0：不在

組織内に品質保証を企画するプロセスがなく，またシステム開発ライフサイクル(SDLC)の方法論もない。上級マネジメントおよび IT スタッフは，品質プログラムが必要であることは認識していない。品質管理の観点からプロジェクトや運用がレビューされたことは一度もない。

1：初期／その場対応

品質保証の必要性に対する認識をマネジメントは持っている。問題が起きたときに，各専門家が品質保証を行っている。そこで行われている品質保証活動は，IT プロジェクトや IT プロセス関連の取組みに焦点が当てられており，まだ全社的プロセスには焦点が当てられていない。一般的に，IT プロジェクトおよび IT 運用の品質について評価は行われていないが，マネジメントはインフォーマルに，品質について審査している。

2：再現性はあるが，直感的

基本的な品質評価尺度が定義されており，IT 組織内でプロジェクトからプロジェクトへと反復して使用できるようになっている。また，品質保証活動を管理するためのプログラムも確立されている。品質保証活動に関し，IT の管理計画やモニタリング実務は確立されているが，広く実施されてはいない。品質管理に関する共通のツールと実務ができ上がりつつある。品質に関する満足度調査が，時折行われている。

3：定められたプロセスがある

IT 管理者は品質評価尺度についての知識ベースを構築している。品質保証プロセスが定められ，マネジメントによって周知されており，IT マネジメントおよびエンド利用者マネジメント双方を巻き込んだものになっている。品質についての教育および研修プログラムは，組織内の全階層の要員に対して行われるよう制度化されている。組織全体にわたり，品質に対する意識は高いレベルにある。品質管理ツールと実務は標準化され，原因分析が時折行われている。また，品質を測定するための標準化された手続があり，十分に体系化されている。品質に対する満足度調査も一貫して行われている。

4：管理，測定されている

組織は常に一貫して，プロセス，サービス，成果物およびプロジェクトの品質を測定している。品質保証については，サードパーティに依頼しているプロセスも含め，すべてのプロセスについて対応している。品質測定尺度に関する標準化された知識ベースが確立されつつある。品質に対する満足度調査が定常的に実施されており，原因分析に役立てられている。品質保証の取組みに合理性を持たせるため，費用対効果分析手法が用いられている。実行責任と説明責任について，IT プロセスに対してだけでなく，全社的なビジネスプロセスに対してもさらに明確に定義されてきている。また，業界や同業他社の標準に対するベンチマーキングも増えている。

5：最適化

品質に対する意識は組織全体で非常に高いレベルにある。品質保証は，IT 活動全体の中に統合され，制度化されている。品質保証プロセスは柔軟性があり，IT 環境の変化に適応できるようになっている。あらゆる品質に関する問題について，原因分析が行われている。品質に対する満足度調査が，継続的な改善プロセスに欠くことができないものになっている。知識ベースは，組織外のベストプラクティスも取り込んでより充実したものになっている。また，他社の標準に対するベンチマークが定期的に行われている。組織全体の製品やサービスが他社との競争において優位を保てるように，IT プロセスにおける品質保証と，ビジネスプロセスにおける品質保証とは完全に整合性が取れている。

調達と導入

AI1：コンピュータ化対応策の明確化

利用者の要請(ユーザ要件)を満たすために，効果的で効率的なアプローチを確実なものにすることをビジネス目標としているITプロセスの**コンピュータ化対応策の明確化**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，利用者の要請に対比して，**客観的かつ明確に識別し，分析された代替案として示された機会を計ること**で可能となる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 有効な対応策に関するノウハウがマーケットに存在していること
- 設計の確かさや機能面での安定性だけではなく，成果，拡張性，統合性を含む操作性や，管理，保守，サポート面の許容範囲，コスト，生産性，外観の点での耐久性なども考慮するように定めていること
- 自社開発，購入，アウトソーシングなどの選択肢の検討規準が定義されていること
- 一般的な調達や開発・導入の方法，あるいはシステム開発ライフサイクル方法論(SDLC)が明確になっており，それが理解され，受け入れられていること
- 対応策の計画，実施および承認について，透明度の高い，迅速かつ効率的なプロセスがあること
- 対応策の分析や改善を支援する，主要な利用者が明らかになっていること
- 対応策は，前もって定義された構成要素(コンポーネント)から作成されていること
- 構造化された要件分析のプロセスが導入されていること
- サプライヤーの責任について明確な定義があること
- 原則として，実証済みのテクノロジを使用し，ビジネス上必要な場合，そしてその使用が正当化される場合にだけ新しいテクノロジを使用すること

- 対応策の TCO(所有に掛かるトータルコスト)についての認識があること
- セキュリティおよびコントロール要件は，早い段階から考慮されていること

重要目標達成指標(KGI)*4

- プロジェクト中断後に再開された，あるいは再度取り組むことになったプロジェクトの件数または割合
- 未着手の対応策の件数，またはバックログの件数
- 最高技術責任者(CTO)または設計者(アーキテクト)から，IT 戦略および IT アーキテクチャとの整合性が取れていることについて承認を受けている対応策の件数，または割合
- 利用者の要請を完全に満たしていることが，利用者によって最終的に確認されている対応策の数あるいは割合
- 代替案，実現可能性およびリスクについて，十分に検討されている対応策の数，または割合
- ビジネスオーナおよび IT 組織によって正式に承認され，導入された対応策の割合

重要成果達成指標(KPI)*5

- 要件定義から，対応策を選定するまでの間のタイムラグ
- 受入テストで不合格になった対応策の件数，または割合
- 選定した対応策が承認されるまでの時間
- 要件定義や対応策の選定に当たり，利用者が積極的に関与しているプロジェクトの件数
- 機能変更に伴い，重大な変更要求が生じたことによって影響を受けた対応策の件数

AI1 成熟度モデル

利用者の要請(ユーザ要件)を満たすためにベストアプローチを取ることをビジネス目標としている IT プロセスの**コンピュータ化対応策の明確化**についてのコントロール

0：不在

組織は，システム，サービス，インフラ，ソフトウェア，データ等に関わる対応策を作成し，導入し，改善するために，機能面や運用面からの要求事項を明らかにする必要性はないと考えている。また，当該ビジネスに関連する潜在的に利用可能な技術的対応策があることにも気がついていない。

1：初期／その場対応

要件を定義し，技術的な対応策を明らかにする必要性に気がついている。しかしながら，そのアプローチは一貫しておらず，一定の調達および導入の方法論で行われていない。インフォーマルに個々のグループが必要性や要件について議論する場をインフォーマルに持っているが，通常，その内容は文書化されていない。対応策は，各担当者によって，限定されたマーケット情報に基づいて，あるいはベンダからの提案に応じて選択されている。利用可能なテクノロジについての体系的な分析や研究は，ほとんど行われていない，もしくは全く行われていない。

2：再現性はあるが，直感的

正式に定められた調達と導入の方法論はないが，IT 組織内では，共通の業務慣行があるため，ビジネスの枠を越えて同じような方法で要件定義が行われる傾向がある。また，IT 部門における経験や知識に基づいて，対応策がインフォーマルに選択されている。各々のプロジェクトの成功はキーとなる少数の IT 部門担当者の専門的技術に依存しており，文書の品質および意思決定にはかなりばらつきがある。

3：定められたプロセスがある

組織として調達と導入にかかわる方法論を確立しており，その中では，ビジネス要件を満たす IT 対応策を決定する際に，透明度の高い体系的なアプローチが求められる。また，そのアプローチでは，ユーザ要件，技術的タイミング，経済的な実現可能性，リスク評価およびその他のファクターについて，代替案を評価，検討することが求められている。しかし，すべてのプロジェクトにおいてこのようなプロセスがとられているわけではなく，関与したスタッフ個人の裁量，投入した管理時間，当初のビジネス要件の優先順位や規模などによってまちまちである。一般に，このプロセスは省略されているか，あるいは現実的ではないとみなされている。

4：管理，測定されている

組織は調達と導入の方法論を確立しており，その方法によらないことのほうがむしろ例外であるというレベルに達している。文書化の品質は高く，文書化によって各段階で適切な承認を受けている。また，要件は明確に記述され，前もって定められた体系に沿っている。この方法論においては，情報に基づいた選択ができるように，対応策の代替案について適切に検討し，費用対効果分析を実施することが強く求められている。また、方法論は明確に定義され，一般的に理解し，計測することが可能になっている。そのため，マネジメントは例外事項を早期に発見し改善することができる。対応策はユーザ要件を効率的に反映しており，前向きな対応策が，ビジネスプロセスの改善や競争優位性の向上につながるという認識を持っている。

5：最適化

組織の調達と導入に関する方法論は，間断のない改善を積み重ね，テクノロジの変化に対応している。方法論には柔軟性があり，大規模で全社的なアプリケーションから，特定の戦略的なプロジェクトまで，さまざまなプロジェクトに用いることができる。また，テクノロジ対応策に関する参考資料を含めて，組織内外の知識データベースによって方法論は支援されている。方法論自体が，本番運用と保守を効率的に行うためにあらかじめ定められた体系に従い，コンピュータ化された文書様式を提供している。その結果，競争上優位に立つこと，ビジネスプロセスの再構成の促進，全体的な効率の改善のために，テクノロジ利用の新たな機会を見出せる組織体制になっている。

AI2：アプリケーションソフトウェアの調達と保守

ビジネスプロセスを効果的に支援するためのコンピュータ化された機能を提供することをビジネス目標としている IT プロセスの**アプリケーションソフトウェアの調達と保守**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**機能面や運用面に関する要求事項の詳細記述書の定義，および明確な成果物を伴う段階的な導入によって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
S	万全性
S	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
✔	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 調達および開発・導入の方法論を，上級管理者が強力に支援していること
- 調達の手続が明確で，また広く理解され，受け入れられていること
- 正式に受け入れられ，理解され，かつ実施されている調達および開発・導入の方法論があること
- 一連の自動化された支援ツールを使うことが可能となっており，最も条件に合うものに絞り込むことでソフトウェアの選定に要する時間を短縮できること
- 開発業務とテスト業務の分離がされていること
- 時間，品質あるいはコスト面の都合で解決できない場合，可能な範囲での削減を行うえで，主要な要件の優先づけがされていること
- アプリケーションの業務目的適合性に基づいて，アプローチの仕方や投入されるリソースが決められていること
- 導入に当たり要求される文書化のレベルと様式が合意されており，それが守られていること
- 企業の IT アーキテクチャの遵守について，遵守外の事例を認める正式なプロセスも含めてモニタされていること

重要目標達成指標(KGI)*4

- 仕様書の要件を満たし，IT アーキテクチャとの整合性が確保され，期限どおりに納入されたアプリケーションの件数
- 導入時にシステム統合の問題が生じなかったアプリケーションの件数
- アプリケーションごとの保守コストが設定金額以下になっていること
- 明らかな機能停止やサービスの低下を引き起こしている各アプリケーションについて，本番稼働上で発生した問題の件数
- 現在承認されている IT 戦略との整合性が取られていない対応策の件数
- 新規に開発したアプリケーションに関する保守工数の低減率

重要成果達成指標(KPI)*5

- アプリケーションのポートフォリオ平均に対する，各アプリケーションの実際の保守コスト比率
- ファンクションポイント法あるいはモジュール法のような尺度に基づいて，機能性を評価するまでに要する平均時間
- バグや重大なエラー，新しい機能仕様によって生じた変更要求の件数
- アプリケーションごと，保守における変更ごとに，発生した本番上の問題や機能不全の件数
- 文書化されていないアプリケーションや，納期に間に合わせるために行った未承認の設計，テスト期間の短縮など，標準手続からの逸脱件数
- 返品されたモジュールの数や受入テスト後に必要となった手戻りのレベル
- 問題を分析して修正するまでのタイムラグ
- 保守のために効果的に文書化されているアプリケーションソフトウェアの数または割合

AI2 成熟度モデル

ビジネスプロセスを効果的に支援するためのコンピュータ化された機能を提供することをビジネス目標としている IT プロセスの**アプリケーションソフトウェアの調達と保守**についてのコントロール

0：不在

アプリケーションを設計し，仕様を決める業務プロセスがない。アプリケーションは，ベンダからの提案や，ブランドイメージ，あるいは IT スタッフに馴染みがある製品かどうかに基づいて調達されており，実際の要求事項については，ほとんどまたは全く検討されていない。

1：初期／その場対応

アプリケーションの調達と保守に関する業務プロセスが必要であるという認識はある。しかし，アプローチはプロジェクトごとにまちまちで一貫性がなく，一般に他のプロジェクトとは全く異なる。組織内で，個別にさまざまな対応策が取られる傾向があり，保守やサポートに関して以前からある課題や非効率性の問題を現在も抱えている。ビジネス利用者は IT 投資を有効利用することができていない。

2：再現性はあるが，直感的

アプリケーションの調達と保守に関して似たようなプロセスはあるが，IT 部門内のノウハウをベースにしており，文書化されたプロセスには基づいていない。アプリケーションの成功は，組織内の技術力および IT 部門内のスタッフの経験レベルに大きく依存している。保守には何らかの問題がいつもあり，社内の知識を持ったものが流失した場合には害を受けることになる。

3：定められたプロセスがある

文書化された調達と保守のプロセスがある。文書化されたプロセスを他のアプリケーションやプロジェクトにも一貫して適用しようとする試みはあるが，いつでも，全て導入に実際的であるとは限らず，また最新のテクノロジ対応策に対応しているわけではない。一般には柔軟性が低く，すべてのケースに適用することが難しいため，しばしばステップが省略される。このため，アプリケーションがバラバラな方法で調達される結果を招いている。保守は決められたアプローチによっているが，時間が掛かり，効率が悪くなっていることが多い。

4：管理，測定されている

正式に承認され，内容が明確で，適切に理解されたシステム調達と導入についての方法論と方針がある。そこには，設計や仕様を決める正式なプロセスや，アプリケーションソフトウェアの調達規準，テストプロセスや文書化の要件などが含まれており，あらゆるアプリケーションを一貫した方法で調達, 保守することができるようになっている。また，正式な承認のメカニズムが構築され，すべてのステップで実行されており，例外事項は必ず承認を受ける仕組みになっている。これらの方法論は，組織に十分適合しており，すべてのスタッフによって積極的に利用され，大多数のアプリケーションの要件に適用可能なものになっている。

5：最適化

合意されたプロセスに従って，アプリケーションソフトウェアの調達と保守が行われている。そのプロセスにおけるアプローチは，あらかじめ定められ，ビジネスニーズに適合した標準アプリケーションの構成(コンポーネント)を基にするものである。また，全社的なアプローチが通常取り入れられている。調達と保守のプロセスは十分に発達しており，ビジネス要件の変更に対しても迅速な対応が可能であり，柔軟性を持つと同時に高い感応性を備えている。アプリケーションソフトウェアの調達と導入プロセスに対しては絶えず改善が行われており，参考資料やベストプラクティスを含む組織内外の知識データベースによって補完されている。このような方法論を用いることによって，あらかじめ定められた体系に従ってコンピュータ上の文書が作成され，本番運用と保守が非常に効率的に行えるようになっている。

AI3：技術インフラの調達と保守

ビジネスアプリケーションを支えるための適切なプラットフォームを提供することをビジネス目標としているITプロセスの**技術インフラの調達と保守**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**熟慮したハードウェアの調達，ソフトウェアの標準化，ハードウェアとソフトウェアの成果評価および一貫したシステム管理によって**可能となる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
S	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
	アプリケーション
✔	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 調達および開発・導入の方法論を，上級管理者が強力に支援していること
- 調達の手続が明確で，また広く理解され，受け入れられていること
- 異なるテクノロジプラットフォーム間の統合が容易であること
- ビジネス戦略およびそれに関連したアーキテクチャの要件が，上級管理者によって定められ，適切に示され，かつ支援されていること
- ハードウェアとソフトウェアのインフラについての最新の棚卸リストが利用できる状態になっていること
- ベンダとの良好な関係を築いていること
- 異なるテクノロジのプラットフォーム間で重複しているコストを適切に解消できること
- 自社開発するのか，外部のインフラやアウトソーシングを利用するのかについて，適切な選択をうながすような方針が定められていること
- 再利用性の高い構成要素かどうかに着目して選択していること
- 単独のサプライヤへの依存状況を管理するための方針が定められていること
- 変更管理プロセスとシステムとの整合性が保たれていること
- 適切に定義されたライフサイクルの手法を用いて，インフラ技術を選択，調達，保守，

廃棄していること
- 調達において，能力(キャパシティ)や成果管理プロセスと整合性を取りながら，成果と能力の要件を十分に検討していること
- 一連の自動化された支援ツールを使うことが可能となっており，最も条件に合うものに絞り込むことでソフトウェアの選定に要する時間を短縮できること

重要目標達成指標(KGI)*4

- 合意された技術インフラに合致していないプラットフォームの削減数
- インフラの不備のためにシステム導入が遅れた件数
- 新規開発に関する保守工数の低減率
- インフラをあらかじめ定義し，柔軟性を持たせることによって実現した，システムを市場投入するまでに要する時間の短縮
- インフラの機能停止時間の短縮
- 相互運用性に深刻な問題があるシステムの削減数
- 技術インフラの不備に起因するアプリケーションの成果上の問題数

重要成果達成指標(KPI)*5

- 異なるプラットフォーム利用の削減数
- プラットフォームの使用年数
- 共有している機能とリソースの数
- 変更の回数と頻度
- 予防保守の欠如による障害発生件数
- システムソフトウェアの変更による障害発生件数
- 工数と所要時間をベースにして算出した，システムソフトウェアやインフラへの主要な変更に掛かる諸コスト

AI3 成熟度モデル

ビジネスアプリケーションを支えるための適切なプラットフォームを提供することをビジネス目標としている IT プロセスの**技術インフラの調達と保守**についてのコントロール

0：不在

技術アーキテクチャが，対応すべき重要な課題であるとは考えられていない。

1：初期／その場対応

インフラの変更が，全社的な計画がないままに，新しいアプリケーションごとに行われている。IT インフラが重要であるという認識はあるが，一貫した全社的なアプローチがない。

2：再現性はあるが，直感的

IT インフラを調達，保守する際に，戦術的なアプローチにおいては一貫性が保たれて

いるが，何ら決められた戦略に基づいているわけではなく，また，支援すべきビジネスアプリケーションのニーズについても考慮していない。

3：定められたプロセスがある

IT インフラの管理について，明確に定められ，一般に理解されている業務プロセスが明らかになっている。このプロセスによって，重要なビジネスアプリケーションのニーズを支援し，IT およびビジネス戦略との整合性が保たれている。しかし，一貫して適用されているとはいい難く，したがって，インフラがビジネスアプリケーションのニーズを十分に支援しているとは言えない。一般に，問題に対応するため，または特定の機会に応えるため，IT インフラの全体，もしくは一部をアウトソーシングする。

4：管理，測定されている

技術インフラの調達と保守のプロセスは，ほとんどの状況で適切に機能するレベルにまで整備されてきており，IT 部門内では一貫してそのプロセスをとっている。また，プロセスは構成要素(コンポーネント)に基づいており，再利用性に焦点が当てられている。正式に承認され定められたプロセスに従っていないインフラへの変更は，事前に検出され，防止されている。IT インフラは，ビジネスアプリケーションを適切に支援しているといえる。プロセスは体系化されてはいるが，前向きな対応を行うというより，むしろ場当たり的な対応になっている場合が多い。また，拡張性，柔軟性，統合性における期待レベルを達成するために必要なコストやリードタイムの最適化はまだ行われていない。IT インフラの全体，もしくは一部をアウトソーシングすることは戦術計画の一部になっている。

5：最適化

技術インフラの調達と保守のプロセスは先を見通したものになっており，主要なビジネスアプリケーションや技術アーキテクチャと厳密に整合性が保たれている。技術的な対応策に関連するベストプラクティスの追求によって，全社的なアプローチや，信頼性，可用性，ネットワークセキュリティのレベル向上の必要性などを含む最新のプラットフォームの開発，および最新の管理ツールについての知識を得ている。また，インフラの構成要素(コンポーネント)を合理化し標準化することや，自動化ツールを利用することによってコストが削減されている。組織内には高度な専門技術力があり，アウトソーシングを選択肢の一つとして検討することも含め，成果を積極的に改善していくための最適な方法を見出すことが可能である。また，既存のインフラの成果をモニタし，測定することによって，問題をタイムリに検出することができるようになっている。IT インフラは，IT の効果的な利用のキーとなる遂行能力であるとみなされている。単一のソース・サプライヤに対するリスク管理も積極的に行われている。

AI4：操作，運用手続の作成と維持

導入されるアプリケーションや技術的対応策の適切な利用を保証することをビジネス目標としているITプロセスの**操作，運用手続の作成と維持**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**利用者，運用手続書，サービス要件，研修資料の作成に対する構造化されたアプローチによって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
S	万全性
S	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 適切に定められたサービスレベルアグリーメントがあり，文書化の標準に明確にリンクしていること
- 研修講師，ヘルプデスク，利用者グループの間で，利用者手続書，技術手続書，研修資料の共有が促進されるように，インフラおよび組織がデザインされていること
- 操作手続に関する利用者研修は，組織およびIT研修計画の中にまとめられていること
- ビジネスプロセス，業務手続書およびIT手続書の一覧リストが，自動化されたツールによって保持されていること
- 開発プロセスでは，標準運用手続書や標準画面操作法(ルック・アンド・フィール)が必ず使用されていること
- 文書化や諸手続書に関する標準のフレームワークを定め，モニタしていること
- ナレッジマネジメントやワークフロー技法，自動化されたツールが，手続書の作成，配布，保守に利用されていること

重要目標達成指標(KGI)*4

- IT手続書が，ビジネスプロセスの中に継ぎ目がなく組み込まれているアプリケーショ

ンの件数
- 利用者手続書，運用手続書，研修資料の欠如など，適切に文書化されていない技術的対応策の件数
- 研修資料，利用者手続書，運用手続書についての満足度を図るための複合評価尺度
- 利用者手続書，運用手続書，研修資料の作成，および保守に掛かるコストの低減
- 利用度をもとに割り出したシステム利用者の熟練度

重要成果達成指標(KPI)*5

- 各アプリケーションにおける利用者とオペレータの研修への参加状況
- システム変更要求の正確性および，利用者手続書，IT 手続書，研修資料の完全性
- システム変更から，研修資料や手続書，文書類が改訂されるまでのタイムラグ
- 研修資料，利用者手続書および運用手続書に関する満足度調査の指標
- ヘルプデスクが対応した，研修対応コール数の減少
- 文書化の不備によって起こった問題の件数
- 適切な利用者研修が行われているアプリケーションの件数

AI4 成熟度モデル

導入されるアプリケーションや技術的対応策の適切な利用を保証することをビジネス目標としている IT プロセスの**操作，運用手続の作成と維持**についてのコントロール

0：不在

利用者手続書，運用手続書，研修資料の作成に関する業務プロセスがない。唯一，購入した製品に付属の資料だけがある。

1：初期／その場対応

組織内で，文書作成の業務プロセスが必要であることに気がついている。文書化は時々行われているが，各所でばらばらに作業しており，その利用は，限定されたグループに限られている。多くのマニュアルや手続書は古くなっており，異なるシステム間やビジネスユニットをまたがる手続書については全く整合性が取られていない。研修資料は品質にばらつきがあって，一回限りのものになる傾向にあり，たいていの場合，サードパーティが提供する汎用的な資料で，組織向けにカスタマイズはされていない。

2：再現性はあるが，直感的

手続書の作成と文書化に関して用いられているアプローチは似通っているが，構造化されたアプローチやフレームワークに基づいていない。利用者手続書，運用手続書は文書化されているが，同一体系のアプローチがないため，これらの文書の正確性や可用性のかなりの部分は，正式なプロセスに基づいているというよりはむしろ，担当者個人に依存している。研修資料は利用できるようになっているが，個人的に作成される傾向にあり，品質も作成に携わった個人の裁量に委ねられている。したがって，実際の手続書や利用者支援の質は，低いものから高いものまでばらつきがあり，組織全体では，ほとんど一貫性も整合性もない。

3：定められたプロセスがある

利用者手続書，運用手続書，研修資料に関して，明確に定められ，広く受け入れられ，理解されているフレームワークがある。手続書は正式のライブラリに保管，保守されており，必要な時には誰でもアクセスすることができるようになっている。また，必要に応じて手続書の改善が行われている。手続書類はオフラインでの利用が可能で，災害が発生した場合にもアクセスや保守が可能となっている。手続書の変更を把握し，研修資料に変更プロジェクトについて明確に盛り込むためのプロセスがある。定められたアプローチがあるにもかかわらず，標準を遵守させるためのコントロールがないため，実際の内容にはばらつきがある。利用者は，インフォーマルにこれらのプロセスに関与している。また，自動化されたツールが手続書の作成と配布に徐々に使われ始めている。

4：管理，測定されている

一貫性が遵守されており，手続書や研修資料を保守するためのフレームワークの改善が行われている。すべてのシステムおよびビジネスユニットにおいて，特定のアプローチが取られているため，各プロセスをビジネスの視点から見ることができ，従属関係やインタフェースも含めて，プロセス全体の整合性が取られるようになっている。また，標準が守られ，すべての業務プロセスに対して手続書が作成され，保守されることを保証するコントロールがある。利用者からのフィードバックを集め，そのスコアが悪い場合には，改善のアクションが取られる。そのため，文書類や研修資料は，信頼性と可用性において，通常，期待できる良い水準を保っている。手続書の自動作成によって，アプリケーションシステムの開発との整合性がますます取られるようになり，手続書作成の一貫性が高められ，手続書への利用者のアクセスが促進されている。

5：最適化

利用者および運用に関する文書化のプロセスは，新しいツールや方法論の導入によって絶えず改善されている。手続書は，最新のナレッジマネジメントやワークフロー，配信テクノロジを用いて，コンピュータ管理されている知識データベースの中に常に蓄積されているため，アクセスや保守がしやすくなっている。文書類は，組織上，運用上，ソフトウェア上の変更を反映して更新されており，ビジネスプロセスの定義と完全に整合性が取られている。したがって，IT だけを対象にした手続書というよりはむしろ，全社的な要求事項を支援できるものになっている。

AI5：システムの導入と受入信認

意図した目的に対応策が適しているかを検証し，確認することをビジネス目標としているITプロセスの**システムの導入と受入信認**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**十分に定型化された，導入，移行，変換，受入計画を実行することによって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
	効率性
	機密性
S	万全性
S	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 調達と導入の方法が確立され，かつ一貫して適用されていること
- 本番環境と分離したテスト環境を実現するために利用可能な資源があること。またテストプロセスに十分な時間を割り当てていること
- テスト，研修および移行プロセスにおいて，利害関係者(ステークホルダー)の関与責任(コミットメント)と参画が保証されていること
- テストデータが利用可能で，種類と量の面において本番データを代替するものとなっており，またテスト環境は可能な限り本番環境に近い環境になっていること
- プロセスの最適化および継続的な改善のために，フィードバックの仕組みが導入されていること
- 新システムを稼働する前には，新システムに対する負荷テストを実施していること
  また，システムへの変更が加えられた場合には，既存システムに対する退化テストを行っていること
- セキュリティに関する正式な認証と受入信認のシステムの手続が，一貫して定められ遵守されていること
- 運用上の要件についての明確な理解と評価があること

重要目標達成指標(KGI)*4

- 導入ミスや受入信認のマイルストーンの削減数
- セキュリティの認証や受入信認のプロセスの最初から最後まで，導入や受入信認が完了するまでに要する時間
- 導入時に，信認のプロセスがなかったために受入信認なしで運用されているシステムの削減数
- 導入されたシステムのオペレーションを最適化するために必要なシステム変更の回数
- システムの受入テスト後に必要になったシステム変更の回数
- 導入および受入信認のプロセスに関する内部または外部監査における検出事項の数
- 対応策を本番環境に組み入れた後で，問題点の修正のために必要となったシステム変更の回数

重要成果達成指標(KPI)*5

- 導入と受入信認のプロセスにおける利害関係者(ステークホルダー)の関与度
- 自動化されている導入と受入信認のプロセスの件数
- 経験則(レッスン・ラーンド)の報告頻度
- 導入と受入信認のプロセスに対して報告された利用者の満足度(経験則)
- 導入と受入信認の機能に関する品質保証レビューにおける検出事項の数
- テストプラットフォームの再利用性

AI5 成熟度モデル

意図した目的に対応策が適しているかを検証し，確認することをビジネス目標としているITプロセスの**システムの導入と受入信認**についてのコントロール

0：不在

正式な導入や受入信認のプロセスが全くなく，上級管理者あるいはITスタッフは対応策が意図した目的に適合していることを確認する必要性を認識していない。

1：初期／その場対応

導入された対応策が意図した目的に適しているか検証し，確認する必要性に気づいている。受入テストはいくつかのプロジェクトにおいて行われているが，テストに対するイニシアティブは各プロジェクト・チームに委ねられており，そのアプローチは多様である。正式な受入信認やサインオフはほとんど行われていないか，もしくは全く行われていない。

2：再現性はあるが，直感的

テストアプローチと受入信認アプローチの間には若干の整合性が見られるが，それらは特定の方法論に基づいているわけではない。通常，個々の開発チームがテストアプローチを決定しており，統合テストが欠落していることが多い。インフォーマルな承認プロセスがあるが，必ずしも標準化された基準に基づくことが求められているわけではない。受入信認やサインオフも時折行われている。

3：定められたプロセス

導入，移行，変換，受入に関する正式な方法論がある。しかしながら，マネジメントは，その方法論に対する遵守性を評価する能力を持っていない。IT の導入プロセスと受入信認プロセスは，システムライフサイクルとの整合性が取られ，ある程度自動化されている。研修やテスト，本番移行および受入信認は，各担当者の裁量に委ねられており，決められたプロセスとは乖離する場合もある。本番環境に組み込まれるシステムの品質は統一されておらず，新システムには導入後にも重大な問題が頻繁に発生している。

4：管理，測定されている

手続書が正式化され，適切に体系化されており，また，テスト環境や受入信認手続が定義されているため実務的なものになっている。実務上，システムに対するすべての主要な変更は，この正式なアプローチに従っている。ユーザ要件の満足度評価は標準化され，測定可能であり，マネジメントによって効果的にレビュー，分析ができるような評価尺度が示されている。本番稼働しているシステムの品質は，マネジメントにとって満足がいくものであり，導入後発生する問題は合理的なレベルのものである。プロセスの自動化はその場対応的で，各プロジェクトに依存している。システム導入後の評価も定期的な品質レビューも一貫して行われていないが，マネジメントは現状の有効性レベルに満足していると思われる。テスト用のシステムは本番環境を適切に反映している。主要なプロジェクトについて，新システムに対する負荷テストや既存システムへの退化テストを行っている。

5：最適化

導入プロセスおよび信認プロセスは，継続的な改良と改善によって，ベストプラクティスのレベルにまで到達している。IT の導入と受入信認のプロセスは，システムライフサイクルの中に完全に統合されており，有効な場合には自動化され，最も効率的な研修やテスト，新システムへの本番移行が促進される仕組みになっている。また，十分に整備されたテスト環境，問題の記録や問題解決のプロセスが，効率的かつ効果的に本番環境へ移行されることが保証されている。受入信認で通常差し戻しになるものは限られている。また，導入後の問題も普通は小さな修正程度のものとなっている。導入後のレビューも標準化されており，継続的な品質改善を保証するために経験則(レッスン・ラーンド)がそのプロセスの中に組み込まれている。新システムに対する負荷テストや修正されたシステムに対する退化テストが一貫して行われている。

AI6：変更管理

システムダウンや未承認の変更，エラーの発生率を最小限にとどめることをビジネス目標としている IT プロセスの**変更管理**についてのコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**既存の IT インフラに対して変更を依頼され，実施したすべてのものを分析，導入およびフォローアップできる管理システムがあることによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
P	万全性
P	可用性
	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 変更方針は，明確で周知されており，厳密かつ組織的に実行されていること
- 変更管理はリリース管理との整合性が高く，構成管理の不可欠な要素となっていること
- 変更の認識，分類，影響度評価，優先順位付けなどを含む，迅速，かつ効率的な計画，承認，開始のプロセスがあること
- ワークフロー定義，定型のスケジュール表，承認テンプレート，テスト，構成，配布を支援するための自動化したプロセスツールが利用可能であること
- 変更実施前に，目的にそった包括的な受入テストの手続が適用されていること
- 個々の変更だけでなく処理パラメータの変更も追跡し，フォローするためのシステムがあること
- 開発から運用への正式な引継ぎプロセスが定義されていること
- 変更による容量や成果要件への影響が考慮されていること
- 完全で最新のアプリケーションおよび構成資料が利用可能であること
- 相互関係を考慮しながら，変更の前後での調整を管理するプロセスがあること
- 変更が成功なのか，失敗なのかを検証する独立したプロセスがあること
- 開発と本番で，職務の分離がなされていること

重要目標達成指標(KGI)*4

- 変更によってシステムにもたらされたエラーの数の削減数
- 不適切な変更管理によるダウン(可用性の損失)の数の削減数
- 変更に起因するダウンの影響度の低減度
- 変更回数に対する，変更に必要とされたリソースと時間の割合の低減度
- 緊急修正対応の回数

重要成果達成指標(KPI)*5

- 同時に異なるバージョンがインストールされた件数
- プラットフォームごとのソフトウェアリリースおよび配布方法の数
- 標準構成から乖離している件数
- 通常の変更管理が遡及的に適用されなかったために緊急修正対応した件数
- 修正が可能になってから導入されるまでのタイムラグ
- 導入要求が拒否された変更に対する，導入が受け入れられた変更の割合

AI6 成熟度モデル

システムダウンや未承認の変更，エラーの発生率を最小限にとどめることをビジネス目標とする IT プロセスの**変更管理**についてのコントロール

0：不在

決まった変更管理のプロセスはなく，さまざまな変更を，事実上コントロールなしで行うことができる。このような変更が IT およびビジネスの運用に対して，混乱を引き起こす可能性があるという認識がなく，変更管理の利点についても気がついていない。

1：初期／その場対応

変更については管理され，コントロールされるべきであると認識しているが，従うべき一貫した業務プロセスがない。実務はばらばらで，未承認の変更が行われる可能性が高い。変更に関する文書化は，ほとんどないか，あるいは全く実施されておらず，構成の文書化は不完全で，信頼性がない。不十分な変更管理が原因で，本番環境を中断せざるを得ないようなエラーが起こり得る。

2：再現性はあるが，直感的

インフォーマルな変更管理プロセスが適用され，多くの変更がこのアプローチに従っている。しかしながら，そのプロセスは体系化されておらず，不完全でエラーが発生しやすい。構成の文書化の正確性は一貫しておらず，計画の段階や変更の実行前に影響分析が行われているにすぎない。そのため，かなり非効率的であり，手戻りも多く発生している。

3：定められたプロセスがある

カテゴリごとの分類，優先順位付け，緊急時の手続，変更の承認，リリース管理などを含めた正式に決められた変更管理プロセスが適用されている。しかし，これらのプロ

セスの遵守を制度化していない。決められたプロセスは常に適切で実務的であるとは限らないため，その結果として回避策がとられたり，プロセスが省略されたりしている。また，エラーも発生しやすく，未承認の変更が時々行われる。新しいアプリケーションやテクノロジのロールアウト計画を支援するために，IT の変更がビジネスに与える影響の分析が正式化されつつある。

4：管理，測定されている

変更管理プロセスが適切に策定され，すべての変更に対して一貫して適用されており，マネジメントは例外処理がないことに確信を持っている。プロセスは効率的，かつ効果的であるが，一定の品質を保証するために，多くの手作業による手続とコントロールに依存している。すべての変更は，本番移行後に問題が発生する可能性を最小限にするために，計画策定と影響分析を徹底して行うことを条件としている。また，変更の承認プロセスも整備されている。変更に対しては正式に追跡が行われており，変更管理文書は最新かつ正確なものになっている。構成の文書化も通常，正確である。IT の変更管理に関する計画策定と導入は，ビジネスプロセスの変更との整合性が高まり，研修，組織改編，事業継続問題にも対処できるようになっている。また，IT の変更管理とビジネスプロセスの再設計との間の整合性も高められている。

5：最適化

変更管理プロセスは定期的にレビューされ，ベストプラクティスとの整合を保てるように更新されている。構成の情報は，コンピュータ上に載せられ，バージョン管理にも利用されている。ソフトウェア配布が自動化され，リモートモニタリング機能が利用可能になっている。構成管理やリリース管理，変更の追跡には最新の技術が導入されており，未承認やライセンスのないソフトウェアを検出するツールを持っている。IT によって，組織の生産性を高め，新しいビジネスチャンスを作ることを確実に実現するために，IT の変更管理はビジネスの変更管理と一体化している。

サービス提供とサポート

DS1：サービスレベルの定義と管理

提供すべきサービスレベルに関して共通の理解を得ることをビジネス目標としているITプロセスの**サービスレベルの定義と管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**サービスの質と量を測定評価するための成果規準を正式に定めるためのSLA（サービスレベルアグリーメント）の確立によって**可能となる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
S	準拠性
S	信頼性

（P）主　（S）準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

（✔）該当

主要成功要因(CSF)　*3

- 可能な限り，エンドユーザのビジネス用語でサービスレベルを表現すること
- サービスレベル違反が発生した場合，原因分析を実施すること
- サービスレベルに関する有益でタイムリな情報を提供するための，スキルとツールが利用可能になっていること
- 重要なビジネスプロセスのITへの依拠状況が明らかになっており，SLA(サービスレベルアグリーメント)の対象に含まれていること
- IT管理者の説明責任と実行責任が，サービスレベルにリンクしていること
- IT組織が，原価差異の原因を特定することができること
- 原価差異について，詳細な一貫した説明ができること
- 個別の変更を追跡，事後調査するためのシステムがあること

重要目標達成指標(KGI)　*4

- 主要なビジネス目標とサービスレベルが整合していることを，戦略的ビジネスユニットが確認し承認していること
- サービスレベルが期待どおりであるという利用者の満足度

- サービスレベルに従った予算に対する実際のコストの比率
- IT に依拠している重要なビジネスプロセスのうち SLA(サービスレベルアグリーメント)の対象範囲に含まれている割合
- SLA(サービスレベルアグリーメント)のうち，一定期間ごとに見直されるものや大幅な改訂を行ったものの割合
- 提供されたサービスレベルのモニタリング情報を，サービスレベルパートナ(サービス提供相手)が確認し，承認している割合
- SLA(サービスレベルアグリーメント)の条件を満たしている IT サービスの割合

重要成果達成指標(KPI)　*5

- サービスレベルの変更依頼から解決までのタイムラグ
- 利用者満足度調査の頻度
- サービスレベルに関する課題が解決されるまでのタイムラグ
- サービスレベルに関する課題の原因分析と対応が期限内に完了した回数
- 規定のサービスレベルの提供に必要な追加投資額の規模

DS1 成熟度モデル

提供すべきサービスレベルに関して共通の理解を得ることをビジネス目標としている IT プロセスの**サービスレベルの定義と管理**におけるコントロール

0：不在

経営者はサービスレベルを定める必要があると認識していない。サービスレベルをモニタリングするための実行責任や説明責任は誰にも割り当てられていない。

1：初期／その場対応

サービスレベルを管理する必要性は認識している。しかしそのプロセスはまだ正式なものではなく，事後対応的である。 成果をモニタリングする実行責任と説明責任は，インフォーマルに定められている。成果評価尺度は定性的であり，目標はあいまいである。成果報告書は，たまに発行される程度であり，また一貫していない。

2：再現性はあるが，直感的

SLA(サービスレベルアグリーメント)は合意されているが，正式なものではなく，また再検討されることはない。サービスレベルの報告書は，不完全で，不適切であり，また誤解を招きやすく，個々の管理者のスキルや取組みに依存している。サービスレベル・コーディネータ(進行責任者)は，実行責任を明確にしたうえで任命されているが，十分な権限を持っていない。SLA(サービスレベルアグリーメント)を遵守するかどうかは裁量に任されており，強制されていない。

3：定められたプロセスがある

実行責任は明確にされているが，自由裁量に任されている。 SLA(サービスレベルアグリーメント)作成手順は整備されており，サービスレベルの再査定と利用者満足につい

てのチェックポイントが決められている。サービスレベルの規準は決まっていて，利用者の合意済みであり，より高い水準で標準化されている。サービスレベルが期待を下回った場合は検知されているが，解決のための計画立案はまだ正式なものではない。投下した資金と期待されるサービスレベルの関係は，徐々には正式になってきている。サービスレベルは徐々に業界のベンチマークに基づいてきているが，組織固有のニーズに対処していない場合がある。

4：管理，測定されている

サービスレベルはシステムの要件定義段階で定義されるようになり，アプリケーションとオペレーション環境の設計にも織り込まれるようになってきている。利用者満足度は定期的に測定，査定されている。 成果測定評価は，単に IT 目標に対する評価というよりも，徐々にエンドユーザのニーズを反映したものになってきている。利用者サービスレベルの評価基準は，標準化されつつあり，業界標準を反映したものになっている。サービスレベルが満たされない場合は，原因分析が行われる。サービスレベルをモニタリングするための報告システムは，徐々に自動化されてきている。合意されたサービスレベルを満たさない場合の運用上，財務上のリスクは明確にされ，理解されている。

5：最適化

IT 目標と経営目標とが整合するようにサービスレベルは，継続的に再評価されている。同時にサービスレベルは技術進歩とプロダクト価格／成果比の向上を享受している。サービスレベルのプロセスにおいてすべて，継続的な改善を行っている。サービスレベルを定める規準は，ビジネスの重要度に基づいており，その規準には，可用性，信頼性，成果，能力(キャパシティ)の伸び，利用者サポート，業務継続計画，セキュリティ対策を含んでいる。利用者満足度はモニタリングされ，満足のいくように高められる。サービスレベルは，業界標準と比較して評価されるばかりでなく，ビジネスユニットの特定の戦略目標も反映している。IT 管理者にはサービスレベルの成果目標を達成するのに必要な資源を割り当てられており，それに対する説明責任を有している。さらに IT 責任者の役員報酬は，組織目標を達成させるためのインセンティブとして働くような仕組みになっている(組織目標の達成度に応じて，IT 責任者の役員報酬が支払われる) 。

DS2：サードパーティのサービスの管理

サードパーティの役割と実行責任が明らかに定められ，遵守され，継続して要求事項が満たされることをビジネス目標としているITプロセスの**サードパーティのサービスの管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**契約と手続を，その有効性と組織の方針への遵守性の観点から，レビュー，モニタリングすることを目的としたコントロール手段によって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- サービス要件や成果評価尺度があり，明確になっている。
- 組織には説明責任と統制力を持って，外部サービスを前向きに管理している。
- サービスプロバイダが成果評価を報告する仕組みがある。
- サードパーティ・プロバイダは，品質保証プログラムを整備している。
- すべての提供すべきサービス(オペレーション要件と成果要件を含む)が十分に定義され，すべての関係者に理解されている。
- サービス要件と成果評価尺度に関する，効果的な変更手続がある。
- 契約締結の前に，法務担当によるレビューと承認を受けることが条件となっていること
- 財務，オペレーション，法務，コントロール上の問題を取り扱うための適切な経営・管理規定があること
- SLA(サービスレベルアグリーメント)の適用上の報償／報酬やペナルティについて，お互いに合意していること
- 社内の契約担当責任者をサードパーティとの唯一の契約窓口としていること
- あらかじめ定められ，合意された評価規準を備えた，提案依頼書(RFP)作成のプロセス

があること
- サービス上の問題点について，問題の重要性と必要な対策に基づいて分類するプロセスがあること

重要目標達成指標(KGI)　*4

- サービスプロバイダのうち，目標が正式に合意されているものの割合
- サービスプロバイダの適格性が検討された，重要な契約の割合
- サービスプロバイダのうち，正式に適格とみなされたものの割合
- サードパーティ契約者のうち，目標が明確にされ，期待されるサービス提供内容が定められているものの数
- 現在の経常的関係に対する当事者双方の満足度
- サードパーティ契約者のうち，目標やサービスレベルを達成できなかったものの数
- 契約締結が不適切であったり，あるいは契約は適切であったが成果が不十分であったために生じた，サードパーティとの争議(紛争)の数とコスト

重要成果達成指標(KPI)　*5

- レビューミーティングの回数と頻度
- 契約を改定した数
- サービスレベルに関する報告書の発行頻度
- 未解決課題の数
- 問題を解決するまでのタイムラグ
- 法的レビューを受けていない契約の割合
- 市場動向の変化に対し，最近実施した契約レビューから経過した時間
- サービス契約のうち，標準的な契約条件ではなかったり，承認された例外条項を使っていない契約の数

DS2 成熟度モデル

サードパーティの役割と実行責任が明らかに定められ，遵守され，継続して要求事項が満たされることをビジネス目標としている IT プロセスの**サードパーティのサービスの管理**におけるコントロール

0：不在

実行責任も説明責任も明らかでない。サードパーティとの契約締結方法について，正式な方針や手続がない。サードパーティから受けたサービスを，管理者は一度もレビューや承認したことがない。サードパーティからの報告もなく，評価活動は行われない。契約で報告義務を定めていないため，上級管理者は提供されたサービスの質に興味がない。

1：初期／その場対応

サイン捺印した契約書を入手すること等，サードパーティからサービスの提供を受ける際の方針や手続を文書化する必要性を経営者は感じている。契約書の標準的な契約条項は定められていない。提供されたサービスの評価は事後的に行われるが，正式なもの

ではない。実務は，担当者の経験やサプライヤ側の都合によってさまざまである。

2：再現性はあるが，直感的

サードパーティ・サービスプロバイダやその提供するサービスをモニタリングする手続はインフォーマルである。標準的な契約条件や提供されるべきサービスについての記述などが盛り込まれた，所定の汎用的な様式が契約には利用されている。評価は行われているが，的外れであり適切ではない。報告は行われているが，経営目標の達成に役立つものではない。

3：定められたプロセスがある

サードパーティからの調達の管理についてきちんと文書化された手続がある。手続にはベンダの適格性調査やベンダとの交渉を必ず適切に行うように明確な手順が定められている。サードパーティとの関係は，純粋に契約に基づくものである。提供されるサービスの性質は，契約で詳述されており，運用上，法律上そしてコントロール上の要求事項に言及されている。サードパーティのサービス提供を監督する責任者が任命されている。契約条項は，標準テンプレートに基づいている。契約に関連したビジネスリスクは評価され，報告される。

4：管理，測定されている

仕事の範囲，提供されるサービス，成果物，前提条件，予定時間，コスト，請求処理，実行責任，ビジネス条件などを確定するために，正式な標準規準が定められている。契約行為とベンダ管理を行う責任者は任命される。ベンダの適格性や能力を検証している。要求事項は明確にされ，経営目標にリンクしている。サービスの成果は契約条項に照らしてレビューされており，この情報は現在や将来のサードパーティの利用に役立てられる。サービス調達には移転価格モデルが使われる。すべての利害関係者は，サービス，コスト，マイルストーンの期待水準を周知している。

5：最適化

お互いにサインした契約書を，サービスの開始以後も定期的にレビューしている。サービス提供やベンダサポートに関する品質保証の責任者が任命されている。契約条項を遵守しているかどうかは運用上，法律上，コントロール上の観点からモニタリングされ，改善対応が取られる。サードパーティは，独立した第三者によるレビューを定期的に受けることを条件付けられている。レビューの結果はフィードバックされる。ビジネス状況の変化に応じて，評価尺度もダイナミックに変っている。評価することで，問題を早期発見することができる。サービスレベルに関する報告は分かりやすく明瞭であり，サードパーティへの報酬にリンクしている。報告制度があることで，潜在的な問題に対し早期に警告がなされ，タイムリに問題解決することができる。

DS3：成果と能力(キャパシティ)の管理

十分な能力(キャパシティ)が利用可能であり，求められる成果を満たすように最善，最適な利用を行うことをビジネス目標としている IT プロセスの**成果と能力(キャパシティ)の管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**情報システム資源の成果，アプリケーションのサイジングおよび作業負荷需要に関するデータを収集，分析，報告することによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
S	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 重要なビジネスプロセスすべてについて，IT サービスの提供に必要な成果と能力(キャパシティ)が明確に理解されている。
- すべての IT 開発・保守のプロジェクトで，成果要件が明示されていること
- システムの調達と開発におけるすべての適切な段階で，成果と能力の問題が取り扱われていること
- 技術インフラを定期的にレビューし，コスト成果を向上させ，最小コストで最大の成果を発揮するような資源の調達活動を可能にしていること
- 現在と将来の能力を分析するために，利用できるスキルやツールがあること
- 利用者や IT 管理者は，現状および計画中の能力やその使用状況を，理解しやすく使いやすい形で利用できること

重要目標達成指標(KGI)　*4

- 対利用者ビジネスプロセスのうち，IT の能力や成果が不適切であったことが原因で，中断や供給停止にあった数

- 主要ビジネスプロセスのうち，サービス可用性計画(service availability plan)の対象に含まれていないものの数
- 主要 IT 資源のうち，ピーク時の負荷から見ても，成果と能力が適切であるものの割合

重要成果達成指標(KPI)　*5

- 能力や処理成果が不十分であることに起因する，ダウン事故の件数
- (負荷の)通常時やピーク時に余っている能力の割合
- 能力問題の解決に要した時間
- 全アップグレード数に占める，計画外のアップグレード件数の割合
- 需要の変動に応じて能力調整を行った頻度

DS3 成熟度モデル

十分な能力(キャパシティ)が利用可能であり，求められる成果を満たすように最有効利用することをビジネス目標としているITプロセスの**成果と能力(キャパシティ)の管理**におけるコントロール

0：不在

経営者は，主要ビジネスプロセスが高水準の IT 成果を必要とすることを認識していない。また IT サービスに対する全社的なビジネスニーズを実現させるには能力が足りないことも認識していない。能力計画はない。

1：初期／その場対応

成果と能力の管理は事後対応的で，時々散見される程度である。利用者は成果や能力の制約があるために，しばしば代替的解決策を工夫しなければならない。ビジネスプロセスのオーナは，IT サービスの恩恵を受けていることをほとんど理解していない。IT 管理者は，成果と能力を管理する必要性に気づいているが，対応は通常事後的であるか，不完全である。計画プロセスは正式なものでない。

2：再現性はあるが，直感的

ビジネスの管理者は，成果や能力を管理しない悪影響に気づいている。一般的に重要性の高い範囲については，成果・ニーズを満たすようにまかなわれているが，これは個別的なシステム評価やサポートチームやプロジェクト・チームに蓄積された知識に基づいて対応しているにすぎない。成果や能力の問題を診断するために使われている個別のツールもあるが，結果が一貫しているかどうかは主要な要員のノウハウに依存する。IT インフラの成果能力について，全社的な査定は行われていない。ピーク時や最悪時の負荷状況も検討されていない。可用性に関する問題は，予期せぬときにランダムに起きやすく，さらに診断して，改善するために相当の時間を要する。

3：定められたプロセスがある

システム調達と開発の全過程で，成果と能力の要件は，考慮される。サービスの要求レベルは定められ，成果評価のための評価尺度もある。将来的な成果要件もモデルを利

用して予測することができる。成果統計を示す報告書が生成されている。問題はいまだ発生しやすく，改善には時間が掛かる可能性が高い。サービスレベルが公表されているにもかかわらず，エンドユーザは時々サービス提供能力に対して疑問を抱いている。

4：管理，測定されている

システムの使用状況を測定して，決められたサービスレベルと比較するために，利用できるプロセスとツールがある。最新情報が利用可能で，成果統計の標準レポートを提供し，能力不足や処理能力不足といった不具合に警告を出している。成果や能力の不足を原因とする障害は，標準手続に従って対応される。ディスク記憶装置，ネットワークサーバ，ネットワークゲートウェイといった特定資源をモニタするために自動化ツールが用いられる。成果統計をビジネス用語で報告する試みもある。これによってエンドユーザが IT のサービスレベルを理解することができる。利用者は現在のサービス提供能力におおむね満足しているが，より高いレベルを要求しているところである。

5：最適化

成果や能力の計画は，ビジネスの予測，ビジネス計画やその目的と，完全に同期が取られている。最小コストで最適能力を確実に実現するために，IT のインフラは定期的なレビューを受けていることを条件としている。より向上したプロダクト成果を取り入れることができるように，技術の進歩について注意深く情報収集している。IT 成果測定に使う評価尺度は重要領域に焦点が当たるように十分に調整されており，またすべての主要ビジネスプロセスにおける KGI，KPI と CFS へと置き換えられている。主要 IT 資源をモニタリングする標準化されたツールがあり，可能な限りプラットフォームの別を問わず，全社的な障害管理システムにリンクさせている。モニタリングツールは成果に問題が発生すると検知して自動的に修正するまでに進化している。例えば，記憶装置空間の配分を増大させたり，ネットワークトラフィックの経路を指定し直したりする。ビジネスボリュームの増大によって成果上の差し迫った問題が起こりそうな兆候があれば検知され，不測の障害に対する計画と回避策を立てることができる。利用者は，「1 日 24 時間週 7 日年 365 日」のいつでも利用できることを期待している。

DS4：継続的なサービスの保証

IT サービスが必要な時に利用でき，大きな中断があってもビジネスへの影響を最小限に押さえることをビジネス目標としている IT プロセスの**継続的なサービスの保証**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**実効的な，テスト済みで，かつ，全社的な事業継続計画およびその関連するビジネス要件と整合している IT 継続計画を策定することによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
P	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 無停電電力設備が備えられ，定期的にテストされていること
- 発生可能性のある潜在的なリスクが事前に検知され，対処されること
- 重要なインフラの構成要素を明らかにし，継続してモニタリングされること
- 継続的にサービスを提供するためには，優れた能力(キャパシティ)プランニングの立案，可用性の高い設備機器の調達，代替設備(冗長性)の確保，事前にテストされたサービス継続計画の存在，多重化していないことによる共倒れ事故の回避といった一連の体制が必要であること
- 実際に発生したダウン障害やサービス継続計画のテスト結果を通して得た教訓に基づいて対応が取られること
- 可用性の要求事項について，分析が定期的に行われること
- SLA(サービスレベルアグリーメント)を通じて，事業継続に対するサプライヤの意識を高め，サプライヤとの協働関係を高めること
- 報告／報告のプロセスが明確に理解されており，また可用性の事故における重要性の分類に応じた報告がなされること
- サービス中断によるコストをできる限り把握し定量化し，緊急設備の計画の適切な策

定や手配のきっかけ(誘因)になっていること

重要目標達成指標(KGI)　*4

- 社会的信頼の失墜を招くような事故が発生していないこと
- IT に依拠している主要ビジネスプロセスのうち，適切なサービス継続計画のあるものの数
- 事業継続計画が実行的であることの定期的かつ正式な証明
- ダウン時間の低減
- 重要なインフラ構成要素(コンポーネント)のうち，可用性を自動モニタリングする機能を持ったものの数

重要成果達成指標(KPI)　*5

- サービス継続に関する未解決の問題のうち，いまだに解決または対処されていないものの件数
- 障害継続時間とその影響度を規準として評価した，サービス継続障害の数と影響範囲
- 組織が変更されてから，サービス継続計画が改訂されるまでの間のタイムラグ
- 障害を診断し，サービス継続計画の実行を決定するまでに要する時間
- サービス継続計画を実行した後，サービスレベルを正常化させるまでに要する時間
- 障害が起きる前に可用性を改善した数
- サービス継続が短時間ストップしたときに，それを処理するまでのリードタイム
- サービス継続に関する研修の実施頻度
- サービス継続に関するテストの実施頻度

DS4 成熟度モデル

IT サービスが必要な時に利用でき，大きな中断があってもビジネスへの影響を最小限に押さえることをビジネス目標としている IT プロセスの**継続的なサービスの保証**におけるコントロール

0：不在

IT 運用上のリスク，脆弱性，脅威や，IT サービスを提供できなくなった場合のビジネスへの影響を理解していない。サービス継続が経営上の要注目課題であるとみなしていない。

1：初期／その場対応

サービス継続の実行責任者は正式に任命されたわけではなく，限定された権限しか付与されていない。経営者は，継続的にサービス提供できなくなるリスクやサービス継続の必要性を認識し始めているものの，ビジネス機能よりはむしろ IT 機能に重点を置いている。利用者は抜本的な問題解決がなされないため，代替的方法で対応している状況である。大きな中断に対する対応は事後対応的であり，準備対策がなされていない。電源装置の定期点検のための停電の計画は，ビジネス上の必要性より，IT のニーズを優先

するようにスケジュールが組まれている。

2：再現性はあるが，直感的

サービス継続の実行責任者が任命されている。継続的なサービス提供への取組みはバラバラと断片的で体系的ではない。システムの可用性についての報告書は，不完全であり，ビジネスに与える影響を考慮に入れていない。サービス継続の可用性の検討に利用者は参加しており，主な原則は周知されているが，文書化された事業継続計画や利用者向けの計画は存在しない。主要システムとその構成要素について，十分信頼できる棚卸リストがある。サービス継続手順は標準化されつつあり，プロセスのモニタリングが始められている。しかしその良否は個人のノウハウに依存している。

3：定められたプロセスがある

説明責任ははっきりと明確になっており，サービス継続計画とテストの実行責任者も明確に任命されている。計画は文書化され，システムの重要性とビジネスへの影響を基準に作成されている。サービス継続計画のテスト結果は定期的に報告される。各個人は，標準に準拠するように取り組むとともに，訓練を受けている。経営者はサービス継続の必要性を一貫して周知している。だんだんと可用性の高い構成要素を使い始め，システムに冗長性が高まっている。重要なシステムとその構成要素(コンポーネント)の棚卸リストを厳密にきっちりと維持している。

4：管理，測定されている

サービス継続に関する実行責任が明確化され，標準が制度化されている。サービス継続計画を維持する実行責任者も任命されている。計画の維持には，ビジネス環境の変化や，サービス継続テストの結果や，社内のベストプラクティスなどを考慮に入れている。サービス継続に関するデータは体系化され，収集，分析，報告されて，対応に役立てられている。サービス継続に関する研修が行われている。可用性の高い構成要素を使うことを含めて，システムの冗長性が一貫して高められている。システムの冗長性とサービス継続計画とは，相互に関連している。サービス継続を損なう事故は分類分けされ，関係者には報告手続が周知されている。

5：最適化

サービス継続プロセスは統合化されており，事前対応的である。また，自動化されており，自動調整や自己分析ができるようになっている。またベンチマーキングや社外のベストプラクティスを考慮に入れている。サービス継続計画と事業継続計画は統合されて，整合性が取られ，定期的に保守される。購入したものに対するサービスの継続については，ベンダや主なサプライヤが保証している。広域的なテストを実施し，テスト結果は保守プロセスの一部としてフィードバックされる。サービス継続の費用効率は，技術革新や統合化によって最適化されている。データを収集，分析して改善機会をとらえるために用いている。冗長性とサービス継続計画は，完全に関連している。経営者は，多重化していないことによる共倒れ事故を認めておらず，その改善対応を進めている。報告手続は理解され，完全に遵守されている。

DS5：システムセキュリティの保証

無許可の情報の使用，開示または改ざん，あるいは損害や喪失などから情報を保護することをビジネス目標としているITプロセスの**システムセキュリティの保証**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**システム，データおよびプログラムへのアクセスが，承認されている者だけに制限されることを保証する論理的アクセス管理によって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
	有効性
	効率性
P	機密性
P	万全性
S	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*4

- 全般的なセキュリティ計画が策定されている。その計画では，セキュリティ意識を喚起し，明確な方針と標準を設定し，費用効率のよい継続的に実行可能な導入を明らかにし，モニタリングと遵守を強制するためのプロセスが定められる。
- セキュリティ計画をレベルアップするには時間が掛かることが理解されている。
- 企業のセキュリティ担当部門は，上級管理者への報告責任とともに，セキュリティ計画を実行に移す責任を負っている。
- マネジメントとスタッフはセキュリティ要件，組織の脆弱性，脅威に関する共通の理解を持っている。さらに自らのセキュリティ遵守責任を理解している。
- セキュリティ方針とその体制について，サードパーティによる評価が定期的に行われる。
- 最低限実行すべきセキュリティの遵守事項が明らかになっている。
- いわゆる「運転免許」制度が設けられ，システムの開発，導入，運用に従事するスタッフに対して”セキュリティ認定“を行っている。
- セキュリティ違反行為について，それを検知，記録，重要性の分析，事故報告，対応

するために必要な能力と手段が，セキュリティ担当部門にある。一方で，侵入テストや常時モニタリングを行って事故発生の危険性を最小限にする。

- 利用者管理のプロセスとシステムを集中管理することで，標準的・効率的な方法で利用者へ権限付与することができる。
- 合理的なコストの，導入が容易で使いやすい，利用者認証のプロセスが整備されている。

重要目標達成指標(KGI)　*2

- 社会的信頼の失墜を招くような事故が発生していないこと
- 重大な事故は速やかに報告されること
- アクセス権は職務と整合していること
- セキュリティ上の懸案事項によって延期となった新規導入案件の数の低減
- 最低限のセキュリティ要件については完全に守られていること。または，要件からの乖離については承認され記録されていること
- 未承認のアクセスや，情報の喪失または改ざんが発生した事故数の低減

重要成果達成指標(KPI)　*5

- セキュリティ関係のサービスコールの回数，変更要求の回数，修復の回数の低減
- セキュリティ事故に起因するダウンの合計時間
- セキュリティ管理の要求ジョブの提出から出力返送までのターンアラウンドタイムの短縮
- 侵入検知プロセスのあるシステムの数
- アクティブ・モニタリング機能のあるシステムの数
- セキュリティ事故の調査時間の短縮
- セキュリティ事故の発見，報告，対応までのタイムラグ
- IT セキュリティ意識をテーマとした研修の日数

DS5 成熟度モデル

無許可の情報の使用，開示または改ざん，あるいは損害や喪失などから情報を保護することをビジネス目標としている IT プロセスの**システムセキュリティの保証**におけるコントロール

0：不在

組織は IT セキュリティの必要性を認識していない。セキュリティについて，実行責任者と説明責任者が任命されていない。IT セキュリティ管理を支援する評価尺度がない。IT セキュリティに関する報告体制がなく，IT セキュリティ違反に対処するプロセスがない。システムセキュリティの管理は全くない。

1：初期／その場対応

組織は，IT セキュリティの必要性を認識しているが，セキュリティに対する意識は各人によってまちまちである。IT セキュリティは，事後対応的に対処され，評価もされていない。もしセキュリティ違反が検出されると，実行責任が明確になっていないので，いわゆる「非難し合うこと(責任のなすり合い)」だけに終始する。IT セキュリティ違反

への対応についての準備がされていない。

2：再現性はあるが，直感的

IT セキュリティのための実行責任と説明責任が，IT セキュリティ・コーディネータに割り当てられているが，管理権限までは与えられていない。セキュリティに対する意識はまばらで断片的かつ限定的である。IT セキュリティに関する情報が生成されているが，分析は行われていない。固有のニーズを把握することなく，サードパーティの提案を鵜呑みにしているため，IT セキュリティ事故への対応は，後手に回りがちである。セキュリティ方針が策定されているものの，十分とはいえないスキルとツールがなお使われている。IT セキュリティの報告体制は不完全で，誤解を招きやすく，適切ではない。

3：定められたプロセスがある

セキュリティに対する認識があり，また経営者によって注意喚起されている。セキュリティ意識を喚起するための従業員に対する説明会は標準化されており，正式なものとなっている。IT セキュリティ手続が定められており，セキュリティ方針や手続体系と整合性が取れている。IT セキュリティの実行責任は割り当てられているが，一貫して強制実行されるわけではない。IT セキュリティ計画があり，リスク分析やセキュリティ対応策を推進している。IT セキュリティのに関する報告は，ビジネスよりもむしろ，IT に重点をおいている。侵入テストは場当たり的に行われている。

4：管理，測定されている

IT セキュリティの実行責任が明確に割り当てられて，管理され，そのとおり運用(強制 or 制度化)されている。IT セキュリティ上のリスクと影響度の分析が一貫して行われる。セキュリティの方針と手続は整備されており，最低限の遵守事項が定められている。職員に対するセキュリティ説明会は必須になってきている。利用者識別，認証，権限付与手続は標準化されている。スタッフに対する“セキュリティ認定”が確立されている。改善のため，正式な標準プロセスとして侵入テストが行われている。費用対効果分析が一層活用され，セキュリティ評価に役立てられている。IT セキュリティプロセスは全社的なセキュリティ体制と整合性が取れている。IT セキュリティの報告体制は経営目標とリンクしている。

5：最適化

IT セキュリティは，ビジネスと IT 両管理者の連帯責任となっており，企業の経営目標と統合されている。 IT セキュリティ要件は明確にされ，最適化されており，テスト済みのセキュリティ計画に織り込まれている。セキュリティ機能は，設計段階でアプリケーションに組み込まれ，また利用者はセキュリティの管理についてより責任を負うようになっている。重要なシステムについては，自動化された常時モニタリングアプローチを活用して，IT セキュリティの報告によって，リスクの変化と発生に対して早期警告を発する。事故は，自動化されたツールで支援された正式な事故対応手続によって直ちに処理される。セキュリティ計画導入の有効性について定期的に評価している。新たな脅威や脆弱性についての情報は，システマティックに収集され，分析され，リスクを軽減するために，速やかに適切なコントロールが導入される。侵入テスト，セキュリティ事故の原因分析，事前対応的なリスクの把握がなされ，継続的な改善の基礎となっている。セキュリティ手続とテクノロジは，全社的に統合されている。

DS6：コストの捕捉と配賦

IT サービスに掛かる費用を正しく認識することをビジネス目標としている IT プロセスの**コストの捕捉と配賦**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**費用を記録・計算し，提供したサービスに対して適切かつ必要とされる詳細レベルで配賦計算する原価計算システムによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
	有効性
P	効率性
	機密性
	万全性
	可用性
	準拠性
P	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- エンドユーザ，ビジネスプロセス責任者，IT 部門の三者は，原価計算の要件と費用配賦に関して共通の理解をしている。
- 直接費と間接費の識別，捕捉，記録，分析がタイムリに自動的に行われる。
- 費用はサービス利用実績に応じて内部請求され，費用配賦の原則に従って記録される。費用配賦の原則は正式に認められたものであり，定期的に再評価される。
- 予算の成果のレビューやコスト最適化のための機会の探索，成果の信頼できるデータに対比させたベンチマーキングを行うために，原価報告を関係者全員が利用している。
- サービスの費用と SLA(サービスレベルアグリーメント)とは直接リンクしている。
- 費用配賦と最適化の結果は，効果の実効性(実現率)の検証に利用されるとともに，次年度予算へフィードバックされる。

重要目標達成指標(KGI)　*4

- IT 部門の情報サービスコストの継続的最適化度合
- 利用者の情報サービスコストの継続的最適化度合
- IT サービスの実際費用に対し明らかにできる便益向上比率

- 外注，内作した場合の費用と比較した効率性指標
- IT に掛かる費用とサービスの水準に関して，ビジネス管理者が理解し認容しているレベル

重要成果達成指標(KPI)　*5

- 実績対予算(または予測)差異の割合
- 情報サービス料の値下げの割合
- 利用者からのサービス依頼を最も効果的に実現した件数の増加割合
- IT 資源の最有効活用が増加した割合
- コストの最効率化の取組みの数

DS6 成熟度モデル

IT サービスに掛かる費用を正しく認識することをビジネス目標としている IT プロセスの**コストの捕捉と配賦**におけるコントロール

0：不在

情報サービスの費用を捕捉，配賦するプロセスは全くない。原価計算に関して対処すべき問題があるという認識がなく，その問題を周知させることもしていない。

1：初期／その場対応

情報サービスにかかる費用全体に関する一般的な理解はある。しかし利用者ごと，部門ごと，利用者グループごと，サービス機能ごと，プロジェクトごとあるいは成果物ごとなどにどの程度の費用が掛かっているか詳細を把握してはいない。費用の総計が経営者に報告されるだけで，事実上費用のモニタリングはしていない。情報サービスの提供に掛かる費用を利用者に請求するための内部請求プロセスや仕組みはない。

2：再現性はあるが，直感的

費用を捕捉し，配賦する必要性についての全般的な意識はある。インフォーマルで原始的な仮定(例えば，ハードウェアは高いものだ等)に基づき費用が配賦される。これは，IT サービス提供がもたらす付加価値要因(value drivers)とは関連のない配賦である。費用配賦プロセスはある程度定着してきており，モニタリングを始めたプロセスもある。標準原価の設定と配賦の手続に関して，正式な研修はなく周知もされていない。実行責任は割り当てられていない。

3：定められたプロセスがある

情報サービスのコストモデルが定められ，文書化されている。コストモデルは制度化され周知されており，インフォーマルだが研修が実施されている。情報サービスの提供に掛かる費用について適切に認識されている。自動化された原価計算システムはあるものの，ビジネスプロセスよりは，情報サービスの機能に重点が置かれている。

4：管理，測定されている

情報サービスの原価管理についての実行責任と説明責任が定められ，すべての階層で十分に理解されている。また，原価管理の正式な研修も行われている。直接費と間接費はタイムリに自動捕捉され，マネジメント，ビジネスプロセス責任者，利用者に報告される。たいていの場合，原価はモニタリングされ，評価されており，プロセスが効果的，効率的に機能していない場合には対応がとられる。多くの場合対応がとられるが，すべてというわけではない。原価管理プロセスは継続的に改善され，社内のベストプラクティスが推進強化されている。情報サービスの原価報告は，経営目標やSLA(サービスレベルアグリーメント)にリンクしている。社内の原価管理関係者全員が責任関与している。

5：最適化

提供されたサービスに掛かった費用は認識，捕捉，要約されて，経営者，ビジネスプロセス責任者，利用者の三者に報告される。費用は請求可能項目となっており，サービスの利用実績に基づいて，利用者部門へ適切に請求する，内部請求システムに支えている。内部請求システムでは，原価明細が，SLA(サービスレベルアグリーメント)を支える。サービスの費用はしっかりとモニタリングされ，評価される。予算実績差異額を把握され，差異を分析し，分析結果に基づいて対応がとられる。原価数値を用いてサービスの効果が検証され，予算編成プロセスに活用される。インテリジェント報告システムを通して，情報サービスの原価報告がビジネス要件の変更に対し早期警告を発する。提供されたサービス量に応じて，変動費が計算されるようなコストモデルを使用している。継続的に改善し，他社の成熟度モデルの参照などを行ってきた結果，原価管理はベストプラクティスのレベルにまで高められている。社外の専門家の意見を取り入れ，原価管理のガイドラインとしてベンチマーキングも行っている。

DS7：利用者の教育と研修

利用者がテクノロジを効果的に利用し，関連するリスクや責任を認識することをビジネス目標としているITプロセスの**利用者の教育と研修**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**包括的な研修計画や研修開発計画によって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
S	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 包括的な教育研修プログラムがあり，個人や企業のニーズに重点を置いたものであること
- 教育研修プログラムは，予算面，資源面，設備面および講師面で支援されていること
- 研修と教育は従業員のキャリア形成のための重要な要素となっていること
- 従業員と経営者は，研修のニーズを把握し，文書化していること
- 必要な研修がタイムリに行われていること
- 従業員が，倫理的かつ安全な方法で職務遂行するように上級管理者が支援していること
- すべての従業員は，セキュリティ実務の研修を受ける。その研修では，可用性，機密性，万全性(インテグリティ)に影響を与える障害を受けることのないようにシステムを保全することを学ぶこと
- 企業方針として，全従業員に基礎的な研修の受講を義務付けていること。この研修は倫理行動規範，システムセキュリティ実務，IT資源の使用の許可範囲などを扱っている。
- 研修費用はテクノロジ所有に要する総費用(TCO)を削減する効果を持つ投資であることを，経営者が理解している。

重要目標達成指標(KGI) *4

- 企業価値を最大化するための IT 担当者を最適化について，改善された点
- 倫理行動要件に関する従業員の意識，システムセキュリティ原則，及び倫理的で安全な職務遂行の三点に関して改善された点
- 可用性，機密性，万全性(インテグリティ)に影響を与える障害を受けることのないようにシステムを保全するために，セキュリティ実務を改善した点
- 研修や問合せのため，ヘルプデスクにかけられた電話件数
- 導入した新テクノロジに対するユーザ満足度の増加割合

重要成果達成指標(KPI) *5

- 研修を受けた従業員の割合
- 従業員の研修カリキュラムの古さ
- 研修ニーズを把握してから実施されるまでのタイムラグ
- 従業員が選択可能な社内・社外の研修の数
- 倫理行動要件の教育を受けた従業員の割合
- 従業員による倫理違反行為の発生件数
- セキュリティ実務の研修を受けた従業員の割合
- 従業員が関係したセキュリティ違反事故の数
- 研修ニーズを把握・文書化して，タイムリに研修を行った件数の増加

DS7 成熟度モデル

利用者がテクノロジを効果的に利用し，関連するリスクや責任を認識することをビジネス目標としている IT プロセスの**利用者の教育と研修**におけるコントロール

0：不在

教育研修のプログラムは一切ない。研修に関して対処すべき課題があることを組織は認識しておらず，課題についても周知されていない。

1：初期／その場対応

研修と教育プログラムの必要性を認識しているが，標準化されたプロセスはない。体系的なプログラムがないため，従業員は自ら研修コースを選択して，参加している。この中には，倫理行動規範や，セキュリティ意識や，セキュリティ実務をテーマとしたものもある。全般的に管理手法としてはまとまりがなく，教育上の課題やアプローチについては，散発的で一貫性のないコミュニケーションが行われている。

2：再現性はあるが，直感的

全社的に，教育研修プログラムが必要であり，関連プロセスが必要であるという意識はある。従業員の業績計画の過程で研修(の必要性)が認識され始めている。教育プロセスが見られる段階に至っているが，非公式にさまざまなインストラクターが，同一のテーマに対して異なるアプローチで教育研修を担当している。倫理行動規範，セキュリティ意識やセキュリティ実務をテーマにしているクラスもある。いまだ，個人の知識レベ

ルへの依存度が高い。ただ全社的な課題や，それに対処する必要性に関して一貫したコミュニケーションはある。

3：定められたプロセスがある

教育研修プログラムは制度化され，周知されている。従業員や管理者は研修・ニーズを把握し文書化している。教育研修プロセスは標準化され，文書化されている。教育研修プログラムを支援するために，予算，資源，設備や講師が用意されている。倫理行動規範，セキュリティ意識，セキュリティ実務などについて正式なクラスが，従業員のために用意されている。多くの教育研修プロセスはモニタリングされているが，すべての課題点が管理者によって発見されるわけではない。教育研修上の問題分析は，時々しか行われない。

4：管理，測定されている

包括的な教育研修プログラムがあり，個人や企業のニーズに焦点が当てられている。研修の成果を評価する仕組みもある。実行責任は明確で，プロセスオーナーシップが確立している。教育研修は従業員キャリア形成の一要素である。マネジメントは，教育研修の開催を支援し，参加している。すべての従業員が，倫理行動規範とセキュリティ意識の研修を受けている。また，可用性，機密性，万全性(インテグリティ)に影響を与える障害を受けることのないように保全するため，セキュリティ実務の研修を受ける。継続的に教育研修のプログラムとプロセスをレビューし改善し，経営者は遵守状況をモニタリングしている。プロセスは改善が進んでおり，社内のベストプラクティスを推進している。

5：最適化

教育研修の結果，個人の成果向上につながっている。教育研修は，従業員のキャリア形成にとって極めて重要な構成要素である。十分な予算，資源，設備と講師が教育研修プログラムのために用意されている。社外のベストプラクティスを活用するとともに，成熟度モデルを利用し他社比較を行うことによって，プロセスはますます洗練されてきており，現在も継続的に改善されている。すべての問題と逸脱行為は原因を分析され，タイムリに効果的な対応策を明らかにし，対処する。倫理行動規範とシステムセキュリティの原則に関して前向きな教育研修プログラムのツールを自動化して提供するために，広範に統合化され，最適な方法で IT が利用されている。社外の研修専門家の活用が進み，ベンチマークがガイドとして使われる。

DS8：利用者に対する支援と助言

利用者が直面するすべての問題が適切に解決されることをビジネス目標としているITプロセスの**利用者に対する支援と助言**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**第一線で支援と助言を行うヘルプデスク機能によって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
	テクノロジ
	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- ＦＡＱ(頻繁に出される質問)とその解答のデータベースが，常に更新されており，簡単にアクセスできること
- 支援スタッフは知識が豊かで利用者指向であり，問題管理担当者と緊密に協働して問題解決に取り組むこと
- 利用者からのすべての問合せを，ヘルプデスクが一貫してすべて記録していること
- すぐに解決できなかった利用者からの問合せは，適切に報告されていること
- 利用者からの問合せが解決されリストから外れていっているか，モニタリングしていること
- 利用者からの問合せは迅速に解決すること
- 解決に時間が掛かっている利用者からの問合せについて，調査の上，対処していること
- 経営者は傾向をモニタリングし，事前対応的に原因を見極めること。分析によって継続して適用できる解決策を見つけることで事後対応すること
- テクノロジの使い方とセキュリティ実務に関する利用者の研修について，企業方針とプログラムが定められていること
- 経営者は支援サービスのコストとシステムダウンに伴う利用者コストを認識していること。また，根本的な原因に対処する必要性についても認識していること

- 支援コストは，簡単なツールと明確な方針によって，ビジネス部門に内部請求されること

重要目標達成指標(KGI)　*4

- 問題解決に要する平均時間の短縮
- 解決済みの問題に対して，同じ質問が繰り返される回数の減少
- ヘルプデスクや効率性や効果に対する利用者満足度の向上
- ヘルプデスクのサービスに対する利用者信頼度の向上
- システムの支援に関連したヘルプデスク資源の削減によって評価される効率性の改善
- 一回の電話対応で解決された問題の割合
- 1 コール当たりの通話時間

重要成果達成指標(KPI)　*5

- 繰り返し質問される問合せの数
- (その場では解決がつかずに専門スタッフやマネージャに)報告した数
- 問合せの件数
- 問合せを解決するまでに要した時間
- 問題解決を要する利用者問合せ数の減少
- 問合わせ 1 回当たりの費用

DS8 成熟度モデル

利用者が直面するすべての問題が適切に解決されることをビジネス目標としている IT プロセスの**利用者に対する支援と助言**におけるコントロール

0：不在

利用者からの問合せや問題の解決を手助けする手段がない。ヘルプデスク機能は全くない。対処すべき問題があることを組織は認識していない。

1：初期／その場対応

利用者の問合せに対応し，問題解決を管理することを目的とした，ツールとスタッフの手当てをされたプロセスが必要であることを認識している。しかし，標準化されたプロセスはなく，事後的に対応されるだけである。管理者は利用者の問合せ，問題やその傾向をモニタリングしていない。問題が確実に解決されることを保証する報告手続がない。

2：再現性はあるが，直感的

ヘルプデスク機能が必要であるという認識が組織にある。知識の豊富な個人とのネットワークを通して，インフォーマルな形で支援を受けることができるようになっている。このような個人は，問題解決の支援に使える共通のツールを利用している。正式な研修はなく，標準手続は周知されておらず，また実行責任は個人に委ねられている。しかし，

全社的な問題とそれに対処する必要性については，一貫して周知されている。

3：定められたプロセスがある

ヘルプデスクの必要性は認識され受け入れられている。手続は標準化，文書化され，インフォーマルに研修が行われ始めている。しかし，研修を受け，標準を遵守するかどうかは各人の裁量に委ねられている。ＦＡＱ(頻繁に出される質問)や利用者ガイドラインが策定されてはいるが，各人はそれがどこにあるのか自分で探し出さなければならないし，必ずそれに従うというわけでもない。問合せや問題は，手作業でフォローされ，個々にモニタリングされている。しかし，正式な報告制度はない。ようやく問題が報告されるようになったところである。問合せや問題に対して迅速な対応がされているかどうかは評価されていないので，問題は未解決のままになっているかもしれない。

4：管理，測定されている

組織のすべてのレベルでヘルプデスクの効果は十分に理解されており，ヘルプデスク機能を担う部門が設けられている。ツールと技術は問題と解決策についての統合知識ベース(Knowledge base)として自動化されている。ヘルプデスクスタッフと問題管理スタッフとは緊密に連係している。実行責任は明確であり，ヘルプデスクが有効に機能しているかどうかはモニタリングされている。コミュニケーション，上司への例外報告，問題解決のための手続が確立されて，周知されている。ヘルプデスク要員は研修され，タスク専用(task-specific)のソフトウェアを通してそのプロセスは改善されている。問題の原因が特定され，そのトレンドが報告されて，問題をタイムリに修正する結果に結びついている。プロセスの改善は進行中であり，社内のベストプラクティスが制度化されている。

5：最適化

ヘルプデスク機能は確立し，うまく組織化されている。十分な知識を装備し，利用者の立場を中心に考え，役立つサービス提供することによって，利用者サービス指向を実現している。広範で，包括的な「FAQ」は，知識ベース(Knowledge base)にとって不可欠なものである。ツールが整備され，利用者が問題を自分で診断して，自ら解決することができるようになっている。問題解決を支援する自動知識ベースへのアクセスを作成・管理・改善するために IT が利用されている。アドバイスは一貫しており，体系化された報告プロセスによって，問題は迅速に解決される。経営者は，事前対応的な通知プロセスや傾向分析を活用しており，問題を未然防止するために傾向をモニタリングしている。継続的な改善活動と成熟度モデルを利用した他社比較の結果，プロセスは社外のベストプラクティスのレベルにまで洗練されてきている。

DS9：構成管理

すべての IT 構成(コンフィギュレーション)に責任を持ち，無許可の変更を防止し，物理的な存在を確認し，健全な変更管理のための基礎を提供することをビジネス目標としている IT プロセスの**構成管理**におけるコントロールは

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**内部統制が整備されすべての IT 資産とその設置場所が認識・記録されており，定期的に棚卸を行うことによって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
	効率性
	機密性
	万全性
S	可用性
	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
✔	アプリケーション
✔	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- すべての構成に対して所有責任者が決められており，その所有責任者が棚卸リストの保守や変更管理に責任を持っていること
- 最新の棚卸リストと包括的な命名規則によって，構成に関する情報は保守され，アクセス可能となっていること
- 開発，テストおよび本番の各環境のニーズに対処した，ソフトウェアライブラリ構造が適切に整備されていること
- リリース管理の方針があり，それを強制するシステムになっていること
- 記録と物の保管の職務は分離されていること
- 購買調達プロセスと変更管理プロセスとは整合性が取れていること
- ベンダカタログと構成は整合性が取れていること
- 構成の基底線(baseline)があり，その中には最小限必要な標準構成，統合化要件，一貫性や統合規準などが明らかになっていること
- 構成上の不整合の自動検知やチェックのメカニズムが利用できること
- 自動分散制御(distribution)とアップグレードのプロセスが導入されていること
- 違法ソフトウェアは一切許容しないこと

重要目標達成指標(KGI) *4

- IT 構成のうち，特定され責任が明確にされているものの割合
- 会計記録と棚卸結果(実際の場所)との差異の縮小割合
- 相互関係，年数，変更履歴，状態，関連する問題の判断規準などを含む，情報の品質指標
- 予防保全やアップグレード判断規準を含む，事前対応に役立つ情報の利用指標

重要成果達成指標(KPI) *5

- 構成に関するデータが自動的に保存，更新されている構成の割合
- 実地棚卸の頻度
- 構成の冗長性や，構成の陳腐化とその修正などを対象にした例外事項分析の頻度
- 構成を修正してから記録を更新するまでの間のタイムラグ
- リリース件数
- 元に戻さざるを得なかった変更の割合

DS9 成熟度モデル

すべての IT 構成に責任を持ち，無許可の変更を防止し，物理的な存在を確認し，健全な変更管理のための基礎を提供することをビジネス目標としている IT プロセス**構成管理**におけるコントロール

0：不在

経営者は，ハードウェアとソフトウェア構成両方の IT インフラについて報告し，管理するプロセスを整備することの効果について理解していない。

1：初期／その場対応

構成管理の必要性は認識されている。ハードウェアとソフトウェアの棚卸リストを保守するといった基本的な構成管理タスクが，個人ベースで行われている。標準的な手続はない。

2：再現性はあるが，直感的

経営者は IT 構成をコントロールすることの効果について気がついているが，暗黙裡に技術要員の専門知識と専門技術に依存している状態である。構成管理ツールはある程度利用されているが，プラットフォーム間で異なる。さらに，標準的な手続は定められていない。構成に関するデータは内容が限定的なため，変更管理や問題管理のような相互に関連する複数のプロセスで活用されていない。

3：定められたプロセスがある

構成に関する情報が正確で完全であることの必要性は理解され，実施されている。手続は文書化され，標準化されて，周知されている。しかし標準手続についての研修を受講するかどうかやそれを適用するかどうかは個人の判断に委ねられている。似通った構

成管理ツールがいろいろなプラットフォームで導入されるようになっている。標準手続から乖離しても検知されることは少なく，物理的な検証も一貫した方法では行われないことが多い。若干の自動化が行われ，装置やソフトウェア変更の証跡をたどることができる。構成に関するデータは相互に関係する複数のプロセスで使われている。

4：管理，測定されている

構成管理の必要性は組織のすべてのレベルで認識されている。ベストプラクティスは常に新しいものへと進化している。手続と標準は周知され，研修に組み込まれている。また標準手続からの乖離はモニタされ，追跡され，報告される。いわゆる「プッシュ(push)」技術などのような自動化ツールが利用されており，標準どおり実施させ，安定性を向上させている。構成管理システムは IT インフラの大部分をカバーしており，それが適切なリリース管理と分散制御(distribution control)を可能にしている。物理的な検証と同様，例外分析が一貫して行われ，その原因が調査される。

5：最適化

すべてのインフラ構成は構成管理システムを使って管理されている。そのシステムには構成要素とそれらの相互関係について必要な情報がすべて載っている。構成データはベンダカタログと整合的である。相互関係のある複数のプロセスは，十分に統合され，構成データを利用し更新している。ベースライン(baseline)に関する監査レポートはハードウェアとソフトウェアの基本データを提供し，各個別装置(unit)に対する修理，サービス，保証，アップグレードと技術的な評価などに資する。ソフトウェアの導入規則は承認済みで，遵守されている。マネジメントは分析レポートに基づいて，修理とアップグレードについて将来予測を立てる。このレポートにはアップグレードの予想時期やテクノロジ再生機能(refreshment capabilities)に関する情報が提供されている。各人の作業端末を追跡しモニタリングすることによって，資産を保護し，盗難や誤用，乱用を未然に防止している。

DS10：問題と事故の管理

問題や事故を解決し，再発防止のために原因を調査することをビジネス目標としているIT プロセスの**問題と事故の管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**すべての事故を記録し，進捗管理する問題管理システムによって**可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
	万全性
S	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 問題管理は可用性管理や変更管理と明らかに整合性があること
- 各構成について発生した問題を追跡できるばかりでなく，構成データへアクセスできるようになっていること
- 問題の発生，兆候，診断および対策を適切なサポート要員に正確に伝達するための手段が整備されていること
- 問題管理者に報告する必要がある例外的な事象や兆候を，利用者や IT 部門に正確に伝達する手段があること
- 要員を支援するために，問題解決技術の研修が行われていること
- 事故管理を支援する，役割と実行責任の最新の一覧表が用意されていること
- 問題調査と解決にはベンダも関与していること
- 問題対応手続について事後分析が行われること

重要目標達成指標(KGI)　*4

- IT 資源における問題や事故の影響の低下度
- 最初に兆候の報告があってから問題解決するまでに掛かる時間の短縮度
- 未解決の問題や事故件数の減少度
- 先手を打って手当てすることによって避けることのできた問題の増加数
- リスクの高い問題や事故の発見から報告までの間のタイムラグの短縮度

重要成果達成指標(KPI)　*5

- 最初に兆候を認識してから問題管理システムに入力するまでの経過時間
- 問題の記録から解決までまたは報告までのそれぞれ掛かった時間
- 問題を調査してベンダが修正する(パッチを当てる)までに掛かった時間
- 報告された問題のうち，解決手法がすでに判明しているものの割合
- 変更管理と可用性管理の要員との間の調整のための打合わせの頻度
- 構成に関する問題分析報告がなされる頻度
- 正式な問題管理手法を用いなかった問題コントロール件数の減少

DS10 成熟度モデル

問題や事故を解決し，再発防止のために原因を調査することをビジネス目標としている IT プロセスの**問題と事故の管理**におけるコントロール

0：不在

問題管理や事故管理が必要であるという認識はない。問題解決プロセスはインフォーマルで，利用者と IT スタッフは問題に対して別々にそれぞれのやり方で対処している。

1：初期／その場対応

問題を解決し，事故を評価する必要性を認識している。知識の豊富なキーとなるスタッフが，自分の専門分野の問題や責任を負っている問題についてだけ，その解決をある程度支援している。情報は他の人たちと共有されていないので，対応策は担当者ごとに異なったものになっている。このため問題の対応策を模索している間に，また新たな問題が発生したり，ビジネス活動の停止によるロスが発生する結果になる。マネジメントは頻繁に，重点項目や指示，運用・技術サポートスタッフを変えてしまっている。

2：再現性はあるが，直感的

IT 関連の問題と事故を管理することの必要性は，ビジネスユニットと情報サービス部門の両部門で広く認識されている。問題解決プロセスは改善されており，数人の主要なスタッフが問題と事故の発生を管理する責任を負っている。情報は要員間で共有されているが，プロセスはまだ体系化されておらず，インフォーマルで，多くは事後対応的である。サービスレベルにはばらつきがあり，各問題解決担当者が利用できる知識が十分に体系化されていないため，サービスレベルの標準化が進んでいない。マネジメントへの事故報告制度や問題の分析は，限定的でインフォーマルである。

3：定められたプロセスがある

効果的な問題管理システムが必要であると考えられている。その証拠として，問題緊急対応チームの要員確保，研修と支援のための予算がとられている。問題解決・報告のプロセスは標準化されているが，まだ洗練されているとはいえない。それでも，問題や事故を誰に対してどのように報告するのかについて，利用者には明確に周知されている。問題管理のためのツールは，統合化されておらず分析されていないので，問題やその対応策についての記録や追跡は，問題対応チーム内でバラバラに行われている。問題管理の基準や標準は確立されているが，そこからの逸脱行為は，検知されない可能性がある。

4：管理，測定されている

問題管理プロセスの必要性は，組織内のすべてのレベルで理解されている。プロセスの実行責任とオーナーシップは明らかになっており，確立されている。方法や手続は文書化され，周知されており，またその有効性が評価されている。ほとんどの問題と事故は，特定，記録され，報告，分析され，継続的改善が行われ，また利害関係者に報告されている。この機能は，財産であり IT 目標達成の主要な寄与力であるとみなされているので，その知識と専門性が培われ，維持され，より高められている。事故対応能力は定期的にテストされている。問題や事故管理は，変更管理，可用性管理，構成管理など相互に関係する複数のプロセスとうまく整合が取れており，データ管理，設備管理，運用管理の側面で利用者に役立っている。

5：最適化

問題管理プロセスは，先見的，事前対応的であり，IT 目標達成に貢献している。問題を想定しているので，未然に防止される場合もある。定期的にベンダや専門家と連絡を取り合うことで，過去発生した問題や将来予想される問題や事故のパターンに関する知識が維持されている。問題とその解決策の記録，報告，分析は，自動化されていて，十分に構成データ管理と統合されている。大部分のシステムは自動検出と警告のメカニズムを備えており，継続的に追跡され，評価されている。

DS11：データ管理

データの入力，更新および保管の間，データの完全性，正確性，正当性を保証することをビジネス目標としているITプロセスの**データ管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**IT運用に関する業務処理統制および全般統制の効果的な組み合わせによって**可能となる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
	有効性
	効率性
	機密性
P	万全性
	可用性
	準拠性
S	信頼性

(P) 主　(S) 準

IT資源(*2)	
	人
	アプリケーション
	テクノロジ
	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- データ入力要件が，データベースとファイルのインタフェースを含むすべてのレベルで明確に示され，実行され，自動的な方法によって支援されていること
- データのオーナーシップとインテグリティ要件の実行責任が明確に示され，組織全体で受け入れられていること
- データの正確性とデータの標準は明確に周知され，研修や個人の能力開発プロセスの中に組み込まれていること
- データ入力の基準やデータ修正(手順)が，入力時に遵守されていること
- データ入力，処理，出力における万全性(インテグリティ)の標準が，正式化され，遵守されていること
- エラーではじかれたデータは訂正されるまで仮ファイル(サスペンド)の状態で保持されること
- データの正確性と万全性(インテグリティ)の標準を強制するために，効果的な検知方法が取られていること
- 変化するビジネスニーズに合わせて，万全性(インテグリティ)と信頼性を損なうことなく，プラットフォーム間で効果的にデータの変換ができるようになっていること

- データの手入力や二重入力が減少していること
- 効率的で柔軟性の高い対応策があり，データの効果的な利用を図っていること
- データはアーカイブ保管や保護され，復元のため必要なときはいつでも利用できること

重要目標達成指標(KGI)　*4

- データを準備するプロセスやタスクの減少度
- データの品質・適時性・可用性の改善度
- データに対する利用者満足度および信頼性の向上度
- データ修復やデータ破損の危険性の低減度
- データの冗長や重複，矛盾等のデータ欠陥数の低減度
- 法規制への遵守上の問題がない

重要成果達成指標(KPI)　*5

- データ入力エラーの割合
- 再処理しなければならなかった更新の割合
- 自動的なデータの万全性(インテグリティ)チェックがアプリケーションに組み込まれている割合
- 入力段階において防いだエラーの割合
- アプリケーションとは別に独立して実行された，自動的なデータの万全性(インテグリティ)チェック回数
- エラーの発生から検知，修正までに掛かった時間
- データ出力に関する問題の減少
- アーカイブ保管データを復旧させるまでの時間の短縮

DS11 成熟度モデル

データの入力，更新および保管の間，データの完全性，正確性，正当性を保証することをビジネス目標としているITプロセスの**データ管理**におけるコントロール

0：不在

データは企業の資源であり，資産であるとは考えられていない。データのオーナーシップは定められておらず，データの万全性(インテグリティ)，信頼性に対する説明責任者が任命されていない。データの品質やセキュリティは低いか，あるいは全くない。

1：初期／その場対応

データが正確であることの必要性を認識している。データ入力，処理，出力のエラーを予防・検出するために，いくつかの手法が個人レベルで開発されている。エラーの検出と修正は手作業によって行われている。またその手作業のルールや要件は，スタッフの異動，離職時に後任者に引き継がれていない。経営者は，コンピュータがプロセスに関与しているのだからデータは正確なはずだと思い込んでいる。データの万全性(インテグリティ)とセキュリティは，管理すべき対象となっていない。仮にセキュリティが導入

されているとすれば，それは情報サービス部門によって管理されている場合である。

2：再現性はあるが，直感的

データの正確性，万全性(インテグリティ)を確保する必要があるということは，組織全体で広く認識されている。データのオーナーシップという考え方が芽生えているが，それは部門やグループレベルにとどまる。主要な個人によってデータのルールと要件は文書化されているが，組織やプラットフォーム全体で一貫したものではない。データは情報サービス部門の管理下にあり，ルールと定義は，ビジネスではなくITからの要求事項を主体に作成されている。データセキュリティと万全性(インテグリティ)は，基本的には情報サービス部門の責任とされ，他部門はわずかしか関与していない。

3：定められたプロセスがある

データ・インテグリティの必要性は，組織全体で理解され，受け入れられている。データの入力，処理，出力の標準は正式化されており，遵守されている。エラーの検出と修正のプロセスは自動化されている。データのオーナーシップが割り当てられ，データの万全性(インテグリティ)とセキュリティは担当者の責任によってコントロールされている。自動化技術を，エラーや不整合を未然に防止したり，検知するのに活用している。データの定義，ルール，要件は，データベース管理部門によって明確に文書化され，保守されている。データは，プラットフォームにまたがり組織全体で一貫するようになっている。情報サービス部門は，データ保管の役割を引き受け，データ・インテグリティのコントロールはデータのオーナ側に移管されている。マネジメントは意思決定や将来計画立案にあたり，報告書や分析結果に依拠している。

4：管理，測定されている

マネジメントが，より意思決定支援に役立ち，より有益な報告を求めるようになり，データは企業の資源であり資産であると位置付けられている。データの品質における実行責任は明確にされ，割り当てられ，組織内に周知されている。標準化された手法が文書化され，保守され，データの品質をコントロールするために使われている。ルールは遵守され，データはプラットフォーム間，ビジネスユニット間で一貫している。データの品質は評価され，情報に対する利用者満足度がモニタリングされている。マネジメント報告は，顧客・傾向・製品を評価するうえで，戦略的な価値を持つようになっている。データの万全性(インテグリティ)が重要性を増し，データのセキュリティはコントロール要件として認識されている。組織全体の正式なデータ管理部門が確立され，データの標準化を実施するために経営資源と権限を与えられている。

5：最適化

データ管理は成熟した状態であり，統合され，機能横断的なプロセスになっている。また，利用者に高品質の情報を提供するという，明確でよく理解された目標と万全性(インテグリティ)・可用性・信頼性の規準もある。組織は，企業価値を最大化することを目標として，データ・情報・知識を，企業の資源，資産として考え積極的に管理している。知的財産の主要な要素として保護し取り扱うべき高品質のデータの重要性が，企業文化で強調されている。データの所有責任者は，すべての要求事項・ルール・規制・考慮事項について明確に文書化，保守，周知しており，戦略的な実行責任を担っている。

DS12：設備管理

人災や自然災害からIT設備および人員を保護することのできる適切な物理的環境を提供することをビジネス目標としているITプロセスの設備管理におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**適切な環境と物理的コントロールを導入し，適切に機能していることを定期的にレビューすることによって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
	有効性
	効率性
	機密性
P	万全性
P	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
	人
	アプリケーション
	テクノロジ
✔	設備
	データ

(✔) 該当

主要成功要因(CSF)*3

- 施設・設備すべてにおいて，設置場所の選定，建設，保安，人的安全，機械や電気システム，火事・落雷・洪水対策などを含む，戦略と標準が，明確に定められていること
- 施設・設備の戦略と標準は，ITサービス可用性の目標水準や情報セキュリティ方針と整合性が取れており，さらには業務継続計画や危機管理とも統合されていること
- 施設・設備について，実際の検査や監査だけでなく，明確な誤差許容範囲を定めた監査ログを残す機能のある自動システムや，CCTV(所内監視カメラ，閉回路テレビ)，また必要な場合には侵入検知システム等で定期的にモニタリングされていること
- 予防保全スケジュールが厳格に遵守され，設備のハウスキーピング(一般保全)管理のために厳格な規律があること
- 物理的なアクセスは，厳格に監視されていること。「そこにいる必要のある人だけ(need-to-be)」と「区域分け(zoning)」の原則に基づいており，また，身分証明(身元確認)と必要な場合には例外承認手続を適用していること
- 警察，消防署やその他地域の行政機関とのよい関係を保ち，情報交換を行っていること
- 明確で簡潔な最新の検知，検査，報告手続があり，それらが研修プログラムによって

周知されていること

重要目標達成指標(KGI)　*4

- 窃盗，損害，情報漏洩，停電，保健・安全に関わる問題等を含む設備や物理的なセキュリティ上の事故の減少度
- ユーティリティの停電を原因とするダウン時間の短縮度
- 適用される法規制に対する遵守度
- 保険方針の要求事項に対する遵守度
- コスト/リスク比の改善度

重要成果達成指標(KPI)　*5

- 多重化されていないため共倒れ事故の原因となる個所の特定ができるような網羅的な棚卸リストと配置図の有無
- 安全や施設・設備，セキュリティ対策についての要員研修の頻度
- 火災報知器や避難訓練のテストの頻度
- 物理的検査の頻度
- 入室制限された設備室への未承認の入室回数の減少度
- 無停電電源装置への即応型切替え／利用者の気にならない，スムーズな定期的な連続電源への切替度
- 物理的な事故が記録されてから終結するまでに掛かった時間

DS12 成熟度モデル

人災や自然災害から IT 設備および人員を保護することのできる適切な物理的環境を提供することをビジネス目標としている IT プロセスの**設備管理**におけるコントロール

0：不在

設備あるいはコンピュータ資源を保全する必要性についての認識はない。防火，塵埃，電力，高温や高湿度などといった環境要因について，モニタリングもコントロールもされていない。

1：初期／その場対応

人災や自然災害から資源や人員を保護するために適切な物理的環境を供給するというビジネス要件を認識している。しかし，標準手順はなく，設備，装置の管理は，キーとなる個人のスキルと能力に依存している。設備のハウスキーピング(一般保全)作業はレビューされず，人々は制限なく設備の中を動くことができる。管理者は設備環境のコントロール状況や要員の挙動をモニタリングしていない。

2：再現性はあるが，直感的

物理的コンピュータ環境を保護し，コントロールする必要性を認識している。予算や他の資源も割り当てられていることから，それははっきりしている。環境はコントロー

ルされ，オペレーション要員によってモニタリングされている。物理的セキュリティは正式なプロセスでなく，物理的設備の保全に関して高レベルの関心を持つ少人数のグループによって運営されている。設備保守手順はきちんと文書化されておらず，数人の個人のベストプラクティスに頼っている。物理的セキュリティの目標は正式な標準手順に基づいたものではなく，経営者はセキュリティ目的が達成されることを保証していない。

3：定められたプロセスがある

管理されたコンピュータ環境を維持する必要性は理解され，受け入れられている。環境のコントロール，予防保守，物理的セキュリティは，経営者によって承認，追跡される予算項目である。アクセス制限があり，コンピュータ設備へ入室できるのは許可された要員だけである。外部訪問者は記録され，エスコートされる場合もあるが，手続は個人の責任に委ねられている。物理的設備は目立たず，容易に特定できないようになっている。国の機関が保健・安全規制への遵守状況をモニタリングする。リスクに対しては保険が掛けられるが，保険コストを最適化しようとする努力は見られない。

4：管理，測定されている

コンピュータ環境のコントロールを維持する必要性は十分に理解されている。それは組織体系や予算配分を見る中でもはっきりしている。環境および物理的なセキュリティの要求事項は文書化され，入室は厳密に管理され，監視されている。実行責任とオーナーシップは明らかになっており，周知されている。設備のスタッフは，保健・安全上の実務ばかりでなく，緊急事態発生に備えて十分に訓練されている。標準化されたコントロール・メカニズムが整備されており，設備への入館は制限され，環境面や安全面の要因に対応している。マネジメントは，コントロールの有効性や，確立している標準に対する遵守状況をモニタリングしている。コンピュータ資源の復旧は，組織的なリスク管理プロセスに組み込まれている。組織全体の計画が策定され，定期的に統合テストが実施され，テストで得た教訓は計画の改訂に取り入れられる。情報は統合化され，保険のカバー率や関連コストを最適化するために使われる。

5：最適化

設備に関する長期計画があり，組織のコンピュータ環境を支援している。標準手順が全設備について定められており，設置場所の選定，建設，保安，要員の安全，機械的・電気的なシステム，火災・落雷・水害対策などが含まれている。すべての設備は棚卸され，組織が進めているリスク管理プロセスに従って分類されている。入館は，業務上の必要性をベースに厳密に管理され，常時監視されており，また，外部訪問者は必ずエスコートされる。専用の装置によってモニタリングされ，コントロールされており，しかもその装置室は「無人化」されている。予防保守プログラムは，厳密にスケジュールどおり行われ，また重要な装置は定期的にテストされる。設備戦略と標準手順は IT サービスの可用性の目標と整合性が取れており，業務継続計画や危機管理とも統合されている。経営者は継続的に設備をレビューし，最適化し，ビジネスへの貢献度を改善する機会があれば投資する。

DS13：オペレーション管理

重要な IT 支援が，通常どおり規則正しく機能することをビジネス目標としている IT プロセスの**オペレーション管理**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**すべての支援活動が完了するように記録し実施するスケジュール管理を行うことで**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
	機密性
S	万全性
S	可用性
	準拠性
	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- オペレーションの指示は明確に規定されており，合意済みの規準に従っているとともに，カットオフと再起動点に関する明確な指示が提供されていること
- オペレーションは高度に標準化されていること
- 問題管理や変更管理，可用性管理，継続性管理など，複数の関連したプロセスが関係する場合，相互が緊密に調整されていること
- オペレーション・タスクについては，高度に自動化されていること
- オペレーションプロセスが，自動化されたツールを用いて効果的に機能するようにリエンジニアリングされていること
- システム管理ツールの合理化と標準化が実施されていること
- 入出力媒体の取扱いは，できる限り利用者に限定していること
- ジョブスケジュールの変更は厳密に管理されていること
- 新しいジョブスケジュールの受入れについては，書類の配布も含め厳格な手続があること
- 予防的保守計画があること
- サービスサポート契約がベンダと締結され，履行されていること

- 明確で簡潔な，問題の検知，検査，報告手続が確立していること

重要目標達成指標(KGI) *4

- スケジュールの遅延や乖離の減少度
- 出力媒体の適切な配布先への作成・送付の完了した数
- 時間どおり，スケジュールどおりに利用可能である資源の数
- オペレーションに関連したエラーの減少度
- オペレーションの介入によって生じる，計画または計画外のダウン時間の減少度
- 全処理負荷に関するオペレーションコスト総額の削減度

重要成果達成指標(KPI) *5

- さまざまな段階におけるコンピューティングプロセスの終了数
- オペレータ介入回数の減少度
- 問題発生数，スケジュールからの遅延・乖離件数の減少度
- 再実行と再起動の回数の減少度
- 計画外の保守コストの削減度
- ジョブやイベントのうち，計画外に発生した件数の低減度
- 利用者がコントロールできるパラメータ数の増加度
- 利用者からの要請と，能力(キャパシティ)の利用可能性との間のバランス状態
- オペレーションの成果をモニタリングするために行われる分析と報告の頻度
- バックアップ検査の頻度
- 設備の平均的な経過年数

DS13 成熟度モデル

重要な IT 支援が，通常どおり規則正しく機能することをビジネス目標としている IT プロセスの**オペレーション管理**におけるコントロール

0：不在

基本的な IT 支援とオペレーション活動の整備のために，時間や資源を使っていない。

1：初期／その場対応

組織は，IT 支援部門を設ける必要性を認識している。しかし，標準手続は確立されておらず，オペレーション活動は事実上，事後である。大多数のオペレーションは正式にスケジューリングされたものではないばかりか，処理要求は事前の正当性検査なしで受け入れられている。ビジネスプロセスを支援しているコンピュータは，しばしば割込み・処理の遅れ・利用不可能の状態となる。従業員が資源の空きを待つ間に時間ロスが発生している。システムは安定しておらず，利用できない場合があるうえ，出力媒体は予期しない場所に配布されたり，あるいは全く存在しなかったりする。

2：再現性はあるが，直感的

IT を支援するうえで IT オペレーション活動が果たす重要な役割について，組織は十分に認識している。さらに組織は，利用者とシステムオペレーション間の調整を行う必要があることを広く周知している。ツール導入に必要な予算は 1 件ずつ個別に割り当てられている。IT 支援のためのオペレーションは正式なものでなく，直観的に行われる。個人のスキルと能力に大きく依存している。何をするべきか，いつ，そしてどんな順序にすべきかなどの指示は文書化されていない。オペレーションの標準はなく，オペレータの正式な研修も行われていない。マネジメントは，IT オペレーション上のスケジュール達成状況を評価していない。またスケジュールの遅延の分析を行っていない。

3：定められたプロセスがある

コンピュータオペレーション管理の必要性は理解され，組織内で受け入れられている。経営資源が割り当てられ，OJT が行われる場合もある。よく使われ反復性のある機能は，正式に定義され，標準化され，文書化され，オペレーション要員や利用者へ周知されている。起きたイベントや完了したタスクの結果は記録されるが，管理者への報告は限定的であるか，または行われていない。オペレータ介入を制限するために，自動スケジューリングや他のツールが広く利用され，標準化されている。他の通常の IT サポート活動も明確にされており，関連するタスクも定義されている。オペレーション上で新しいジョブを追加することは厳密に管理されている。計画外のイベント数を減らすための正式な方針がある。ベンダとの保守・サービス契約は，実質的にはまだ正式なものではない。

4：管理，測定されている

コンピュータオペレーションとその支援の実行責任が明確に定義され，責任者が任命されている。コンピュータオペレーションには，財務面と人的資源両方の予算が割り当てられている。研修は，正式のもので継続的に実施されており，キャリア形成の一部となっている。スケジュールとタスクは文書化されており，社内の IT 部門とビジネス部門に周知されている。合意した標準成果やサービスレベルと比較することで，日々の活動を評価しモニタリングすることができる。基準からの乖離が発生すると，迅速に対処され修正される。管理者は，コンピュータ資源の使用状況と作業やタスクの完了状況をモニタリングしている。継続的改善の手段として，プロセスを自動化する努力がされている。保守・サービス契約がベンダとの間で正式に締結されている。オペレーション管理のプロセスは，問題管理や可用性管理のプロセスと整合性が取れている。エラーや欠陥の原因分析も行われている。

5：最適化

IT を支援するオペレーションは，効果的，効率的で，柔軟性がある。迅速でサービスレベルのニーズを満たしており，企業活動を損なうこともない。IT のオペレーション管理プロセスは，知識ベース(knowledge base)を利用して標準化，文書化され，継続的に改善されている。複数のシステムを支援する自動化されたプロセスは継ぎ目なく運営されており，利用者が意識することなく利用できる安定した環境作りに貢献している。利用者ニーズと IT オペレーションはこのうえなく整合性がとれている。すべての問題と障害は分析され，原因が特定される。変更管理部門との定期的なミーティングによって，本番スケジュール上でタイムリにさまざまな変更を行える。ベンダの協力で，設備の老朽化や誤動作の兆候が分析され，事実上保守は予防保守が主体となっている。

モニタリング

M1：プロセスのモニタリング

IT プロセスに対して設定された成果目標を達成することをビジネス目標としている IT プロセスの**プロセスのモニタリング**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**関連する成果指標を定め，系統的でタイムリな成果報告を行い，目標から乖離した場合迅速に対応することによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
S	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 有益，正確で，タイムリな管理用報告書が利用できること
- プロセスごとに KGI と KPI が明確となっており，理解されていること
- IT の成果測定には，財務上，運用上の規準や，顧客や組織の学習規準が含まれており，全社的な目標との整合性を取りながら，IT バランススコアカードのようなツールに統合することが可能になっていること
- プロセスの目的が明確に理解され，周知されていること
- IT ガバナンスに関する報告の要件を定義し，それを満たすためのフレームワークが確立されていること
- 過去の成果情報を蓄積した知識ベースが整備されていること

重要目標達成指標(KGI)*4

- 適切な数の成果指標を一貫して適用すること
- プロセス改善が必要なケースを検出し，改善を行った件数の増加数
- 成果報告に対するマネジメントやガバナンス部門の満足度
- 未処理のプロセス上の欠陥数の低減

重要成果達成指標(KPI)*5

- プロセス上の欠陥が発生してから報告されるまでのタイムラグ
- 欠陥が報告されてから対応が取られるまでのタイムラグ
- 報告されたプロセス上の全欠陥に対する，マネジメントによる傾注・フォローアップが必要であると判断された欠陥の比率(ノイズ指標)
- モニタリングされているプロセスの数
- モニタリングによって判明し，紐付けられた事例と効果のリレーション数
- プロセスの有効性に関する外部ベンチマークの数
- ビジネスの変更から，それに対応して成果指標を変更するまでのタイムラグ
- ビジネス目標の変更がないにもかかわらず，成果指標を変更した回数

M1 成熟度モデル

IT プロセスに対して設定された成果目標を達成することをビジネス目標としている IT プロセスの**プロセスのモニタリング**におけるコントロール

0：不在

プロセスのモニタリングは行われていない。IT 部門が独自にプロジェクトやプロセスのモニタリングを行うこともない。また，利用できる有用で，タイムリで，正確な報告書もない。プロセスの目的を明確に理解する必要があるとは認識されていない。

1：初期／その場対応

経営者は，プロセスをモニタリングするために情報を集め，評価する必要があることを認識している。情報収集と評価のための標準的な手順は明確になっていない。モニタリングは実施されているが，評価尺度は，特定の IT プロジェクトやプロセスの必要性に応じてそれぞれ選択されている。一般的に，組織に損失を与えたり，混乱を招くような事故が発生してから，事後的にモニタリングが導入されている。モニタリングは他部門の便益向上のために情報サービス部門が導入しているが，IT プロセスに対しては導入されていない。プロセスの定義やモニタリングの尺度は伝統的な財務，業務，内部統制のアプローチに従っており，情報サービス特有のニーズには対応していない。

2：再現性はあるが，直感的

モニタリングすべき基本的な評価項目は明らかになっている。情報収集と評価の方法・技法は定められているが，モニタリングが全社的に採用されているわけではない。モニタリングプロセスの評価に関する計画や管理を行う部門はあるが，判断は，主要な担当者のノウハウに基づいて行われている。情報収集のために限定されたツールが選定され，導入されているが，専門的技術が不足しているため，ツールの機能を十分に使いこなしていない恐れがある。情報サービス部門は，コストセンタと位置付けられており，収益部門に対する貢献度は評価されていない。

3：定められたプロセスがある

マネジメントは，モニタリングの標準手順を制度化し，周知している。モニタリングについての教育研修が行われている。過去の成果情報を蓄積した知識ベースが正式に作

成されている。評価は，まだ，個々の IT プロセスやプロジェクトのレベルで行われているだけであり，すべての IT プロセス間で統一されているわけではない。組織内の IT プロセスやサービスレベルをモニタするためのツールが導入されつつある。組織の業績に対する情報サービス部門の貢献度の評価尺度は定められているものの，伝統的な財務的規準や業績規準が用いられている。IT 固有の成果の評価尺度も定められているが，非財務的尺度や，戦略的な尺度はまだ正式なものではない。業務部門に提供されたサービスに関する，IT 利用者満足度やサービスレベルが評価され始めている。

4：管理，測定されている

マネジメントは，運用上の許容できる乖離レベルを定めている。モニタリング結果の基準線として，標準または正常レベルが設定されている。すべての IT プロジェクトやプロセスにわたって，標準評価尺度は統一されている。また，情報サービスの管理報告システムが構築され，完全に自動化されている。自動化されたツールは全社的に統合されており，さまざまなアプリケーション，システム，プロセスに関する運用情報を収集し，モニターしている。成果を測定するために，戦略指向の KGI，KPI，CSF を明らかにする仕組みがある。また，成熟度モデルをベースにして，組織の進化度を評価するための規準も定義されている。情報サービス部門の成果測定には，財務的規準，業績規準や，利用者および組織が経験から得た規準を用いており，全社的な目標と確実に整合性が取られている。

5：最適化

継続的な品質改善プロセスがあり，全社的なモニタリング標準や方針を最新のものに維持するとともに，業界のベストプラクティスを取り入れている。モニタリングプロセスはすべて最適化され，全社的な目標の達成に役立っている。KGI，KPI，CSF が，成果測定のために日常的に使われており，IT バランススコアカードのような戦略的評価フレームワークと統合されている。また，プロセスモニタリングと常時のプロセス再設計作業は，成熟度モデルをベースに策定される計画や，全社的な業務プロセスの改善計画と整合性が取られている。比較規準が十分に理解されており，業界や主要な競合企業に対するベンチマーキングが正式に行われている。

M2：内部統制の十分性の評価

IT プロセスにおける内部統制目標を達成することをビジネス目標としている IT プロセスの**内部統制の十分性の評価**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**内部統制をモニタリングし，その有効性を評価し，その結果について定期的に報告を行うことに責任関与することによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
P	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- マネジメントがプロセス上のどの構成要素(コンポーネント)をコントロールする必要があるのかを明らかにしていること
- 内部統制，遵守性，内部監査の実行責任が明確に理解されていること
- 内部統制を遵守させる役割を担う部門(コンプライアンス部門)に的確な能力や権限があり，適切に権限委譲されていること
- IT コントロールプロセスのフレームワークが適切に定められていること
- 明確なプロセスに従い，内部統制上の欠陥をタイムリに報告していること
- 内部統制のモニタリングデータは，正確，完全かつタイムリであること
- 内部統制の欠陥へ対処することについて，マネジメントの責任関与があること
- リスク評価プロセスとセキュリティプロセスの整合性が取られていること
- 内部統制上の事故とその対応策に関して，知識を共有するためのプロセスがあること

重要目標達成指標(KGI)*4

- 内部統制モニタリングの結果報告に対する，上級管理者の満足度と安心度の指標
- 内部統制上の事故発生危険度の低減

- 外部による証明や保証(アシュアランス)における肯定的な報告書(適正意見書)
- 内部統制改善のための取組みの件数
- 規制や法律上の遵守違反がないこと
- セキュリティ上の事故や品質上の欠陥の件数の低減

重要成果達成指標(KPI)*5

- 内部統制の自己評価を行った回数とその範囲
- 内部統制上の欠陥の発生に対する報告の適時性
- 内部統制の遵守に関する報告書の数，頻度，担保範囲
- 内部統制上の問題に対してタイムリに対応した件数
- ルート原因分析によって内部統制が改善された件数

M2 成熟度モデル

IT プロセスにおける**内部統制目標を達成すること**をビジネス目標としている IT プロセスの**内部統制の十分性の評価**におけるコントロール

0：不在

組織には内部統制の有効性をモニタリングする手続がない。また，内部統制に関する報告を行う制度もない。IT 運用におけるセキュリティと内部統制のアシュアランスについても認識されていない。マネジメントや従業員には，総じて，内部統制に関する認識がない。

1：初期／その場対応

運用上のセキュリティや内部統制の保証(アシュアランス)を行うことに対して，正式な経営者の責任関与がない。内部統制の妥当性の評価は，個人のノウハウに依存して場当たり的に行われている。IT 管理者は，内部統制の有効性をモニタリングする責任者を正式に割り当てていない。IT に関する内部統制評価は，伝統的な財務諸表監査の一環として行われ，情報サービス部門のニーズを反映していない方法論やスキルが使われている。

2：再現性はあるが，直感的

組織は改善の取組みのきっかけとして，インフォーマルな内部統制に関する報告書を利用している。計画と管理のプロセスは定められているが，評価のプロセスについては主要な担当者のスキルに依存している。組織は内部統制のモニタリングを行うことについて，だんだんと認識を深めてきている。また，マネジメントは基本的な標準評価尺度を確立し始めている。情報サービスの管理者は，重要な内部統制の有効性を定期的にモニタリングしている。セキュリティ上のコントロールに対するモニタリングも行われ，その結果は定期的にレビューされている。IT 環境に固有の方法論とツールが使われ始めているが，まだ一貫していない。スキルを持った IT スタッフは，日常的に内部統制の評価に関わっている。また，IT 環境に固有のリスク要因が，明確になってきている。

3：定められたプロセスがある

マネジメントは，内部統制のモニタリングを制度化し，支援している。内部統制のモ

ニタリング活動を評価し報告するための方針と手続が作成されている。過去の内部統制のモニタリング情報を蓄積した標準評価尺度知識ベースが整備されている。また，内部統制のモニタリングに関する教育研修プログラムが導入されている。内部統制のモニタリングに関するピアレビュー(相互レビュー)制度も設けられている。運用上のセキュリティや内部統制の保証(アシュアランス)に関して，自己評価や内部統制のアシュアランスレビューが行われており，そこでは，情報サービス部門の管理者がビジネス部門の管理者と一緒に関与している。ツールの利用はあるが，必ずしもすべてのプロセスに取り入れられてはいない。IT 部門のために特別に作成されたコントロール・フレームワークの中では，IT プロセスのリスク評価方針が用いられていている。情報サービス部門では，独自に，技術面での IT の内部統制能力の開発を行っている。

4：管理，測定されている

マネジメントは，内部統制のレビュープロセスに関して，ベンチマークや定量的な目標を定めている。組織は，内部統制のモニタリングプロセスについて許容レベルを設定している。統合され，さらに自動化されたツールが，内部統制レビュープロセスに取り入れられており，定量的な分析やコントロールの利用が増えている。情報サービス部門全体について，プロセス固有のリスクとそれを低減するための方針が定められている。IT 内部統制部門が正式に設置されており，専門的技能と資格を持った専門職員が配置され，上級管理者によって承認された正式なコントロール・フレームワークが利用されている。業界標準に照らしたベンチマーキングやベストプラクティスの作成が正式に行われ始めている。

5：最適化

マネジメントは，全社的な継続的改善プログラムを確立しており，内部統制のモニタリングに業界ベストプラクティスや経験則を取り入れている。組織は最先端のツールを利用しており，適切なものが取り入れられ，更新されている。知識の共有化は正式に行われており，情報サービス部門に特化した正式な研修プログラムが導入されている。IT のコントロール・フレームワークは，単に，IT の技術的な問題を取り扱うだけではなく，組織目標との一貫性を保つことができるように，全社的なフレームワークや方法論に統合されている。

M3：独立した第三者の保証の獲得

組織，利用者，及びサードパーティ・プロバイダ間における信頼を深めることをビジネス目標としているITプロセスの**独立した第三者の保証の獲得**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**独立した第三者による保証(アシュアランス)レビューを定期的に実施することによって**可能になる。

その際に考慮すべき事項として，特定のIT資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
P	準拠性
S	信頼性

(P) 主　(S) 準

IT資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 利害関係者(ステークホルダー)のニーズと継続的な整合性があること
- IT保証(アシュアランス)活動，特に全般統制，品質証明，主要な意思決定などに関するプロセスが定められていること
- 外部のサービスプロバイダのベンチマーキングを日常的に行っていること
- ITにおける重要な意思決定をする際に，事前に，サードパーティによる保証(アシュアランス)意見に関し，要件分析を行っていること
- 独立した第三者による保証を獲得する前に，主要な利害関係者(ステークホルダー)とともに高レベルのリスク評価を行っていること
- 継続的な改善を行うために，独立した第三者による保証の利用に対するマネジメントの責任関与(コミットメント)があること
- 一般に実用化されている，例えばSysTrustのような手続に準拠して保証(アシュアランス)活動が行われていること
- 協力を促進するために，監査人と被監査人との間にパートナーシップがあること

重要目標達成指標(KGI)*4

- 合意した範囲すべてにおけるシステム全般の内部統制に関し，受け入れられた監査意見の増加数
- 合意した範囲すべてにおける品質について，保証や認定を受けた件数の増加数
- システム稼働継続，契約交渉，合弁事業(ジョイント・ベンチャ)，主要調達先の選定などの IT に関する重要な意思決定について，利害関係者(ステークホルダー)に対して報告されたセカンドオピニオンの増加数
- 独立した第三者による内部統制レビュー，品質証明，セカンドオピニオンに関して，期限までに改善を行った勧告事項の割合
- IT に関する重要な意思決定のうち，失敗もしくは保留となっている件数の低減数
- 利害関係者(ステークホルダー)からの信頼を示す指標

重要成果達成指標(KPI)*5

- 保証(アシュアランス)や監査証明の入手に要する間接費用の低減
- 保証(アシュアランス)報告の適時性
- 保証(アシュアランス)活動の適時性
- 着手した保証(アシュアランス)プロセスの数
- 保証(アシュアランス)報告書が受け入れられるまでに内容の修正を繰り返した回数
- 保証(アシュアランス)報告書の入手を目指していない場合でも，保証(アシュアランス)に対する IT の意思決定を必要とする件数
- 保証(アシュアランス)報告書の入手を目指している場合でも，保証(アシュアランス)に対する IT の意思決定を必要としない件数
- 肯定的な保証(アシュアランス)を入手した後に，失敗または保留となった，主要な IT における意思決定数の低減

M3 成熟度モデル

組織，利用者，およびサードパーティ・プロバイダ間における信頼を深めることをビジネス目標としている IT プロセスの**独立した第三者の保証の獲得**におけるコントロール

0：不在

アシュアランスのためのプロセスは整備されていない。セキュリティ方針も導入されていない。SLA(サービスレベル合意書)は結ばれておらず，プロセスは評価されていない。マネジメントは保証(アシュアランス)，証明のプログラムを全く制定していない。

1：初期／その場対応

組織は，別々に IT プロセスを管理している。例外的ではあるが，証明や保証(アシュアランス)のプロセスが見られる。証明やアシュアランスは，規制の変更や法律上の要求，利用者からの要請などを契機に行われている。また，アシュアランスのプロセスは，タスクフォース(専門委員会)やアシュアランススキルを持たない技術スペシャリストによって，事後対応的に行われている。

2：再現性はあるが，直感的

情報サービス部門の管理者は，保証(アシュアランス)活動を管理するプロセスを導入している。保証(アシュアランス)要件は，まだ，ビジネスニーズやビジネス要件に関連したものだけで，情報サービス部門が統括している。リスク管理者は，情報サービス管理の一環として証明や保証(アシュアランス)プログラムを運営している。情報サービス部門はシステムリスクを明らかにするためにリスク評価を行っている。上級管理者は，独立した第三者による保証の獲得を支援し，責任関与(コミットメント)している。証明や保証(アシュアランス)の手法や技法が確立されており，ベストプラクティスを求めてベンチマーキングを行っている。組織内外のリソースを選択するプロセスは正式に承認されている。

3：定められたプロセスがある

IT 保証(アシュアランス)活動のプロセスが定められており，専門性，重要性，必要とされる独立性などのレベルに応じ，組織内外のリソースを利用する際の判断規準が制度化されている。この保証(アシュアランス)プロセスには，法規制上の要件，証明の必要性，組織にもたらされる一般的な効果，ベストプラクティスの把握などが含まれている。IT プロセスに関する保証(アシュアランス)要件も作成されている。マネジメントは，すべての保証(アシュアランス)活動のレビューに参画している。また，情報サービス部門以外の管理職も保証(アシュアランス)，証明レビューに積極的に関与している。証明，保証(アシュアランス)のベストプラクティスに関する知識ベースが作成されている。主要な IT プロセスについては，品質保証もされている。

4：管理，測定されている

主要な IT プロセスを明らかにし，明確な保証(アシュアランス)計画を立てることを確実なものにするため，マネジメントは保証(アシュアランス)のプロセスを導入している。IT プロセスは，それらが支援している業務プロセスの側面からレビューされている。保証(アシュアランス)プロセスは定量的に管理され，コントロールされている。管理者は他のプロセスを改善するために，保証(アシュアランス)や証明プロセスから得た教訓を活用している。新規のプロセスや他のプロセスをベンチマーキングする際に，ベストプラクティスを確実に適用することができるように，知識ベースが利用されている。正式な保証(アシュアランス)プロセスが整備されており，組織内部，外部の利用可能な知識やスキルのバランスを継続的に評価することによって，保証(アシュアランス)機能を保っている。社内および社外の保証(アシュアランス)を実施するためのコスト／利益規準が定められている。

5：最適化

マネジメントは，重要な業務プロセスのすべてについて，各プロセスを支援している IT インフラに対する保証(アシュアランス)プロセスが必ず実施されるように，評価制度を導入している。組織内では，業界のベストプラクティスを反映するように，保証(アシュアランス)や証明プロセスの改善が継続的に行われている。マネジメントは，保証(アシュアランス)や証明活動の結果を，全社的なプロセスの中に迅速に取り入れるノウハウを持っている。サードパーティのサービスプロバイダの有効性やビジネスパートナとの関係は，日常的に評価されている。また，上級管理者が提唱している正式な戦略に基づいて，国内および国際標準への準拠や，業界における知名度や他社に対する優位性を得ることを目指している。

M4：独立監査の実施

ベストプラクティスの助言を受けることで信頼性や利益を向上させることをビジネス目標としている IT プロセスの**独立監査の実施**におけるコントロールは，

当該ビジネスが掲げる情報要請規準(*1)を満たす情報が提供されることを，別掲(*4)の重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，**独立監査を定期的に実施することによって**可能になる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には，重要成果達成指標(KPI)(*5)を用いる。

情報要請規準(*1)	
P	有効性
P	効率性
S	機密性
S	万全性
S	可用性
P	準拠性
S	信頼性

(P) 主　(S) 準

IT 資源(*2)	
✔	人
✔	アプリケーション
✔	テクノロジ
✔	設備
✔	データ

(✔) 該当

主要成功要因(CSF)*3

- 監査委員会は，監査部門の独立性，実行責任，権限と説明責任を規定する監査実施命令書を制定し，支援していること
- 初回レビューや定期的レビューの対象となるビジネス活動と IT 活動を明確にするために，リスク分析に基づいた監査計画が行われていること
- 監査の計画と実施は事前対応的に行われていること
- 監査手法は，適切なツールと技術を備えていること
- 全体のステイタス(グローバル・ステイタス)についての監査勧告事項の追調査や改善を行うために，マネジメントと監査部門の間で明確な実務手続に関する合意がなされていること
- 監査人は，勧告内容について，費用・効果・リスクも考慮して影響分析を行っていること
- 監査は，一般に受け入れられている監査基準に準拠して実施されていること

重要目標達成指標(KGI)*4

- 独立部門による監査活動による信頼性の向上
- 独立部門による監査で受けた助言や勧告の結果，新たに取り入れられたベストプラク

ティスの増加数
- 支出あたりの付加価値の増大
- 監査委員会と上級管理者との間のコミュニケーション深度の向上

重要成果達成指標(KPI)*5

- 監査部門との協働関係に対する満足度の向上
- 新規の検出事項に基づいて取られた，改善的対応や維持対応の件数
- 専門的，技術的資格を持った監査人の増加数
- 計画から報告までの監査プロセスに要する時間の短縮

M4 成熟度モデル

ベストプラクティスの助言を受けることで信頼性や利益を向上させることをビジネス目標としている IT プロセス**独立監査の実施**におけるコントロール

0：不在

マネジメントは独立監査の重要性に気がついておらず，独立監査は行われていない。

1：初期／その場対応

インフォーマルな IT 監査部門があり，時折，独立の立場でのレビューを行っている。しかし，監査の全体計画はなく，各レビューの間の一貫性もない。独立部門による監査の計画・管理・報告は，各担当者のノウハウに依存している。監査サービスの計画や提供の品質は一般に低く，成果物はサービスごとにまちまちで，マネジメントの関与もほとんどみられない。

2：再現性はあるが，直感的

マネジメントは，独立部門による監査を規定することが潜在的に有用であると認識しているが，その目的，権限，実行責任を定めた文書化された方針はない。上級管理者は，定期的に独立部門による監査が確実に行われるようにするためのインフラやプロセスを確立していない。独立部門による監査の計画・管理・報告の方法は，過去の経験や監査チームのメンバのノウハウに基づいており，パターン化している。各監査間の一貫性はなく，前回の監査検出事項のフォローもあまり行われていない。監査プロセスにおける IT 管理者の関心やコミットメントにも一貫性はなく，特定の監査チームのレベルによっている。

3：定められたプロセス

上級管理者によって，IT 監査部門の設立が認可され，その独立性と権限が与えられている。監査管理者は，IT の環境やイニシアチブを認識し，理解している。また，監査計画や管理のプロセスが確立している。監査スタッフは，監査基準の遵守を求められているが，監査結果にはばらつきがある。監査コメントに対する改善は行われてはいるが，フォローはあまり行われず，未解決のままになることも多い。品質保証の基本要素が確

立されており，適切な監査基準に準拠した手続が確実に取られるとともに，監査部門の活動の有効性が高められるようになっている。しかし，一般に，IT 監査，財務諸表監査，および業務監査の機能は統合されていない。IT 管理者は，独立部門による監査の必要性に気付いているが，実際に提供された監査の品質には必ずしも満足しておらず，監査部門が有効な勧告を行うのに必要十分な知識を持っているのかについて疑問を抱いている。

4：管理，測定されている

現在および将来のニーズの評価をもとに，リスク分析に基づいた戦略的監査計画が策定されている。周期的な実施計画やリソースの可用性を考慮して，個別の監査計画が策定されている。また，監査プロセスは，特定の業務に合わせることも可能である。監査プロセスに関する知識ベースが整備されており，品質評価が確実に実施され，有益な勧告が行われるようになっている。IT 監査は，関連する財務諸表監査や業務監査と調和がとられ，統合されている。監査結果はマネジメントに報告され，監査で明らかになった重要な問題に対して，マネジメントが改善策を確実に講じることができるようフォローされている。体系的な品質保証機能によって，監査プロセスの定量的な管理とコントロールが促進されている。IT 監査部門は，対応策の策定に参画するとともに，コントロールが業務プロセス中に適切に組み込まれるように，開発プロジェクトにも関与している。IT 管理者は通常，すべての監査に積極的に責任関与しており，監査結果を活用して業務の改善に努めている。

5：最適化

監査部門は，絶えず全社レベルで発生する業務プロセス関連の懸案事項や IT のコントロール・リスクに関する問題に対して，迅速に対応することができる。監査計画は，ビジネス戦略および IT 戦略と密接に関連している。変化していく環境に適応しながら改善を行うために，監査プロセスはモニタリングされ，分析されている。これには，監査業界で行われている定量的なモニタリング活動や，最先端の業界ベストプラクティスや外部における監査プロセスの変更の動向を取り入れることが含まれている。IT 監査は，ビジネス計画の策定やビジネス計画を支援するすべてのプロジェクトに対して実施され，すべての業務処理プロセスに適切なコントロールが組み込まれることを保証している。また，すべてのプロジェクトに対して，コントロールやビジネスに関する助言を行っている。

付録

付録 Ⅰ

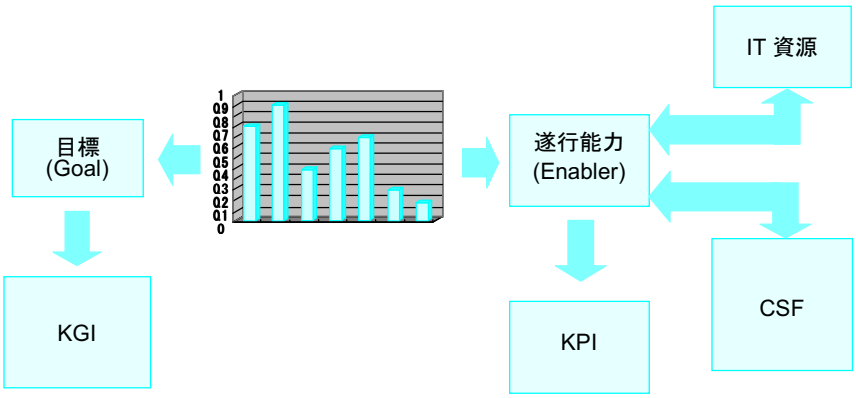
使用法

マネジメントガイドライン

各マネジメントガイドラインでは，前半に 34 の COBIT プロセスの個々のプロセスに関する以下のような要素を記述している。

- プロセスの定義
- プロセスの目標
- 目標を実現する手法(目標達成を確実にするために，プロセスをコントロールするための方法)
- プロセスに関する IT 資源
- 情報規準とそのプロセスにおける相対的な重要度(P＝最も重要度が高いもの，S＝重要度は下がるが無視していいというものでもない)
- CSF(主要成功要因)
- KGI
- KPI

上記の要素は，次の図で表されるように相互に関連性がある。 この関係はバランススコアカードの原則に基づき，KGI で評価される目標と，KPI で成果評価される遂行能力が関係付けられている。遂行能力は多くの CSF(主要成功要因)と関連があり，特定かつ実践的なものになっており，特定の IT 資源を使う。



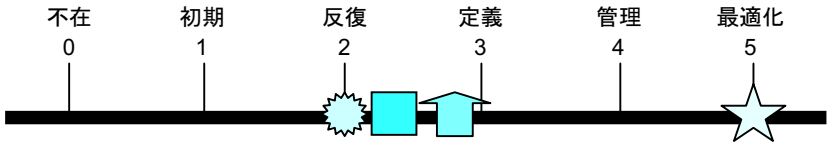
さらに，汎用のマネジメントガイドライン(付録 IV 参照)や IT ガバナンスガイドライン(付録Ⅴ参照) からもガイダンスを入手できる。 これらは両方とも，IT プロセス自体を管理可能な状態に保つというハイレベルなニーズに応えるクイックガイドを提供している。

最後に，本ガイドラインは，CSF から KPI までが網羅されたすべての実施要領を，あらゆる場合に必ず適用しなければならないとしているのではない点には注意する必要がある。適当に取捨選択する必要がある。 個々のプロセスのガイドラインについている成熟度モデル(この付録の中の次のセクションを参照)は，選択をする際に役立つものである。 しかしながら，IT に対して高いレベルの信頼性が必要なビジネスや生き残りが情報活用によって決まるようなビジネスでは，成熟度レベルの 3 または 4 に達した，グローバルなレベルに近いアプリケーションでなければ良質な実務慣行を構成することはできない。

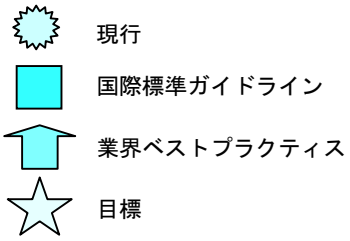
成熟度モデル

独立したツールとして，成熟度モデルが各マネジメントガイドラインの後半の囲みに 34 の COBIT プロセス個々に対して記載されている。 このツールは以下のような段階的な適用の基礎となるものである。

- 組織の現状を判断し，自社の成熟度を自己評価する。
- 自己評価の結果を使って，将来の目標レベルを設定する。その際には，自社のあるべきレベルをもとに設定すべきで，レベル 5 にこだわる必要はない。
- 目標と現状のギャップ分析をベースにして，目標を達成するためにプロジェクトを立案する。
- プロジェクトのクラス分けや費用対効果分析をベースにして，プロジェクトの優先順位を付ける。



凡例



凡例

0：不在------管理プロセスは全くない
1：初期------管理プロセスは場当たり的で組織的ではない
2：反復------管理プロセスが標準的なパターンに従うようになる
3：定義------管理プロセスは文書化され、周知されている
4：管理------管理プロセスはモニタリングされ、評価測定されている
5：最適化---管理プロセスは、ベストプラクティスに従っており、また自動化されている

自己評価と目標の特定

個別の評価に当たっては，組織は 0 から 5 までの 6 ポイント評価を用い，自社のポジションを明らかにすべきである。そうすれば，三つの参照ポイント(自社の目標，国際標準，ベストプラクティス)と容易に，一見して分かる方法で比較をすることができる。

自己評価に当っては，評価テーマについて一つ一つ順番に実施していく必要がある。六つのポイントの説明を読み，どれが組織の現状に最もよく当てはまるかを判断するのである。IT プロセスが組織にとって重要であればあるほど，高いポジションにあるはずである。例えば，比較的安定したビジネス環境においては，サービス提供とサポートのドメインに属する 13 の IT プロセスの成熟度が高い企業が成功している。逆に，かなり劇的に変動するビジネス環境で生き残るだけではなく成功するためには，計画と組織，調達と導入のドメインの成熟度を引き上げることが必要である。

個々のポイントは厳密な評価が必要であり，あるレベルに入るためには，説明にあるすべての条件を満たさなくてはいけない。また能力をもとにした場合と実績をもとにした場

合では差が出ることについても注意しなければならない。例えば，ある特定のセキュリティとコントロールの手続を作成するための能力とスキルを調達するには，1 回の意思決定で足りるが，調達の終了後もその能力が一貫して維持されているか，実績を評価する必要がある。

ビジネス上の要求事項を達成するうえで，情報に対する依存度が高くなることや情報の価値が増大することを特に強調するためには，組織の IT 戦略を踏まえて目指す目標が，6 段階の説明のどれに一番近いか検討する必要がある。自社のおかれている環境や戦略目標を押さえたうえでセキュリティやコントロールに関する現実的な対応レベルをまとめるには，外部とのベンチマーキングが大いに役立つと思われる。

ギャップ分析

多くの場合，二つの自己評価の値(現状と目標)にはチャート上で目に見えるギャップが生じているはずである。ギャップを解消し，戦略目標を達成するために必要な作業のボリュームが，視覚的に分かる。しかしながら，このギャップについても，内容を詳細に記録し，ギャップ分析の結果が使えるようにしておくことが必要である。これは，IT のセキュリティやコントロールに関する戦略目標の実現に向けて組織を変革するための一連のプロジェクトを計画するために必要となる。

ギャップ分析の結果，「現状」と「戦略目標」との間のギャップを解消するために必要なアクションがすべて盛り込まれたリストができあがる。次にこのリストを，必要なアクションを実行するプロジェクトを含めたマッチングリストの作成に利用する必要がある。ギャップとプロジェクトの間は，おそらく多対多(N : N)のマッピング関係になると思われる(次図参照)。

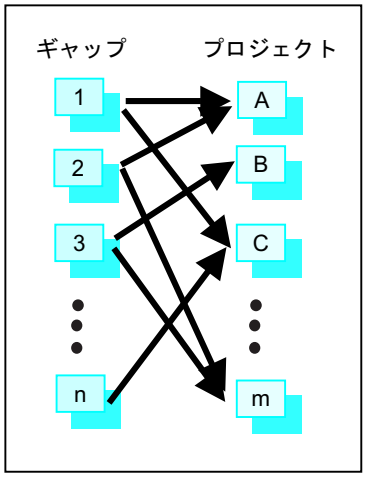
プロジェクトの分類

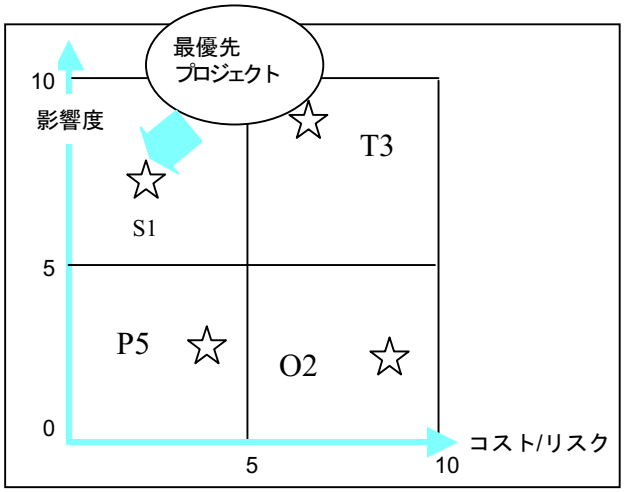
計画立案とコミュニケーションを容易にするために，プロジェクトは，タイプによって分類することが望ましい。戦略上主導的に進めるプロジェクト，戦術的なプロジェクト，組織的な改善のためのプロジェクト，新たな手続を作るプロジェクトである。次の図では，S1，T3，O2，P5 で表されているように，それぞれのプロジェクトにユニークな連番が振られる。

プロジェクト の優先順位付け

プロジェクトに優先順位を付ける目的は，早く成果に結びつくプロジェクトを明確にすることにある。早く成果が出るプロジェクトは，一般にギャップが小さく，低コストで，失敗するリスクが低く，かつ得られる利益は最も大きい。

それゆえ，プロジェクトは，与える影響度とコスト／リスクの両面で分かり，0 から 10 までの評価の物差しを使って評価をしなければならない。プロジェクトは図を使ってプロットされるが，その図では相対的な影響度の大きさやコスト／リスクの指標が，マネジメントにとっての意思決定支援ツールとなる。大きな影響力がありながらコスト／リスクが低いプロジェクトは，早く成果の出るプロジェクトを選定する際の第 1 の候補である。


ギャップ
プロジェクト
1
2
3
n
A
B
C
m


最優先
プロジェクト
10
影響度
5
0
S1
T3
P5
O2
5
10
コスト/リスク

付録 Ⅱ

COBIT のフレームワーク

IT におけるコントロールの必要性

近年，IT におけるセキュリティとコントロールのための参考にすべきフレームワークが必要であることについては，規制者，立法者，利用者およびサービスプロバイダの間でますます明らかになってきている。IT の効果的なマネジメントが，組織の成功と生き残りに関して極めて重要である。 この重大さは， ― 時間，距離，スピードの制約なく情報がサイバースペースを移動するような ― グローバルな情報社会では，以下のことから明らかである。

- 情報およびこの情報伝達するシステムへの依存度の増加
- 脆弱性の増加，サイバー脅威や情報戦争のように広範囲にわたる脅威の増加
- 情報および情報システムに対する現在，将来の投資の規模とコスト
- テクノロジが，組織やビジネス活動を劇的に変えて，新しいビジネス機会を創生したり，コストを削減したりする可能性があること

多くの組織にとって，情報テクノロジは，組織の最も貴重な資産を代表している。事実，情報および情報システムは，利用者のプラットフォームからローカルエリアネットワーク(LAN)やワイドエリアネットワーク(WAN)へ，またクライアントサーバへ，またメインフレームコンピュータへと組織中に広がっている。***多くの組織が，テクノロジから得られる潜在的な効果に気が付いている。 しかしながら，成功した組織は，新しいテクノロジの導入に伴うリスクを理解し，管理している***。このようにマネジメントは，有効な指示や適切なコントロールを行うために，IT のリスクや制約条件について評価し，かつ基本的な理解をしておく必要がある。

マネジメントは，IT のセキュリティとコントロールを確保するために何を投資したらよいのか，また多くの場合，予測が困難な IT 環境の中で，リスクとコントロールに対する投資のバランスをどのように取るかについて決定しなければならない。 情報システムのセキュリティとコントロールは，リスク管理に役立つが，リスクをゼロにするものではない。さらにいえば，ある程度の不確実性が残るため，リスクのレベルについては正確には把握できないのである。 最終的にマネジメントとしては，受け入れられるリスクレベルを決めなくてはならない。特にコストに対して重み付けをする際に受容可能なレベルをどこにおくのかを判断することは，難しい決定になるはずである。 そのために，マネジメントは，現在または将来計画している IT 環境をベンチマークするために，一般的に受け入れられている IT のセキュリティとコントロールの手続が盛り込まれたフレームワークが明らかに必要になってくるのである。

社内やサードパーティによる認証の監査によって，適切なセキュリティとコントロールが確保されていることが保証された IT サービスを望む**利用者**のニーズはますます高まってきている。 しかしながら，現在のところ，情報システムによい IT コントロールを導入することについては，商業ベースで行うべきか，非営利組織で行うべきか，あるいは政府主導で行うべきかについて，混乱が生じている状態である。 混乱の原因は，ITSEC，TCSEC，IS0 9000 の評価，最近現れた COSO 内部統制の評価など異なった評価手法が存

在するためである。結局，利用者には，まず特定の手法に依存しない共通の手法を確立することが必要である。

監査人には，内部統制について評価した結果を報告し，マネジメントに対して実証する義務があるため，国際標準の作成プロジェクトを主導する役割を担ってきている。ある一定のフレームワークなしでは，これは非常に難しい仕事である。このことは，監査人が複雑なセキュリティとコントロールの状況を判断する際の方法について，世界中で並行して行われている最近の研究から明らかになっている。監査人には，今後ますますマネジメントから，IT セキュリティやコントロールに関連する事項に対して，より積極的なコンサルティングや助言を行うことを求められる機会が増えるだろう。

ビジネス環境：競合，変化およびコスト

グローバルな競争が始まっている。 いろいろな組織で，業務合理化のためのリストラクチャリングが開始され，同時に競争優位を獲得するために IT 投資が活発化している。ビジネス・リエンジニアリング，ライトサイジング，アウトソーシング，権限付与(コンパクメント)，フラット化された組織，および分散処理はすべてビジネス組織や政府組織の運営に影響を与えた変化である。世界の組織における，マネジメントレベルのコントロールや，業務運営レベルのコントロールは，このような変化と深いかかわりがあり，今後もこのかかわりは続くことになる。

競争上の優位性を獲得し高いコスト効率性を追求すればするほど，情報テクノロジが組織戦略に占める役割はますます高まることになる。組織機能の自動化は，本質的に，コンピュータやネットワークに，ハードウェアとソフトウェアを使って，より強力なコントロールの仕組みを組み込むことにほかならない。またこの新しいコントロールの基本的な仕組みは，コンピュータやネットワークのテクノロジが進歩するにつれて，同じスピードで“蛙が飛び跳ねる”ように急激に進歩することが特徴である。

急激な変化が日常化している中で，マネージャ，情報システムの専門家，監査人が，本当に効果的な役割を果たすためには，テクノロジやビジネス環境と同じように迅速にスキルアップする必要がある。一般的なビジネス組織や政府組織で見られるコントロール手続の評価に当たり，合理的で慎重な判断をするためには，コントロールが組み込まれたテクノロジやその技術的な進歩についてよく理解しておかなければならない。

ニーズに対する対応

これらの進行中の変化から見て，IT のコントロール目標に関するフレームワークを開発することは，このフレームワークをベースにした IT のいろいろなコントロールに関する継続的な応用研究に加えて，情報テクノロジのコントロールの分野で効果的な進歩を実現する基礎になる。

一方で我々は，アメリカ合衆国の COSO(Treadway 委員会-内部統制とその統合的枠組み，1992 年)，イギリスのキャドバリー委員会，カナダの CoCo，南アフリカのキング報告書に見られるような，包括的にビジネスコントロールモデルを扱った出版物の作成に立ち会ってきている。更に，IT のレベルによって焦点を合わせたコントロールモデルも出現してきている。後者のカテゴリーでのよい事例としては，DTI (貿易産業省，UK)のセキュリティに関する行動規範，CICA(カナダの勅許会計士協会，カナダ)の情報システムコントロールガイドライン，NIST(国立標準技術研究所，アメリカ合衆国)のセキュリティハンドブックが挙げられる。しかしながら，これらのコントロールモデルは，ビジネスプロセスの支援を目的とする IT を管理するために，包括的で使いやすいものにはなっていない。COBIT の目的は，IT に焦点を合わせながら，経営目標と密接にリンクした基盤を作り，ギャップを埋めることである。

(COBIT に最も近いものとしては，最近発表された AICPA/CICA SysTrust™「システムの信頼性に関する原則と規準」がある。SysTrust はアメリカ合衆国の AICPA アシュアランスサービス実行委員会とカナダの CICA アシュアランスサービス開発理事会の両者で公認された正式な出版物であり，COBIT のコントロール目標が部分的に使われている。SysTrust は，ビジネス活動やそれ以外の特定の活動を支援するシステムを提供し，経営者，顧客，ビジネスパートナがより安心して活動できるように設計されている)。

公認会計士が，可用性，セキュリティ，万全性(インテグリティ)，保守性という四つの重要な原則を踏まえて評価を行い，あるシステムの信頼性が高いかどうかを評価する保証(アシュアランス)サービスを提供することが，SysTrust サービスでは必要不可欠となっている。

IT のコントロールに関するビジネスニーズ，新たに生まれたコントロールモデルやそれに関連した国際標準の応用に焦点を当て，監査人のツールであった「コントロール目標」は管理ツールである「COBIT」へと発展した。さらに，マネジメントガイドラインが開発されて，COBIT はさらにレベルアップした。経営者が自社の IT 環境を評価し，情報テクノロジにかかわるコントロールの導入や改善の意思決定ができるように，KGI，KPI，主要成功要因(CSF)，成熟度モデルが盛り込まれた。このような意味で，COBIT は，経営者が IT 関連のリスクを理解し，管理する際に役立ち，IT ガバナンスを大きく進展させたツールといえる。

このことから COBIT プロジェクトの主たる目的は，世界中のビジネス組織，政府組織や専門家組織の賛同を得ながら，セキュリティとコントロールに関する明確な方針と良質な実務慣行を策定することである。主として，経営目標やニーズの視点からこれらのコントロール目標を策定することが本プロジェクトの最終目標であり，(これは内部統制のマネジメントフレームワークを最初に提案し，いまでも主流となっている COSO の考え方に準拠しているものでもある。したがって，コントロール目標は，COSO をベースとして監査目標(財務情報についての証明，有効性，効率性等の内部統制にかかわる指標の証明等)に関する考え方をもとにして策定されている。

読者：経営者，利用者および監査人

COBIT は，3 種類の読者が使えるようにデザインされている。

経営者 ― 予測が困難な IT 環境において，リスクに対するコントロールへの投資がバランスの取れたものとなるように支援する。

利用者 ― 社内 IT 部門やサードパーティによって提供される IT サービスのセキュリティやコントロールについての保証が得られる。

監査人 ― 経営者に対して，内部統制についての意見を証明したり，内部統制に関する助言をする。

上級管理者，監査人，セキュリティやコントロールの専門家といった読者からの直接的なニーズに応えるのとは別に，COBIT は，企業内のビジネスプロセスの責任者が，そのプロセスの情報にかかわるコントロール活動を行う際に利用することもできるし，また企業内の IT 責任者も利用することができる。

経営目標指向

COBIT のねらいは，経営目標を明らかにすることにある。COBIT のコントロール目標は，監査人以外にも，十分意味のある使い方ができるように経営目標との間に明確で詳細な関係付けを行っている。コントロール目標は，ビジネス・リエンジニアリングの原則に従って，プロセス指向の考え方で定義されている。ドメインとプロセスには，上位のコントロール目標があり，理論的に考えられる経営目標への関係付けが行われている。さらに，IT のコントロール目標を定義し，導入するために，留意事項とガイドラインが準備されている。

上位コントロール目標が適用されるドメインの分類(4 ドメインとそれに含まれる 34IT プロセス)，コントロール目標によって大きな影響を受ける IT 資源，そのドメインにおけるビジネス側からの情報ニーズの説明などが一体となって COBIT フレームワークを形成している。 フレームワークには，研究の結果明らかになった 34 の上位コントロール目標と 318 の詳細レベルのコントロール目標が含まれている。フレームワークは IT 業界や監査の専門家に公表し，レビューを受け，実際に活用してもらい，コメントしてもらった。その結果分かったことは適宜修正を加えている。

定義

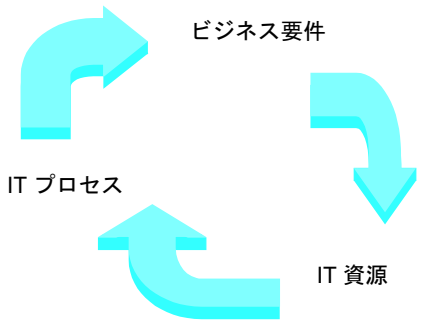
このプロジェクトの目的に沿って，次のような定義が定められた。「コントロール」の定義は，COSO 報告［内部統制の統合的な枠組み，Treadway 委員会，1992 年］をもとに，また「IT のコントロール目標」は SAC 報告［システムの可監査性とコントロールに関する報告，内部監査協会の研究財団，1991 年と 1994 年］をもとにして作成されている。

コントロール	方針，手続，実務慣行および経営目標を達成すること，好ましくない事象の発生を未然に防止すること。たとえそのような事象が発生しても発見し修正することを，合理的に保証できるようにデザインされた組織的体制をさす。
ITのコントロール目標	特定の IT 活動に対して，コントロール手続を導入することによって達成されるべき目的や望ましい結果を記述したものである。
ITガバナンス	企業を動かし，コントロールするためのプロセスとその関係のあり方を指す。その目的は IT や IT プロセスにかかわるリスクとリターン(見返り)のバランスを保ちつつ，企業の最終目標を達成することである。

フレームワークの原則

現在存在するコントロールモデルは，明確に 2 種類に分けられる。「ビジネスコントロールモデル」(例えば，COSO)と，「IT に，より焦点を絞ったコントロールモデル」である(例えば，DTI)。COBIT はこのギャップを橋渡しすることを目指している。したがって COBIT は，一般のマネジメントレベルよりは，扱われている範囲が広く，情報システムの管理のためのテクノロジ標準よりは高いレベルをカバーするものとなっている。このような点から COBIT は，IT ガバナンスのモデルとして適切であるといえる。

COBIT のフレームワークの基本となっているコンセプトでは，IT に関するコントロールを，情報をビジネス目的あるいは要件を支援するために必要なものであると見ると同時に，情報は，IT プロセスによる管理が必要な IT 関連資源を組み合わせた結果として作られるものであると見ることによってとらえられている。



経営目標を満たすためには，COBIT で情報に関するビジネスの要請として参照しているいくつかの情報規準に情報が満たしている必要がある。要請のリストを作り上げるうえで，COBIT では，有名なリファレンスモデルに含まれている原則を組み合わせて用いている。

品質要件	品質 コスト 納期
(一般投資家からの) 受託者の要件 (COSOレポート)	業務の有効性と効率性 情報の信頼性 法律や規則の遵守
セキュリティ要件	機密性 万全性 可用性

品質は，もともと主にネガティブな観点(即ち欠陥のないこと，信頼性など)から理解されており，その多くは万全性規準にも含まれるものである。ただし，品質のポジティブな面は，それほど目に見えないところ(例えば，スタイル，人を引きつける魅力，ルックアンドフィール，期待以上の成果など)は，ここしばらくは IT のコントロール目標の観点から検討されていなかった。 というのは，ビジネス機会の追求より適切なリスク管理を優先することが前提とされているからである。品質の中の操作性の面は，有効性規準でカバーされている。品質の納期の側の面は，セキュリティ要件の可用性とオーバーラップし，有効性，効率性ともある程度オーバーラップすると考えられる。コストの面は，最終的に効率性によってカバーされていると考えられる。

(一般投資家からの)受託の要件については，COBIT では，新たな定義を作ることは行わず，COSO の定義である業務の有効性と効率性，情報の信頼性，法律や規則の遵守をそのまま使っている。ただし，情報の信頼性については，財務情報に限らずすべての情報を含めるように拡大解釈している。

セキュリティ要件に関して，COBIT では，主要な要素として機密性，万全性，可用性を挙げたが，この三つの要素については，全く同じ言葉が IT のセキュリティ要件を記述する際に，世界中で使われていることが分かっている。

品質，受託，セキュリティに関する広義の要件の分析から始めて，部分的にはオーバーラップしているが，七つの独立したカテゴリーを抽出した。COBIT で使われる定義は次のとおりである。

有効性	該当するビジネスプロセスと関係のある有用な情報をあつかうこと，それは，またタイムリに，正確に，首尾一貫して，操作性が確保された形で提供されること。
効率性	資源の最適な(最も生産的かつ経済的に)利用を通じて行われる情報提供にかかわる。

機密性	無許可の開示から機密性が高い情報を保護することにかかわる。
万全性 (インテグリティ)	情報の正確性と完全性，ビジネス価値と期待に見合った情報の正当性にかかわる。
可用性	ビジネスプロセスで必要な情報が今または将来において利用できることに関連する。また，そのために必要な資源や能力の保護にもかかわる。
準拠性	ビジネスプロセスが従わなければならない法律，規制，契約条項の遵守に関することを扱う。すなわち，外部から課されているビジネス規準。
情報の信頼性	マネジメントが組織を運営するために，またマネジメントが財務，法的遵守状況についての報告義務を果たすうえで，適切な情報を提供することに関係する。

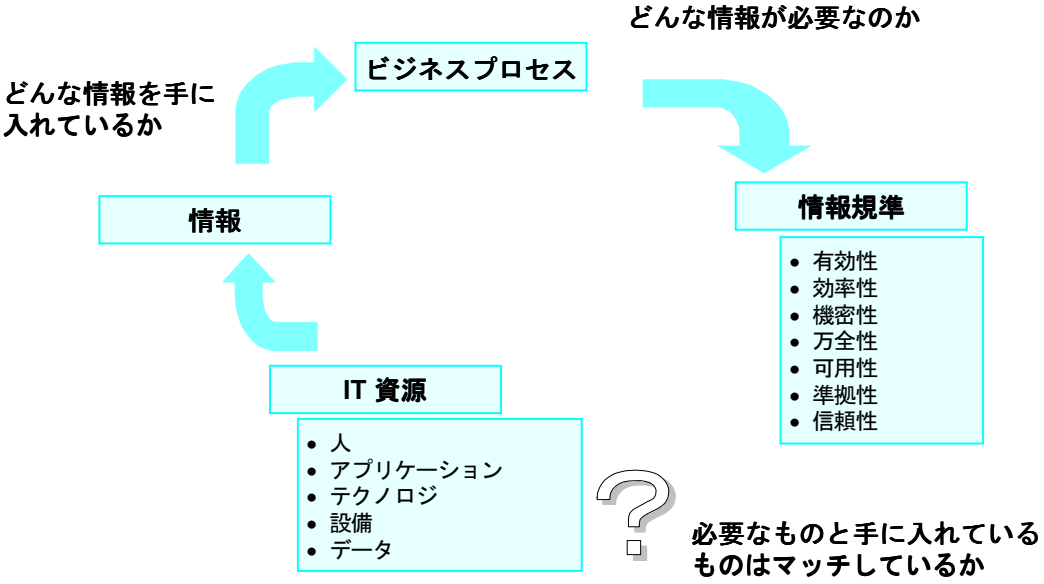
COBIT に示された IT 資源は，次のように説明され，定義される。

データ	最も広い意味におけるオブジェクトであり(外部も内部データも含む)，構造化されているか否か，画像，音等を問わない。
アプリケーション	手作業による手続とプログラム化された手続の集合体として理解される。
テクノロジ	ハードウェア，オペレーティング・システム，データベースマネジメントシステム，ネットワーク，マルチメディアなどを含む。
設備	情報システムを収容(ハウス)，支援するすべての資源である。
人	情報システムやサービスを，計画し，組織化し，調達し，提供し，支援し，モニタリングするために必要なスタッフのスキル，意識，生産性を含めている。

カネや資本が，コントロール目標の分類の中で，IT 資源として扱われていない理由は，上記のすべての資源に投資という形で組み込まれると考えることができるからである。また，このフレームワークでは，ある特定の IT プロセスに関連したすべてのドキュメントを明記しているわけではない点に注意していただきたい。優れた手引きになるものとして，

ドキュメント化は優れたコントロールを行うのに不可欠であると考えられており，ドキュメント化がされていなければ，これを補うためにレビューや分析を追加することが必要となる。

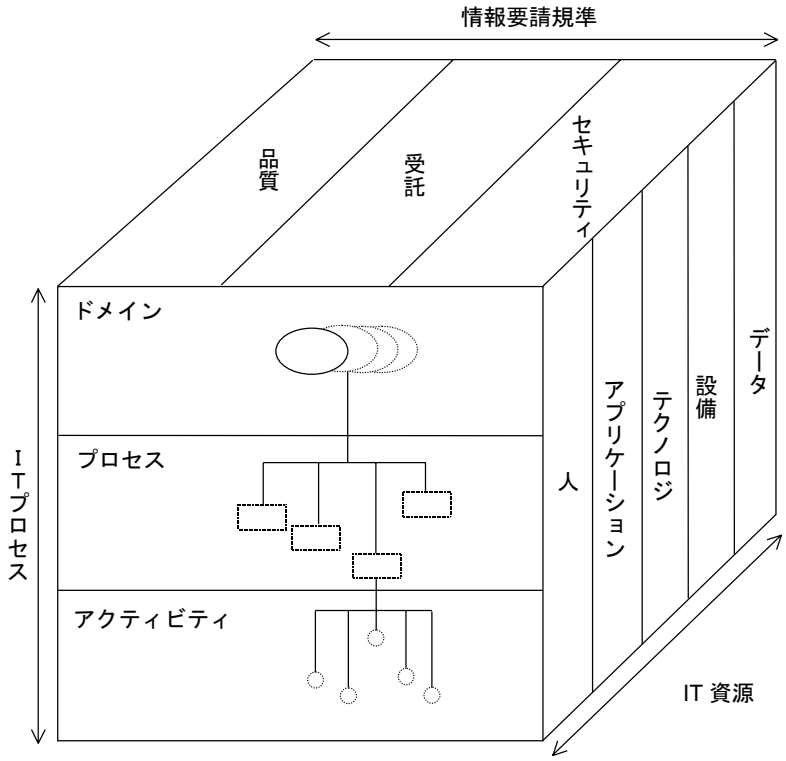
情報についてのビジネス要件が満たされることを保証するために，IT 資源に対する適切なコントロール手段が定義，導入され，モニタリングされる必要がある。 そして，組織に提供される情報が，必要条件を満たしていることをどのように確認すればよいか。これが IT コントロール目標に関する健全なフレームワークが必要とされる理由である。 次の図はこのコンセプトを図解したものである。



COBIT の *フレームワーク*は，上位コントロール目標と，目標を分類するための全体の構造から成り立っている。 分類に関する基本的な考え方は，要するに IT 資源の管理を検討する場合に IT 関連業務を三つのレベルに分けるということである。いちばん下のレベルには，評価ができる成果の達成が求められるアクティビティとタスクがある。タスクには連続性がなく単発的であるが，アクティビティには連続的なライフサイクルがある。ライフサイクルがある場合には，連続性に欠ける場合とは違って，典型的なコントロール要件が必要である。プロセスは，アクティビティより一つ層が上になるレベルで，妥当な(コントロール上の)まとまりを持った一つの関連したアクティビティまたはタスクの集合体として定義されている。最上位レベルでは，プロセスは，自然にいくつかのドメインにグループ化される。このグループ分類は，会社の組織体制における責任範囲を表すドメインとして常に確認されており，マネジメントサイクルや IT プロセスに適用できるライフサイクルと整合性が取れている。

さらに，概念的なフレームワークを，次の三つの視点から検討している。
(1)情報要請規準，(2)IT 資源，(3)IT プロセス。 例えば，マネージャは，品質，受託，セキュリティといった情報要請規準観点から見たいと思うかもしれない(このフレームワークには，七つの特定された情報要請規準が入っている)。ある IT 管理者は，自分に責任がある IT 資源について検討したいと思うかもしれない。プロセスオーナ，IT 専門家や利用

者は，ある特定のプロセス，あるいはアクティビティやタスクに対して，特別な関心を持っているかもしれない。監査人は，コントロールの観点からフレームワークにアプローチしたいと思うかもしれない。これらの三つの視点は，次の COBIT キューブで表現される。



上記のフレームワークの，ドメインの名称には，経営者が日常的に使う用語を使い，監査人の専門用語を使わないようにした。 このようにして，計画と組織，調達と導入，サービス提供とサポート，モニタリングの四つのドメインが定められた。

上位分類のための四つのドメインの定義は次のとおりである。

計画と組織	このドメインは，戦略と戦術を取り扱い，経営目標の達成に IT が最も貢献する方法を明らかにする。さらに，戦略的なビジョンの実現に向かって，計画化され，周知され，いろいろな考え方が統一される必要がある。最終的に，技術的なインフラと同様，適切な組織が適切に編成され，配置されなければならない。
調達と導入	IT 戦略を実現するために，IT 対応策が明らかにされ，開発または調達され，ビジネスプロセスの中に導入・統合されていく必要がある。さらに，既存システムの変更，保守は，このドメインで取り扱われ，システムのライフサイクルを保証する。
サービス提供とサポート	このドメインは，必要なサービスの実際の提供にかかわり，セキュリティや継続性確保等に関する従来業務から研修まで広い範囲にわたっている。サービスを提供するためには，必要な支援プロセスが用意されていなくてはならない。このドメインでは，アプリケーションシステムの実際のデータ処理，よくアプリケーションコントロールといわれているものが含まれている。

モニタリング	すべての IT プロセスでは，将来にわたって定期的に，品質とコントロール要件に関する遵守状況を評価する必要がある。このドメインは，組織内のコントロールプロセスについてのマネジメントの監視活動や，内部，外部監査に，またはそれに代わるものから得られる独立的な保証(アシュアランス)を取り扱う。

これらのプロセスが，会社の組織の中のいろいろな異なるレベルで適用できることに，決定する必要がある。例えば，あるプロセスは企業レベルで適用でき，また別のプロセスは情報サービス部門のレベルで適用でき，また別のプロセスはビジネスプロセスオーナのレベルで適用できる。

また，ビジネス要請に関する対応策の計画または実施プロセスに関する有効性の規準が，時には可用性，万全性，機密性の規準をカバーすることがある点にも注意する必要がある。実際，可用性，万全性，機密性はビジネス要請になってきている。例えば，「対応策を特定する」というプロセスは，可用性，万全性，機密性という要件の提供に有効であるべきである。

すべてのコントロール手段が，情報に関する異なったビジネス要請を，必ずしも同程度に満たす必要がないのは明らかなことである。

- 主(primary)は，
  定義したコントロール目標が，関連する情報規準に直接的な影響を与える程度のものである。

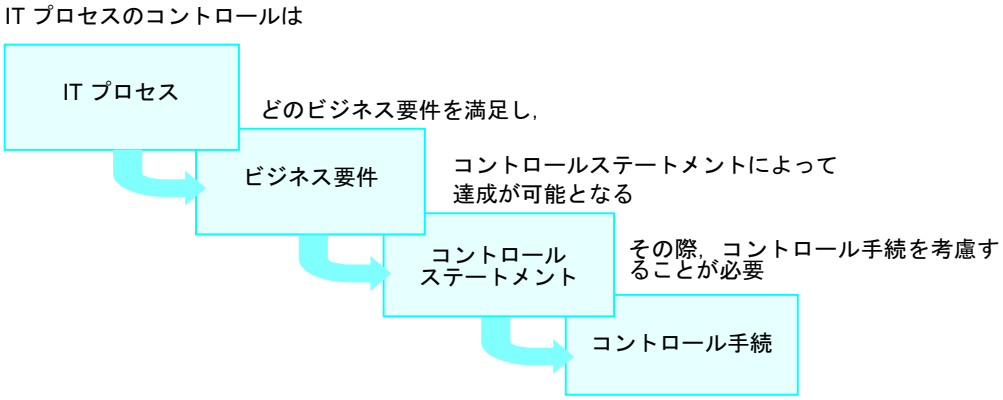
- 準(secondary)は，
  定義されたコントロール目標が，関連する情報規準に対してそれほど大きくはない程度に，あるいは間接的に影響を与える程度のことである。

- 空白(blank)は，
  いろいろな場合があるが，同じプロセス内かまたは別のプロセスにおいて，別の情報規準を当てはめる方がより適切なことを意味している。

同様に，すべてのコントロール手段が，必ずしも同じ程度に，いろいろな IT 資源に影響を与えるわけではない。それゆえ，COBIT のフレームワークでは，プロセスにおける特別な管理が必要 IT 資源(ただ単にプロセスで使われている IT 資源のことではない)の適用可能性を特に表現している。この適用可能性についての区分は，事前に厳密な定義を準備し，研究者，エキスパートやレビューアーに十分なレビューをしてもらったうえで COBIT フレームワークの中で設定したものである。

上位コントロール目標

COBIT フレームワークでは, ある特定の IT プロセスにおけるビジネスニーズという形で上位コントロール目標だけに焦点をあて，その目標の達成を可能にする一つのコントロールステートメントを示し，さらに可能にするために考慮する必要のある潜在的に適用可能なコントロールを示した。

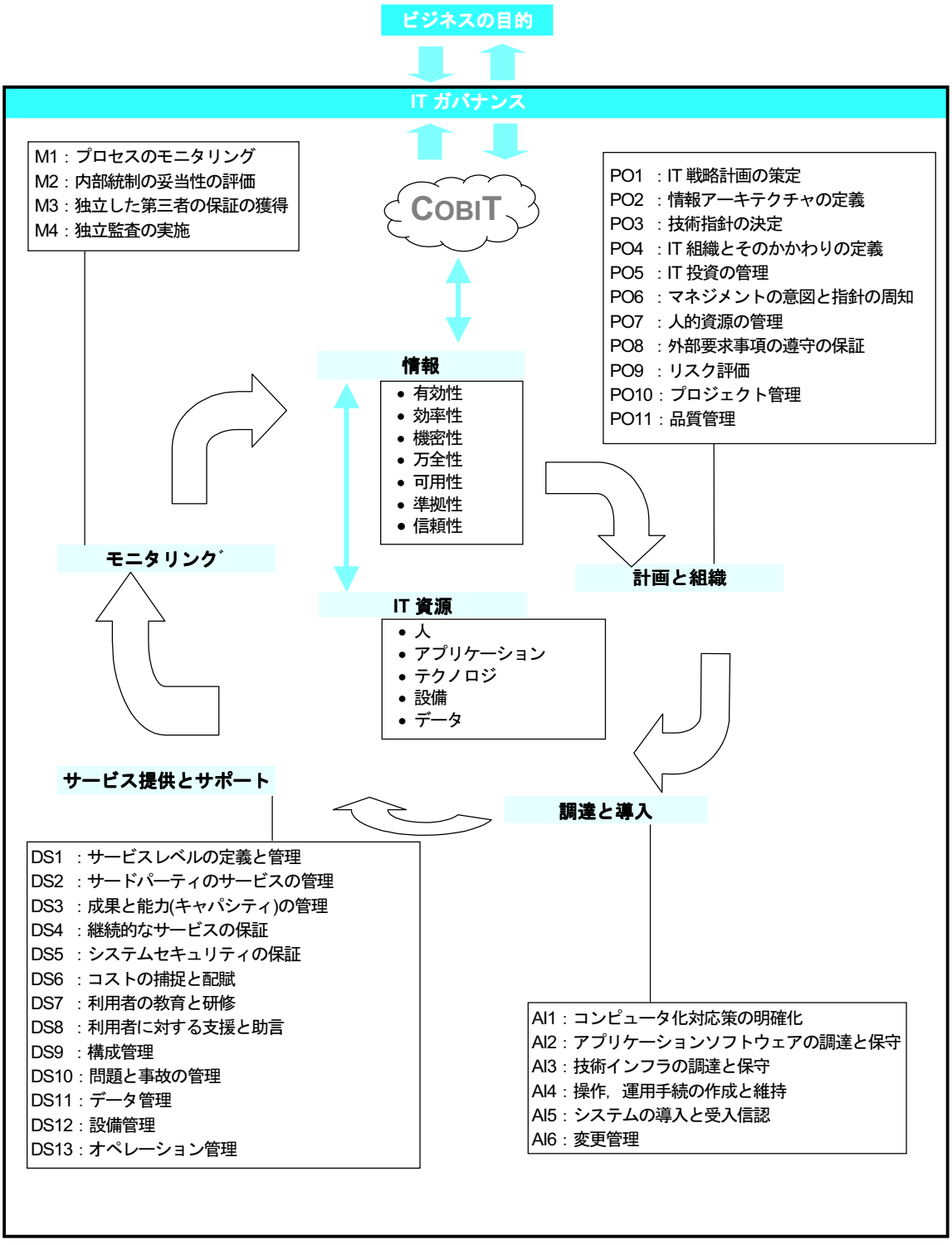


コントロール目標は，組合せやグローバルなアプローチを促進するためにプロセスやアクティビティを中心として形作られてきた。例えばプロセスの導入，適用，プロセスに対するグローバルなマネジメント責任およびプロセスよる IT 資源の利用などである。

コントロール目標では，IT ドメイン，IT 資源，情報に関するビジネス基準を参照できるようにもしている。このことによって，COBIT キューブ(ページ 158 参照)で先に図示したように，三つの視点から IT コントロールの要請を見ることができるようにしている。各上位コントロール目標では，それが属しているドメインを明らかにし，そのドメインに属するプロセスに最も重要な情報規準と，2 番目に重要な情報規準を示し，マネジメントの特別な注意が必要な資源が分かるようにしている。

コントロール目標は，特定の技術プラットフォームに限定しない，一般的な書き方で定義している。しかし，ある特別なテクノロジ環境では，別途異なったコントロール目標を用意する必要が生じることも事実である。

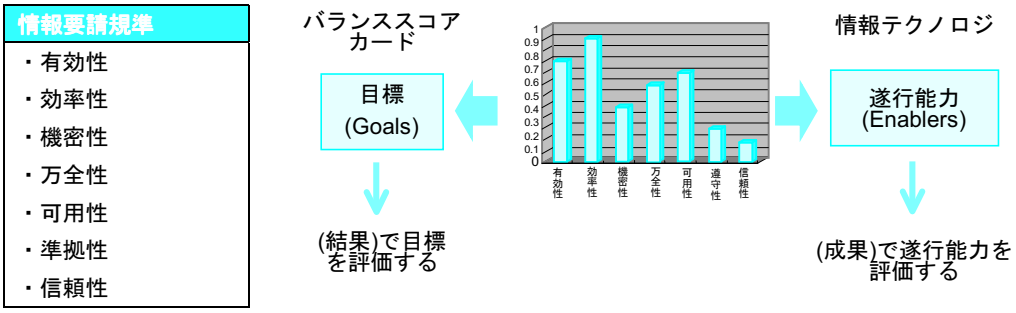
要約すると，組織がその目標を達成するために必要な情報を提供するためには，IT ガバナンスによって，IT 資源が一連の適切な IT プロセスを通じて管理されることが保証されていなければならない。次の図はこのコンセプトを図解したものである。


ビジネスの目的
IT ガバナンス
M1：プロセスのモニタリング
M2：内部統制の妥当性の評価
M3：独立した第三者の保証の獲得
M4：独立監査の実施
COBIT
PO1 ：IT 戦略計画の策定
PO2 ：情報アーキテクチャの定義
PO3 ：技術指針の決定
PO4 ：IT 組織とそのかかわりの定義
PO5 ：IT 投資の管理
PO6 ：マネジメントの意図と指針の周知
PO7 ：人的資源の管理
PO8 ：外部要求事項の遵守の保証
PO9 ：リスク評価
PO10：プロジェクト管理
PO11：品質管理
情報
• 有効性
• 効率性
• 機密性
• 万全性
• 可用性
• 準拠性
• 信頼性
モニタリング
計画と組織
IT 資源
• 人
• アプリケーション
• テクノロジ
• 設備
• データ
サービス提供とサポート
調達と導入
DS1 ：サービスレベルの定義と管理
DS2 ：サードパーティのサービスの管理
DS3 ：成果と能力(キャパシティ)の管理
DS4 ：継続的なサービスの保証
DS5 ：システムセキュリティの保証
DS6 ：コストの捕捉と配賦
DS7 ：利用者の教育と研修
DS8 ：利用者に対する支援と助言
DS9 ：構成管理
DS10：問題と事故の管理
DS11：データ管理
DS12：設備管理
DS13：オペレーション管理
AI1：コンピュータ化対応策の明確化
AI2：アプリケーションソフトウェアの調達と保守
AI3：技術インフラの調達と保守
AI4：操作，運用手続の作成と維持
AI5：システムの導入と受入信認
AI6：変更管理

付録 Ⅲ

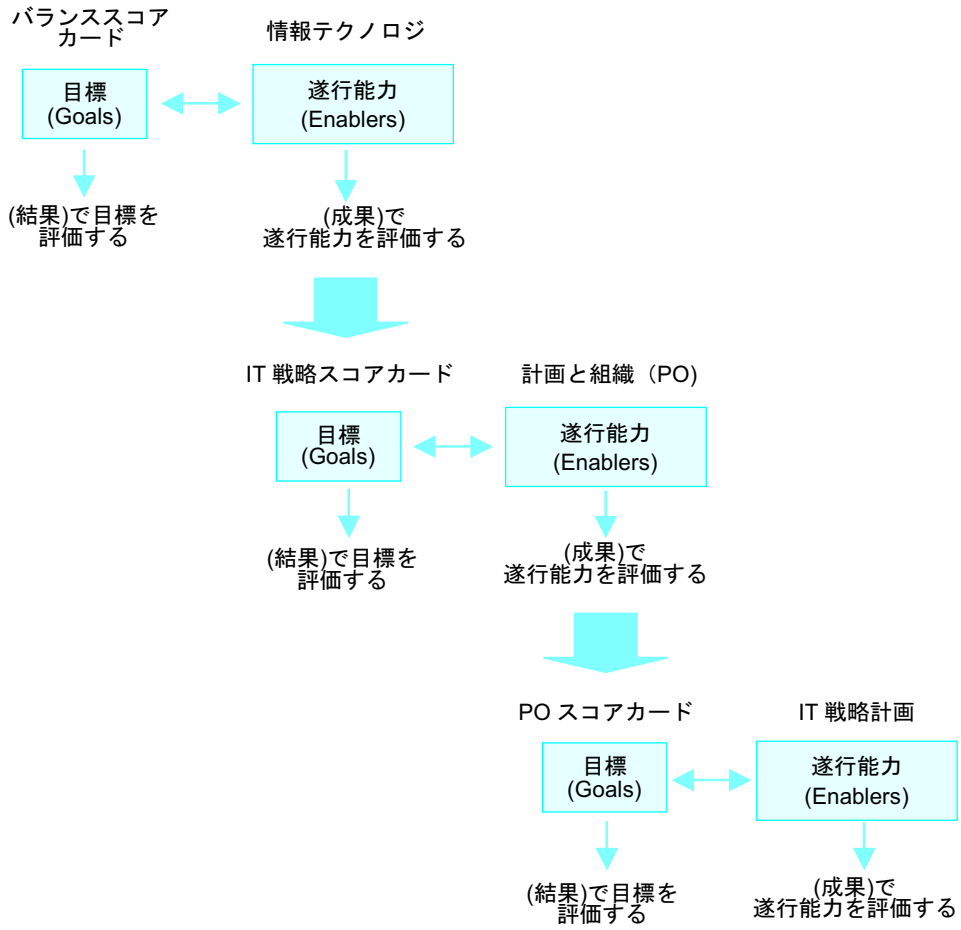
COBIT とバランススコアカード

COBIT フレームワークでは, ビジネスが必要とする情報を IT から提供することによって, ビジネスを遂行すると述べている。したがって，IT の目標とすることは COBIT のフレームワークの中の情報要請規準を用いて評価することができる。



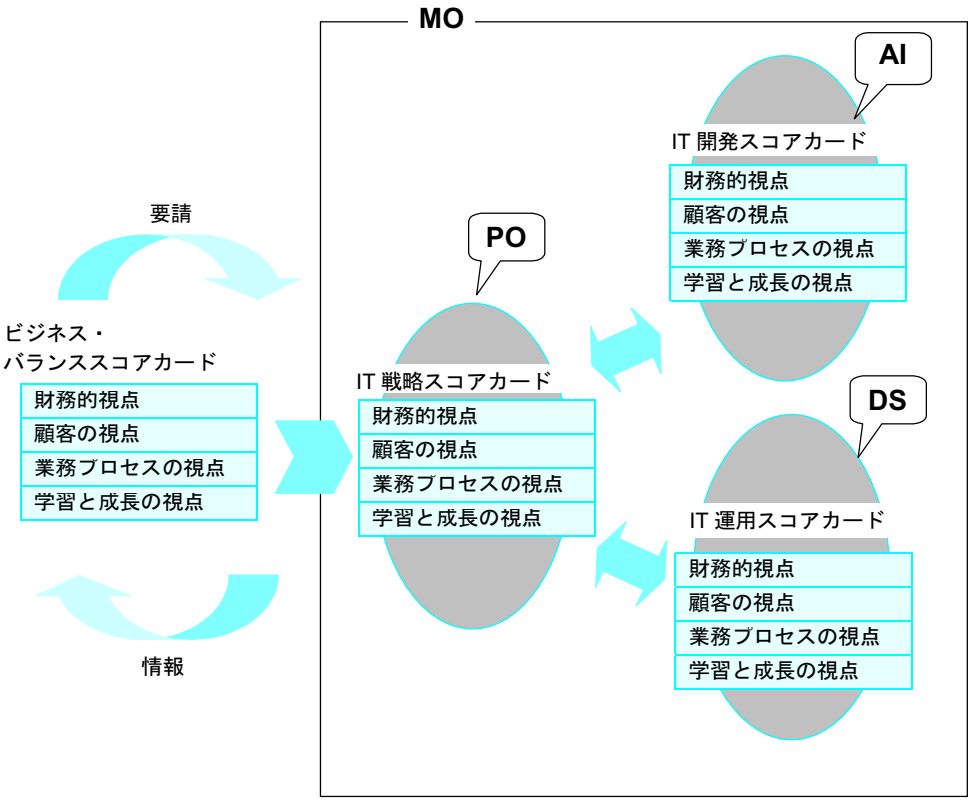
これらの規準の重要性は同等なものでない。重要性は，かかわりのあるビジネスや IT プロセスによって変わってくる。(上図のミニチャートに示された)各規準の相対的な重要度は，ビジネスの期待を表しており，ビジネスを遂行する IT の目標となる。結果や成果を評価するための原則は，バランススコアカードが定めており，マネジメントガイドラインではこの原則を採用している。

遂行能力(Enablers)の成果目標が，IT の目標になり，さらに下位レベルの遂行能力ができるというように，次々に同様のことが繰り返される。この点は，COBIT のドメインにも同じことがいえる。ドメインの成果目標は，プロセスの結果目標として落とし込まれる関係になっている。



このような関係を見るもう一つの視点がある。それはビジネスのバランススコアカードの四つの次元からスタートし，IT がビジネス遂行し，それを IT 戦略のバランススコアカードによってモニタする方法である。IT の戦略目標を実現するためには，開発のスコアカード，運用のスコアカードを作成し，責任範囲を異なった二つのドメイン区分するのが一般的である。

COBIT フレームワークが特定した四つの IT ドメインを用いて容易にこれらのスコアカードをマッピングすることができる。計画と組織(PO)は，IT 戦略のバランススコアカードの評価指標を，調達と導入(ＡＩ)は，開発のスコアカードの評価指標を，サービス提供とサポート(DS)は，運用のスコアカードの評価指標を提供する。ドメイン全体をカバーするのが，モニタリング(MO)であり，マネジメント活動の監視や評価を通じて，また監査や保証を通して，企業全体の IT ガバナンスを実現するものである。


MO
AI
IT 開発スコアカード
財務的視点
顧客の視点
業務プロセスの視点
学習と成長の視点
要請
PO
ビジネス・
バランススコアカード
財務的視点
顧客の視点
業務プロセスの視点
学習と成長の視点
IT 戦略スコアカード
財務的視点
顧客の視点
業務プロセスの視点
学習と成長の視点
DS
IT 運用スコアカード
財務的視点
顧客の視点
業務プロセスの視点
学習と成長の視点
情報

付録 Ⅳ

汎用的なプロセスマネジメントガイドライン

特定の企業目標を目指す IT プロセスと活動に対するコントロールは，

当該ビジネスが掲げる情報要請基準(*1)を満たす情報が提供されることを，別掲(*4)重要目標達成指標(KGI)を用いて評価することによって確実にすることである。

これは，そのビジネスにとって卓越したプロセスや適切なコントロールの仕組みを作り，維持することによって可能となる。

その際に考慮すべき事項として，特定の IT 資源(*2)に影響を与える別掲(*3)の主要成功要因(CSF)があり，その評価には重要成果達成指標（KPI)を用いる。

情報要請規準(*1)
有効性
効率性
機密性
万全性
可用性
準拠性
信頼性

IT 資源(*2)
人
アプリケーション
テクノロジ
設備
データ

主要成功要因(CSF)*3

- IT 成果は，顧客満足度との関係，プロセスの有効性，将来の能力に関する数値化された指標で評価され，IT 管理者は，この評価に基づいて報酬が支払われる。
- プロセスは，IT 戦略や企業目標と整合性が取られている。プロセスには，拡張性があり，その資源は適切に管理され，強化されている。
- プロセスに関与している全員が，プロセス目標に焦点を当てた活動を行っている。また，利用者，内部プロセス，意思決定の結果に関する適切な情報は十分に共有化されている。
- 継続的なプロセス改善が奨励され，組織横断的な協力やチームワークが奨励されるような，企業文化が確立している。
- コントロールの手続は，透過度の向上や，複雑性の低減に役立ち，また学習の活性化，柔軟性や拡張性の向上に貢献している。
- ゴールや目標は，すべての研修を通じて周知され，理解されている。
- プロセス目標の設定と，モニタリングの方法，プロセスの成果責任者が周知されている。
- プロセスについての間断のない品質改善の努力が行われている。
- プロセスの利用者が誰であるか，明確になっている。

- スタッフとしての必要条件(研修，情報の伝達，モラルなど)や，スキル開発の方法(リクルート，内部育成，再研修)が，明確になっている。

重要目標達成指標(KGI) *4

- 提供するサービスレベルの向上
- 利用者数および利用者１人当りのコスト
- システムとサービスの可用性
- 万全性の欠如と機密性にかかわるリスク
- プロセスとオペレーションのコスト効率性
- 信頼性と有効性の確認
- 開発コストと開発スケジュールの遵守
- プロセスのコスト効率性
- スタッフの生産性とモラル
- プロセスやシステムに対するタイムリな変更の数
- 生産性の改善(例えば，従業員別の付加価値)

重要成果達成指標(KPI) *5

- システム故障時間
- スループットとレスポンスタイム
- エラーややり直しの量
- 新しいテクノロジやカスタマサービスの研修を受講したスタッフの数
- ベンチマーク比較
- 内容や形式などが不十分なレポートの数
- 開発時間，運用時間の削減

汎用的なプロセス成熟度モデル

特定の企業目標を持つ IT プロセスと活動に関するコントロール

0：不在

コントロールとして識別可能なプロセスが完全に欠落している。組織は，認識すべき問題があることさえ意識していない。

1：初期／その場対応

組織にコントロール上の問題が存在し，対応が必要なことを認識している証拠はある。しかしながら，標準化されたプロセスはなく，その代わりに個人ベースか，ケースバイケースのその場対応的なアプローチがなされている。マネジメント活動に理路整然としたところはなく，問題や対応方法についてのコミュニケーションは，散発的に行われるだけであり首尾一貫したものではない。

2：再現性はあるが，直観的

問題に対する全社的な認識はある。よく似たインフォーマルで直観的な手続が並存し，同じタスクが別々の担当者によってフォローされ，共通ツールがやっと現れてきた状況

である。したがって，これらのプロセスは再現性があり，一部ではモニタリングも開始されている。標準的な手続についての正式な研修やコミュニケーションの場はなく，実施責任は個人に任されている。個人の知識への依存度が高く，そのためミスも起きやすい。しかしながら，全社的な問題とその対応の必要性については，首尾一貫したコミュニケーションがなされている。

3：定められたプロセスがある

アクションを取らなければいけない必要性は，組織の中で理解され，受け入れられている。手続は，標準化され，文書化されて実行されている。手続は，周知され，インフォーマルであるが研修が確立している。手続は改善されたものではなく，既存の手続を正式化したものである。ツール類は，現在利用できる手法で標準化されている。IT 専門家は，正式化にかかわっているが，IT 専門家でない内部の専門家は，ほとんど参加していない。標準手続の遵守や適用のための研修の受講は個人に任せられている。プロセスの多くは，定められた評価尺度に基づいてモニタリングされているが，乖離が生じた場合，大半は個人主導による対応がなされるが，すべての乖離がマネジメントによって検出される可能性は低い。根本的原因分析は，たまにしか行われない。

4：管理，測定されている

組織のすべてのレベルの問題は完全に理解されており，正式な研修による支援体制も整っている。責任範囲は，明確に定められ，プロセスのオーナーシップが確立している。手続に対する遵守状況をモニタリングしたり，評価尺度をもとにして評価したりすることは可能であり，プロセスが効果的に，あるいは効率的に機能していないと思われる部門に対して必要なアクションを取ることが可能になっている。多くのケースでは必要なアクションが取られているが，すべてのケースに対して取られているわけではない。成果の評価尺度は，まだ伝統的な財務やオペレーションに偏った指標が使われているが，新しい規準が次第に導入され始めている。プロセスは時折改善され，社内のベストプラクティスが全社展開されている。根本的原因分析は標準化されつつある。継続的な改善活動も行われるようになり始めた。コントロール手続は，透明性がますます向上し，フレキシブル，かつ拡張性を持つようになってきている。成熟度の高いテクニックや使いこなされた標準ツール類をテクノロジ基盤としており，新しいテクノロジについては限定的，かつ戦術的な利用にとどめている。IT 戦略と企業戦略との関係はますます深くなっている。社内の各分野の専門家は，要請のある場合はいつも参画する体制となっている。

5：最適化

問題と解決策に関して，高度で，かつ前向きに理解されている。研修やコミュニケーションには，最先端のコンセプトと手法が使われている。ゴールや目標は，成果をモニタするための KGI，CSF，KPI を通して，部門をまたがって共有化されている。プロセスは，間断のない改善や他の組織の成熟度をモデルにするなどの結果，社外のベストプラクティスのレベルにまで高められている。またこの結果，迅速に適応する組織，ヒト，プロセスが生み出されている。IT 戦略は完全に企業戦略と整合性が取られており，ビジネスプロセスの改善や新しいビジネス機会を創出することに，IT 組織を関与させるような企業文化が確立している。すべての問題や乖離は根本原因から分析され，適切に特定

された効率的なアクションが開始される。IT は，広範囲で，統合的，かつ最適な方法で，ワークフローを自動化したり，品質や有効性を向上させるツールを提供するなど，戦略的にテクノロジを強化するために使われる。社外のエキスパートが動員され，ガイドラインとしてベンチマークが利用されている。コントロールの手続は全社に展開され間断なく改善が行われている。IT 成果の評価指標には，財務的な規準，顧客満足度，オペレーションの有効性，将来の能力開発などが挙げられている。IT 管理者の報酬には，企業ゴール達成時のインセンティブも含んでいる。

付録 V

IT ガバナンスに関するマネジメントガイドライン

リスクとリターン(見返り)のバランスを取りつつ, 企業価値を増大させる企業目標を達成するための情報テクノロジとそのプロセスに対するガバナンスは,

当該ビジネスが掲げる**情報要請規準**(*1)を満たす情報が提供されることを，別掲(*4)の**重要目標達成指標(KGI)**を使って評価される。

また，KGI の達成はそのビジネスにとって卓越したプロセス，コントロールの仕組みを作り，維持するとともに，IT によるビジネス価値の提供を方向付け，モニタリングすることによって可能となる。

その際に考慮すべき事項として，すべての **IT 資源**(*2)に影響を与える別掲(*3)の**主要成功要因(CSF)**があり，その評価には，**重要成果達成指標(KPI)** (*5)を用いる。

情報要請規準(*1)
有効性
効率性
機密性
万全性
可用性
準拠性
信頼性

IT 資源(*2)
人
アプリケーション
テクノロジ
設備
データ

主要成功要因(CSF)*3

- IT ガバナンス活動は，全社のガバナンスプロセスの一部に位置付けられ，経営トップのリーダーシップが発揮されるものであること
- IT ガバナンスに焦点を当てるのは，企業の最終目標や，戦略的で主導的な活動，またビジネスを拡大するためのテクノロジの活用，ビジネスニーズを満たすために十分な資源や能力を確保することにある。
- IT ガバナンス活動は明確な目的を持って定義され，文書化され，実行されている。その活動は企業ニーズを反映するとともに，明確な責任が定められている。
- マネジメント手続が，資源をより効率的かつ最適に使用できるよう，また IT プロセスの有効性を向上するように策定され，導入されている。
- 組織内の管理手続が確立され，次のようなことが実現されている。適正な監視活動，コントロール環境／コントロールに対する企業風土，標準的な手続をもとにしたリスクアセスメント，確立された標準の遵守，欠陥やリスクのコントロールに対するモニタリングやフォローアップなど
- 内部統制や監視活動における事故を未然に防止するためのコントロールの手続が定められている。

- 問題管理，変更管理，構成管理のように，複雑化する IT プロセスを統合化し，プロセス間相互のやりとりが円滑に行われている。
- 監査委員会が監査計画を推進する際，特に IT に焦点を当てるために独立した監査人の指名と監督を行うとともに，監査やサードパーティレビューの結果をレビューする体制が確立している。

重要目標達成指標(KGI)*4

- 成果，コスト管理の改善
- 主要な IT 投資に関する収益性の改善
- マーケットへの上市時間の改善
- 品質，イノベーション，リスク管理の改善
- ビジネスプロセスを適切に統合化，標準化すること
- 新規顧客の獲得と既存顧客の満足度向上
- 適切なネットワーク，コンピュータパワーとデリバリーのメカニズム
- 予算どおり納期どおりに，特定プロセスのカスタマの要求事項や期待を満たすこと
- 法律，規制，業界標準，契約条項の遵守
- リスクを取る場合の手続の透明性，正式なリスクプロファイルの遵守
- IT ガバナンスの成熟度に関するベンチマーク比較
- 新しいサービス提供チャネルの開発

重要成果達成指標(KPI)*5

- IT プロセスのコスト効率性の改善(コスト対成果物)
- プロセス改善に関する IT 部門の主導的な活動が増加した数
- IT インフラの利用度の向上
- 利害関係者の満足度の向上(サーベイとクレーム数)
- スタッフの生産性(成果物の数)，モラルの改善(モラル調査)
- 企業管理のための知識や情報の可用性の向上
- IT ガバナンスと企業ガバナンスの間の連携の向上
- IT バランススコアカードによって明確化される成果の向上

IT ガバナンス成熟度モデル

リスクとリターン(見返り)のバランスを取りながら，企業価値を増大させるという企業目標を目的とする情報テクノロジと関連プロセスに対するガバナンスである。

0：不在

IT ガバナンスプロセスに関する意識は全くない。組織には，対応すべき問題があることの認識さえなく，このような問題がコミュニケーションされたことはない。

1：初期／その場対応

組織に IT ガバナンス上の問題が存在し，対応が必要なことを認識している証拠はある。しかしながら，標準化されたプロセスはなく，その代わりに個人ベースがケースバイケースのその場対応的なアプローチがなされている。マネジメントの活動に理路整然

としたところはなく，問題やその対応方法についてのコミュニケーションは散発的に行われるだけであり，首尾一貫したものではない。IT に関連のある企業プロセスの成果指向の成果の一部として，IT の価値がいくらか認識されるようになっている。しかし，標準的なアセスメントのプロセスは存在しない。IT モニタリングは，組織に損失や被害をもたらす事故が発生した際に，受動的に行われるだけである。

2：再現性はあるが，直観的

IT ガバナンスに関するグローバルな認識はある。IT ガバナンス活動，KPI は，現在策定中であり，それには IT 計画，提供，モニタリングのプロセスが含まれている。努力の結果が一部認められ，IT ガバナンス活動は，積極的な上級管理者の関与と監督のおかげで，正式な変更管理プロセスに組み込まれている。選択されたいくつかの IT プロセスは，中核となる企業プロセスの改善やコントロールのためのものとして認知されており，投資の対象として効果的に計画化，モニタリングがなされ，定められた IT アーキテクチャのフレームワークから生み出されるものである。マネジメントは，IT ガバナンスの基本的な成果指標や評価方法を決めているが，このプロセスは他の組織では十分に認知されていない。ガバナンスの標準については，正式な研修や周知徹底はされておらず，実行責任は担当者個人に委ねられている。担当者個人が，さまざまな IT プロジェクトやプロセスの中にガバナンスプロセスを組み込んで指定している。ガバナンスの評価指標を収集するために，特定のガバナンスツールが選ばれ導入されているが，使いこなすための専門的知識が欠如しているためにそのツールが十分に活用されていない可能性がある。

3：定められたプロセスがある

IT ガバナンスに関連する活動の必要性については，理解され，受け入れられている。いくつかの IT ガバナンスの指標を合わせた基準(ベースライン)が策定されており，その中で成果の指標と成果向上(成果ドライバ)の関係が定義され，文書化され，戦略計画，オペレーショナル計画，モニタリングプロセスと統合化されている。手続は，標準化され，文書化され，導入されている。マネジメントによって標準化された手続が周知されており，インフォーマルであるが研修は確立されている。すべての IT ガバナンス活動に関する成果指標は，記録され，追跡されて企業全体の改善につなげられている。手続は評価可能ではあるが，改善されておらず，既存の手続を正式化したものに過ぎない。ツールは，現在利用可能な技術を使って標準化されている。IT バランススコアコアカードの考え方が，取り入れられつつある。しかしながら，研修の受講，標準の遵守と適用は，担当者個人に委ねられている。根本的な原因分析は，まれに行われるだけである。多くのプロセスは，ある(例えば，基準(ベースライン)の)評価尺度に基づいてモニタリングされているが，乖離が生じた場合には，担当者個人の主導によってアクションが取られる。乖離が，マネジメントによって検知される可能性はほとんどない。にもかかわらず，キープロセスの成果に関する全体的な責任範囲は明確であり，マネジメントの報酬は主要な成果の業績評価に基づいて支払われている。

4：管理，測定されている

正式な研修を通じて，すべてのレベルの従業員が，IT ガバナンスの問題について十分に理解している。利用者は誰になるのかについて明確な理解があり，責任範囲は明確に

定義され，サービスレベルアグリーメントを通じてモニタリングされる仕組みがある。責任は明確にされ，プロセスのオーナーシップが確立している。IT プロセスは，ビジネスや IT 戦略と整合性が取られている。IT プロセスの改善は，基本的には定量的な判断に基づいて行われ，手続やプロセスの評価尺度に対する遵守性をモニタリングし，計測することは可能になっている。すべてのプロセスの利害関係者は，リスクや IT の重要性，IT のもたらすビジネスチャンスに気が付いている。マネジメントは，プロセスが運営されるべき許容範囲を定めている。多くの場合にはアクションが取られるが，効果的，効率的に機能していないと思われるプロセスのすべてに対してアクションが取られるわけではない。プロセス改善は時折り行われており，社内のベストプラクティスが全社に展開されている。根本的な原因分析は標準化されつつある。継続的な改善が常時行われ始めている。成熟度の高い技法や全社的な標準ツールをベースにしているので，テクノロジは限定的で，基本的には戦術的な使い方になっている。社内のすべての分野から必要なエキスパートが関与する仕組みがある。IT ガバナンスは，企業全体のガバナンスプロセスへと進化している。IT ガバナンス活動は，企業全体のガバナンスプロセスに統合化されている。

5：最適化

IT ガバナンス上の問題や解決策に関して高度かつ前向きに理解をしている。研修とコミュニケーションは，最先端のコンセプトと技法によって支援されている。プロセスは，常時行われている改善や社外の組織の成熟度モデルをベースに，社外のベストプラクティスと同じレベルにまで高められている。

これらの方針を導入し，組織，従業員，業務プロセスが，IT ガバナンスの要求事項に迅速に対応し，十分それを支援する仕組みになっている。発生したすべての問題や乖離について根本的な原因が分析され，まず効率のよいアクションが特定され，直ちに実行されている。

IT は，広範囲に統合化され，最適な方法で，品質や有効性を改善するためにワークフローを自動化し，ツールを提供する目的で利用されている。IT プロセスのリスクとリターンは明確に定義され，バランスが取られており，企業全体に周知されている。社外のエキスパートが動員され，ガイドラインとしてベンチマークが実施されている。モニタリング，セルフアセスメント，およびガバナンス上期待される事項の伝達は，組織に行きわたっており，計測し，分析し，コミュニケーションや研修を支援するためのテクノロジが適切に使用されている。企業ガバナンスと IT ガバナンスは戦略的な関係を持ち，両者が企業の競争優位性を向上させるために，テクノロジ，人的資源，財務的資源に影響を与えている。