GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

IT ASSURANCE GUIDE

USING COBIT®

ITガバナンスとIT統制の保証の必要性
COBIT®フレームワーク
IT統制の保証アプローチ
COBITはIT統制の保証活動をどのように支えるか

ITガバナンス協会

ITガバナンス協会(ITGITM) (*www.itgi.org*)は、企業の情報技術の方向性とコントロールに関する国際レベルでの議論と標準化を推進するため1998年に設立された。効果的なITガバナンスは、ITによるビジネス達成目標のサポート、ITへのビジネス投資の最適化、およびITにかかわるリスクと機会の適切な管理を確実に保証する上で有用である。ITガバナンス協会は、企業のリーダーや取締役会がITガバナンスにおける責務を果たす上で役立つ独自の調査内容、電子資料、および事例研究内容を提供している。

免責事項

ITGIは、主として専門家への教育目的で、本著作物を作成したものです。ITGIは本著作物の使用に関し、如何なる責任も負いません。本著作物の正確性、完全性、最新性、商用性その他本著作物の使用者の特定の目的に合致することを、一切保証するものではありません。 本著作物の使用は、本著作物の使用者の一切の責任において使用して下さい。

著作権

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

The responsibility for this Japanese translation: ITGI Japan is fully responsible for the quality of Japanese translation of this work.

この翻訳に関する品質については日本 IT ガバナンス協会が全ての責任を負う。

ISBN 1-933284-74-9
IT Assurance Guide: Using COBIT®
Printed in the United States of America

ACKNOWLEDGEMENTS

IT Governance Institute wishes to recognise:

Project Managers and Thought Leaders
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium

Workshop Participants and Expert Reviewers
Mark Adler, CISA, CISM, CIA, CISSP, Allstate Insurance Co., USA
Peter Andrews, CISA, CITP, MCMI, PJA Consulting, UK
Georges Ataya, CISA, CISM, CISSP, MSCS, PBA, Solvay Business School, Belgium
Gary Austin, CISA, CIA, CISSP, CGFM, KPMG LLP, USA
Gary S. Baker, CA, Deloitte & Touche, Canada
David H. Barnett, CISM, CISSP, Applera Corp., USA
Christine Bellino, CPA, CITP, Jefferson Wells, USA
John W. Beveridge, CISA, CISM, CFE, CGFM, CQA, Massachusetts Office of the State Auditor, USA
Alan Boardman, CISA, CISM, CA, CISSP, Fox IT, UK
David Bonewell, CISA, CISSP-ISSEP, Accomac Consulting LLC, USA
Dirk Bruyndonckx, CISA, CISM, KPMG Advisory, Belgium
Don Caniglia, CISA, CISM, USA
Luis A. Capua, CISM, Sindicatura General de la Nacion, Argentina
Boyd Carter, PMP, Elegantsolutions.ca, Canada
Sean V. Casey, CISA, CPA, Ernst & Young LLP, USA
Sushil Chatterji, Edutech, Singapore
Ed Chavennes, CISA, Ernst & Young LLP, USA
Christina Cheng, CISA, CISSP, SSCP, Deloitte & Touche LLP, USA
Dharmesh Choksey, CISA, CPA, CISSP, PMP, KPMG LLP, USA
Jeffrey D. Custer, CISA, CPA, CIA, Ernst & Young LLP, USA
Beverly G. Davis, CISA, Federal Home Loan Bank of San Francisco, USA
Peter De Bruyne, CISA, Banksys, Belgium
Steven De Haes, University of Antwerp Management School, Belgium
Philip De Picker, CISA, MCA, National Bank of Belgium, Belgium
Kimberly de Vries, CISA, PMP, Zurich Financial Services, USA
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA
Zama Dlamini, Deloitte & Touche, South Africa
Troy DuMoulin, Pink Elephant, Canada
Bill A. Durrand, CISA, CISM, CA, Ernst & Young LLP, Canada
Justus Ekeigwe, CISA, MBCS, Deloitte & Touche LLP, USA
Rafael Fabius, CISA, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Christopher Fox, ACA, USA
Bob Frelinger, CISA, Sun Microsystems Inc., USA
Zhiwei Fu, Ph. D, Fannie Mae, USA
Monique Garsoux, Dexia Bank, Belgium
Edson Gin, CISA, CFE, SSCP, USA
Sauvik Ghosh, CISA, CIA, CISSP, CPA, Ernst & Young LLP, USA
Guy Groner, CISA, CIA, CISSP, USA
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Benjamin K. Hsaio, CISA, Federal Deposit Insurance Corp., USA
Tom Hughes, Acumen Alliance, Australia
Monica Jain, CSQA, Covansys Corp., US
Avinash W. Kadam, CISA, CISM, CBCP, CISSP, MIEL e-Security Pvt. Ltd., India
John A. Kay, CISA, USA
Lisa Kinyon, CISA, Countrywide, USA
Rodney Kocot, Systems Control and Security Inc., USA
Luc Kordel, CISA, CISM, CISSP, CIA, RE, RFA, Dexia Bank, Belgium
Linda Kostic, CISA, CPA, USA

John W. Lainhart IV, CISA, CISM, IBM, USA
Lynn Lawton, CISA, BA, FCA, FIIA, PII, KPMG LLP, UK
Philip Le Grand, Capita Education Services, UK
Elsa K. Lee, CISA, CISM, CSQA, AdvanSoft International Inc., USA
Kenny K. Lee, CISA, CISSP, Countrywide SMART Governance, USA
Debbie Lew, CISA, Ernst & Young LLP, USA
Bjarne Lonberg, CISSP, A.P. Moller-Maersk A/S, Denmark
Donald Lorete, CPA, Deloitte & Touche LLP, USA
Addie C.P. Lui, MCSA, MCSE, First Hawaiian Bank, USA
Charles Mansour, CISA, Charles Mansour Audit & Risk Service, UK
Mario Micallef, CPAA, FIA, National Australia Bank Group, Australia
Niels Thor Mikkelsen, CISA, CIA, Danske Bank, Denmark
John Mitchell, CISA, CFE, CITP, FBCS, FIIA, MIIA, QiCA, LHS Business Control, UK
Anita Montgomery, CISA, CIA, Countrywide, USA
Karl Muise, CISA, City National Bank, USA
Jay S. Munnelly, CISA, CIA, CGFM, Federal Deposit Insurance Corp., USA
Orillo Narduzzo, CISA, CISM, Banca Popolare di Vicenza, Italy
Sang Nguyen, CISA, CISSP, MCSE, Nova Southeastern University, USA
Anthony Noble, CISA, CCP, Viacom Inc., USA
Ed O'Donnell, Ph.D., CPA, University of Kansas, USA
Sue Owen, Department of Veterans Affairs, Australia
Robert G. Parker, CISA, CMC, FCA, Robert G. Parker Consulting, Canada
Bart Peeters, PricewaterhouseCoopers LLP, Belgium
Thomas Phelps IV, CISA, PricewaterhouseCoopers LLP, USA
Vitor Prisca, CISM, Novabase, Portugal
Claus Rosenquist, CISA, TrygVesata, Denmark
Jaco Sadie, Sasol, South Africa
Max Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Craig W. Silverthorne, CISA, CISM, CPA, IBM Business Consulting Services, USA
Chad Smith, Great-West Life, Canada
Gustavo A. Solis, CISA, CISM, Grupo Cynthus, Mexico
Roger Southgate, CISA, CISM, FCCA, CubeIT Management Ltd., UK
Paula Spinner, CSC, USA
Mark Stanley, CISA, Toyota Financial Services, USA
Dirk Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA
Scott L. Summers, Ph.D., Brigham Young University, USA
Lance M. Turcato, CISA, CISM, CPA, City of Phoenix IT Audit Division, USA
Ingvar Van Droogenbroeck, PricewaterhouseCoopers, Belgium
Wim Van Grembergen, Ph.D., University of Antwerp Management School, Belgium
Johan Van Grieken, CISA, Deloitte, Belgium
Greet Volders, Voquals NV, Belgium
Robert M. Walters, CISA, CPA, CGA, Office of the Comptroller General, Canada
Tom Wong, CISA, CIA, CMA, Ernst & Young LLP, Canada
Amanda Xu, CISA, PMP, KPMG LLP, USA

The following professors and students for their work on the COBIT 4.1 control practices and assurance test steps
Scott L. Summers, Ph.D., Brigham Young University, USA
Keith Ballante, Brigham Young University, USA
David Butler, Brigham Young University, USA
Phil Harrison, Brigham Young University, USA
William Lancaster, Brigham Young University, USA
Chase Manderino, Brigham Young University, USA
Paul Schneider, Brigham Young University, USA
Jacob Sperry, Brigham Young University, USA
Brian Updike, Brigham Young University, USA

ACKNOWLEDGEMENTS

ITGI Board of Trustees
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, International President
Georges Ataya, CISA, CISM, CISSP, Solvay Business School, Belgium, Vice President
William C. Boni, CISM, Motorola, USA, Vice President
Avinash Kadam, CISA, CISM, CISSP, CBCP, GSEC, GCIH, Miel e-Security Pvt. Ltd., India, Vice President
Jean-Louis Leignel, MAGE Conseil, France, Vice President
Lucio Augusto Molina Focazzio, CISA, Colombia, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Frank Yam, CISA, FHKIoD, FHKCS, FFA, CIA, CFE, CCP, CFSA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Robert S. Roussey, CPA, University of Southern California, USA, Past International President
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Tally Solutions Limited, UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Romulo Lomparte, CISA, Banco de Credito BCP, Peru
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG LLP, Austria
Ronald Saull, CSP, Great-West Life and IGM Financial, Canada

Assurance Committee
Lynn C. Lawton, CISA, BA, FCA, FIIA, PII, KPMG LLP, UK
Pippa G. Andrews, CISA, ACA, CIA, Amcor, Australia
John Warner Beveridge, CISA, CISM, CFE, CGFM, Office of the Massachusetts State Auditor, USA
Daniel Patrick Casciano, CISA, Ernst & Young LLP, USA
Gregory T. Grocholski, CISA, The Dow Chemical Company, USA
Avinash W. Kadam, CISA, CISM, CBCP, CISSP, MIEL e-Security Pvt. Ltd., India
Anthony P. Noble, CISA, CCP, Viacom Inc., USA
Gustavo A. Solis, Grupo Cynthus S.A. de C.V., Mexico
Paul A. Zonneveld, CISA, CA, Deloitte & Touche, Canada
Corresponding Member Robert G. Parker, CISA, CA, CMC, FCA, Canada

COBIT Steering Committee
Roger S. Debreceny, Ph.D., FCPA, University of Hawaii, USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Dan Casciano, CISA, Ernst & Young LLP, USA
Steven De Haes, University of Antwerp Management School, Belgium
Peter De Koninck, CISA, CFSA, CIA, SWIFT SC, Belgium
Rafael Fabius, CISA, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Gary Hardy, IT Winners, South Africa
Jimmy Heschl, CISA, CISM, KPMG LLP, Austria
Debbie Lew, CISA, Ernst & Young LLP, USA
Max Shanahan, FCPA, CISA, Max Shanahan & Associates, Australia
Dirk Steuperaert, CISA, PricewaterhouseCoopers, Belgium
Robert E. Stroud, CA Inc., USA

コントリビューター代表のメッセージ

組織の発展に情報システムの適切な整備と運用が欠かせません。また、組織のみならず社会システムとしての IT とネットワークの重要性はますます高まっています。さらに、個人情報保護法、金融商品取引法に基づく内部統制報告制度等の法規制に伴い、情報システムが適切に整備・運用されていることを確認する必要性も高まっています。そのような環境の中で、情報システムのコントロールの事実上の標準となっている COBIT をベースにした IT Assurance Guide の重要性が高まっていることは間違いありません。

今回、この IT Assurance Guide の翻訳をお手伝いできたことは光栄なことだと思っています。これが、皆様の組織の発展に活用できることを切に願っております。

監査法人トーマツ
丸山 満彦

IT Assurance Guide 日本語版に寄せて

このたび ITGI/ISACA の文献のひとつである”IT Assurance Guide″を、監査法人トーマツ様のご貢献によって、「IT 統制の保証ガイド」として皆様にお届けできることを、私たちは大きな喜びと感じております。

IT のコントロールにおいて、それがどのようにあるべきかということは COBIT に詳細に示されておりますが、それをどのように確認し、保証していくのかについてまとめたものが、今回の文献となります。

もとより COBIT も、今回の IT Assurance Guide も、単に米国の SOX 法や日本の金融商品取引法で求められる IT 統制の実現のための参考文献としてだけではなく、IT を活用するビジネスの全般にわたって参照されるべき文献であります。

IT が組織において健全な開発・運用が行なわれ、そして IT が十分に活用され組織における価値を生み出すために、皆様の組織において活用していただけることを切に願います。

今回の翻訳にあたり監査法人トーマツ様の皆様には深く感謝の意を表します。そして，その翻訳品質確保のためのレビューに貢献していただいた日本大学の堀江正之先生、法政大学の石島隆先生にも深く感謝いたします。

日本 IT ガバナンス協会
会長 松尾 明

最終レビューにあたって

IT Assurance Guide の翻訳ででは、日本語として解り易い事を目指し、英文の全ての単語を含んだ日本語訳よりは、英文の意味を組んだ日本語に意訳している。

assurance activitiesは、保証活動と訳した。
assurance objectiveは、保証の目標と訳した。
assurance professionalは、保証業務の専門家と訳した。
assurance riskは、保証リスクと訳した。
control measures/proceduresは、コントロール手法/手続きと訳した。
control practiceは、コントロールプラクティスと訳した。
inspectは、検査すると訳した。
assurance initiativeは、保証業務と訳した。
assurance planningは、保証計画立案と訳した。
assurance projectは、保証プロジェクトと訳した。
assurance stepsは、保証業務のステップと訳した。
mechanismは、仕組みと訳した。
completenessは、網羅性と訳した。
observeは、観察すると訳した。
determineは、決定と訳しているが、Value driverは、Cobit4.1では、「価値要因」と訳したが、ITAGでは、Risk driverと対で用いられることが多いので、「価値のドライバー」と訳した。

コントリビューター：

監査法人トーマツ

リーダー

丸山　満彦

メンバー

安部　靖雄
大場　敏行
小湊　真智子
申　濬伍
剣　暁寧
深沢　優
横山　麻美
大島　嘉秋
小木曽　保幸
小峰　英篤
滝口　泰弘
妻川　和佳
藤井　信吾

レビューチーム

松原　榮一　（日本 IT ガバナンス協会　翻訳委員会委員長）
堀江　正之　（日本大学）
石島　隆　（法政大学）

翻訳運営チーム

日本 IT ガバナンス協会翻訳委員会

委員長	松原　榮一	
委員	梶本　政利	（最終編集）
委員	木村　章展	
委員	中村　努	
委員	吉丸　成人	

日本語版発行：2009年6月

目次

はじめに

1.はじめに

当ガイドの目的

*IT統制の保証ガイド*の目的は、さまざまなIT統制の保証活動をサポートするためにどのようにCOBITを用いるかについてのガイダンスを提供することである。すでにCOBITをITガバナンスのフレームワークとして用いている場合、保証のためのレビューを計画し、実施するときにCOBITを活用することができる。 それにより、ビジネス、IT、保証業務のそれぞれの専門家が共通のフレームワークと共通の目標のもとで連携することができる。

当ガイドは、IT統制の保証業務を効率的かつ効果的に策定できるようにデザインされており、広く受け入れられた保証アプローチに基づいたロードマップを用いて、計画立案、対象範囲の決定、保証のためのレビューの実行についてのガイダンスを提供している。COBITのプロセスとコントロール目標に基づく詳細なテストのステージにおいてに、どのようにCOBITの資源を用いるかについてのガイダンスも提供している。すべてのCOBITの資源と同様に、このガイダンスおよび提唱されているテストは杓子定規に適用することを意図したものではなく、個別の保証業務に合致するように調整すべきである。

このガイドは主に保証業務の専門家のためのものであるが、ITの専門家やアドバイザの関心にも適うものだろう。

COBIT のあらまし

Control Objectives for Information and related Technology (COBIT)は、組織がITガバナンスとコントロールのフレームワークを採用するのに必要な全ての情報を含む包括的な文書である。COBITは、ドメインとプロセスで構成されるフレームワークを通じて、ITを用いた投資を最適化し、ビジネス要件に対するITサービスの提供を成功させるために、管理しやすく論理的な構成で、すぐれた実践方法（手法）を提供している。

COBITは以下に示す企業のニーズに応えるものである。
- ビジネス要件とITの達成目標との間に測定可能な関連づけを行うこと
- 一般に認められたプロセスモデルに沿ってITアクティビティを体系的に整理すること
- 活用すべき主要なIT資源を識別すること
- 考慮すべき経営上のコントロール目標を定義すること
- 経営のための以下のツールを提供すること
  - ITのパフォーマンスを測定するための達成目標と測定指標
  - プロセスの実行能力をベンチマーク評価するための成熟度モデル
  - 役割と責任とを明確にしたRACIチャート

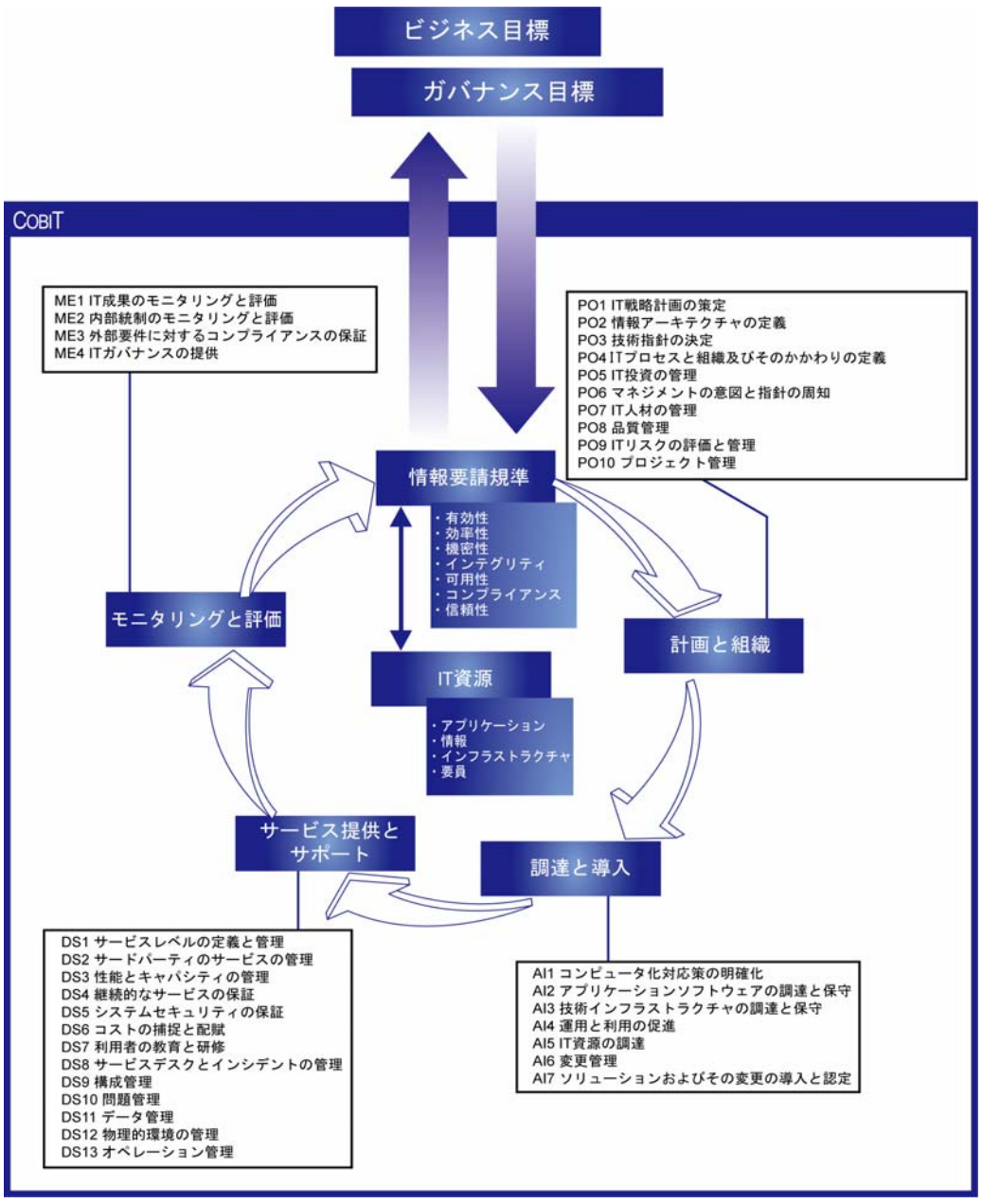
COBITは、ITの適正なガバナンス、管理およびコントロールに何が必要かに焦点を当てており、上位レベルに位置づけられるフレームワークである。COBITでは、他のより詳細なITのフレームワークや標準やベストプラクティスとの整合および調整を行っている。COBITは、これらの多様なガイダンス文書を統合する役割を果たしており、1つの包括的なフレームワーク内で、主要な目標を要約すると同時に、これらの目標とガバナンスおよびビジネス要件との関連付けを行っている。すなわち、COSOが公表している内部統制のフレームワークおよびこれに準拠する同様のフレームワークは、一般的に、企業における内部統制フレームワークとして認知されており、COBITは、IT向けの管理とコントロールのフレームワークとして一般的に認知されている。

ITガバナンスのフレームワークとしてCOBITを導入すると、次のような利点がある。
- ビジネスに焦点をあてた、ビジネスとITとの整合性の向上
- 共通の用語に基づく、すべての利害関係者による理解の共有
- マネジメント層の、ITの役割に関する理解の促進
- プロセス指向による、オーナーシップ（所有者）と責任の明確化

・ サードパーティ（第三者組織）や監督機関でのより広い認知
・ COSOのIT統制環境要件の達成

図1は、CobiTのフレームワークをまとめたものである。

図 1 COBIT フレームワーク

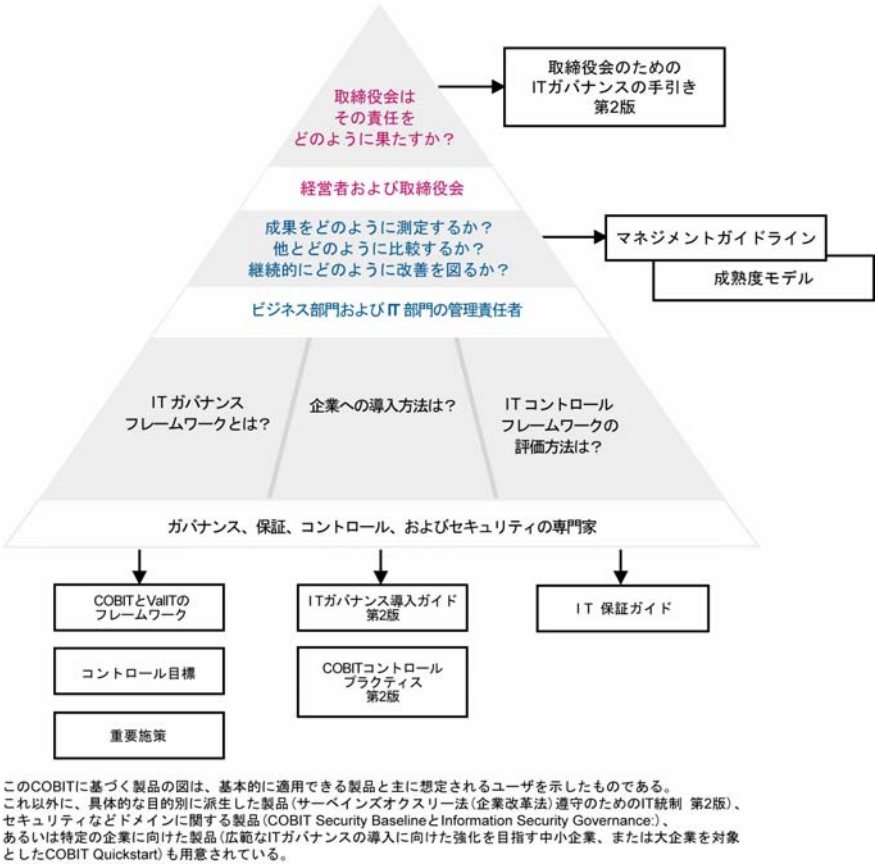


CobiT製品は、以下のグループをそれぞれ支援するように、3層構造になっている。
・ 取締役会と経営幹部層
・ ビジネス部門およびIT部門の管理責任者
・ ガバナンス、保証業務、コントロール、およびセキュリティの専門家

図2は、この3つのレベルのそれぞれで目的としている、ITガバナンス知識体系における、CobiT製品の位置

づけを示したものである。

図 2 COBIT をベースとした主な製品



各著作物の詳細については、付録X「COBITおよび関連著作物」を参照のこと。
COBITおよび関連する著作物、ケーススタディ、訓練の機会、ニューズレター、およびその他のCOBIT特有の情報についての網羅的かつ最新の情報については、*www.isaca.org/cobit* を参照のこと。

主に想定されている読者

この*IT統制の保証ガイド*は、34のITプロセスのそれぞれでさまざまな統制の保証活動をサポートするためにCOBITをどのように用いるかについての詳細なガイダンスを、保証業務の専門家およびIT専門家に提供している。以下についての保証のステップとアドバイスを提供している。

- すべてのプロセスに当てはまる汎用的なコントロール（COBITフレームワークの中で、PCで始まる記号で識別されている）
- アプリケーションコントロール（COBITフレームワークの中で、ACで始まる記号で識別されている）
- 固有のプロセスコントロール（フレームワークの中で、たとえばPO6.3とかAI4.1といったように、ドメインとプロセス番号で識別されている。）

また、それら保証業務のステップとガイドラインは、以下を目的としている。

- コントロールの設計を、コントロール目標に照らしてテストする
- コントロール目標の達成（運用の有効性）をテストする
- コントロールの欠陥とその影響を文書化する

このガイドの利用者は、COBITの考え方を熟知しており、少なくとも基礎レベルと同等レベルの知識（オンラインによるテストでCOBIT® Foundation Certificateを取得することができる）を持ち合わせていることを前提としている。もしそうでない場合には、読者がCOBIT Foundation Course™ を履修することを推奨する。履修の機会についての情報は、*education@isaca.org*宛にメールするか、*www.isaca.org/cobitcampus* のサイトから入手することができる。

また、このガイドの利用者は、保証業務についての一般的な考え方を熟知していることも前提としている。

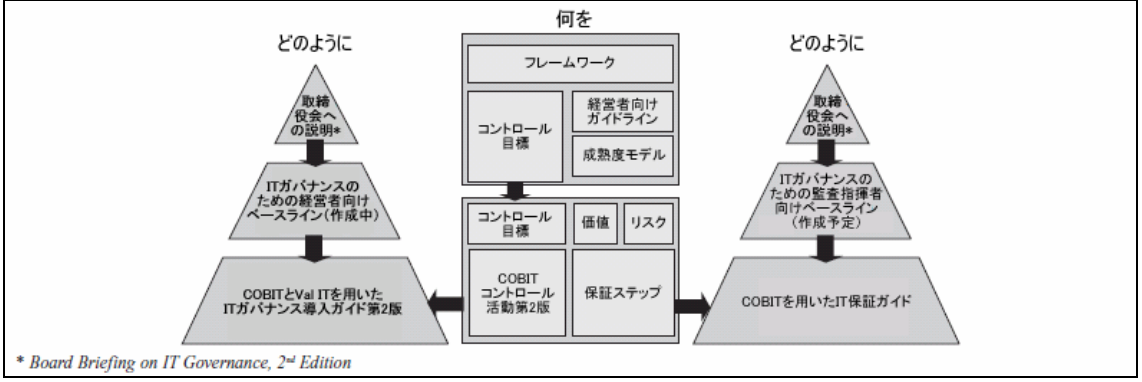
IT 統制の保証活動のための COBIT ガイダンス

図3で示すCOBITフレームワークは、以下の2つのガイドの基礎を提供している。

- *IT Governance Implementation Guide: Using COBIT and Val IT* TM, *2nd Edition* これは、COBITの資源を用いてどのようにITガバナンスを導入するかについてのロードマップとプロセスのガイダンスを提供している。
- *IT Assurance Guide: Using COBIT* これは、保証業務チームに専門的なガイダンスを提供し、ビジネスとITの専門家が理解できるように、COBITフレームワークとリンクした、構造化された保証アプローチを提供している。

図3にあるとおり、それぞれのガイドは異なるインプットによるものである。*IT Governance Implementation Guide* は、*COBIT Control Practices* を活用している一方で、*IT Assurance Guide* は保証業務のステップに基づいている。この2つのインプット（コントロール活動と保証業務のステップ）は、互いに全く異なるプロセスと考えられており、それらのガイドの利用者がITガバナンスプロセスのどちらか一方（導入または保証）に焦点を当てることができるようになっている。

図 3 導入ガイドと保証ガイド



*IT統制の保証ガイド*は、様々なレベルでの統制の保証についてアドバイスを提供している。プロセスレベルでは、コントロール目標を達成しているかどうかをどのようにテストするか、およびコントロールの欠陥をどのように文書化するかについて、プロセス特有のアドバイスを提供している。コントロール目標レベルでは、コントロール活動を基に、特定のコントロール目標のそれぞれについてコントロールの設計をテストするための保証業務のステップを提供している。この詳細なガイダンスは付録 I からVIに収録されている。第6章COBITのプロセスとコントロールのための保証のガイダンスでは、詳細なガイダンスを特定の保証業務にどう活用できるかについて、いくつか例を出している。

様々なレベルで、汎用的なアドバイスも提供している。汎用的なアドバイスはすべてのプロセスやコントロール目標に当てはまり、特定のアドバイスの補足として、あるいはその代替として用いることができる。第6章で、これらのプロセスについてさらに記述する。

実行ステージのテストのステップのために、このガイドでは、IT統制の保証業務の専門家を支援するための特定かつより詳細なガイダンスだけでなく汎用的なガイダンスも提供している。汎用的なアドバイスというのは、アドバイスのタイプによって、いかなるプロセス、コントロール目標、コントロール活動にでも適用することができるという意味である。特定のアドバイスというのは、特定のプロセス、コントロール目標、コントロール活動のために提供されているアドバイスを指す。このプロセスの基礎となるIT統制の保証フレームワークの概要を、**図4**で示す。

IT 統制の保証ガイド の構成要素

詳細な保証ガイダンスの内容は、COBITの34のプロセスをもとに構成されており、以下の構成要素を含んでいる。

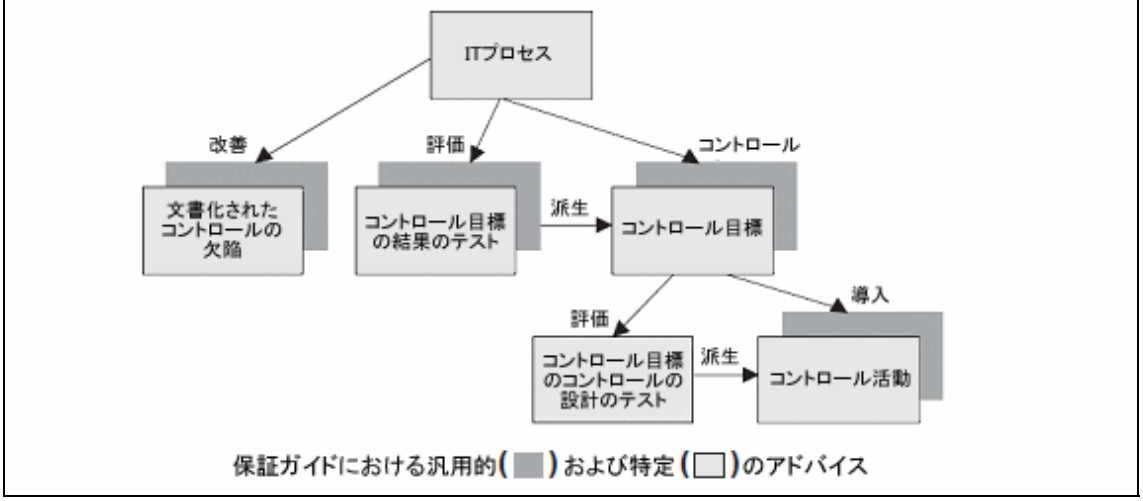
- **コントロール目標**—ITによって組織に価値をもたらし、リスクを管理し、規制上の要件を満たしながら、かつITへの投資が合理的な収益をもたらすことを確実にするには、ITのコントロールが決定的に重要であるという認識が高まっている。

  ITコントロール目標とは、特定のITプロセスにコントロール活動を導入することによって達成すべき望ましい結果や目的を記述したものであり、たいていの場合プロセス内の特定の活動と直接関係している。

  COBITのコントロール目標は、それぞれのITプロセスで有効な上位レベルのコントロールとして検討されたものである。コントロール目標は、実践的な経営活動として、簡潔に書かれている。また、できる限り論理的なライフサイクルに従って記載されている。

  企業経営者はコントロール目標に関して選択肢を有しており、経営陣は次のことを行うべきである。
  - 適切なコントロール目標を選択する
  - それぞれのコントロール目標を達成するのに求められる経営活動を実践するのに必要な投資と、それを達成しないことによって生じるリスクとのバランスを取る

図4 本書で提供する IT 統制の保証のアドバイスの概要



  - どのコントロール活動を導入するかを決定する
  - それぞれのコントロール活動をどのように導入するかを選択する

  COBITの200以上におよぶコントロール目標は、ビジネスの要件に対処しリスクを管理するために、それぞれのITプロセスで何を管理する必要があるかを明確に定めている。これらのコントロール目標によって、明確な方針を定め、ITコントロールのための優れた実践方法（手法）をはぐくみ、プロセスオーナーシップを促進することができる。これらのコントロール目標はまた、優れた実践方法（手法）をビジネス要件に関連づける際のリファレンス（ポイント）も提供している。COBITは40以上の異なるコントロールガイダンスと調整

のうえで構築されており、例えば、情報セキュリティ関連の基準に関するISO/IEC 27000シリーズ、ISO/IEC 9001:2000 Quality Management Systems—Requirements, IT Infrastructure Library (ITIL), *Capability Maturity Model® Integration* (CMMI®), Projects in Controlled Environments 2 (PRINCE2), *A Guide to the Project Management Body of Knowledge®* (PMBOK®) といった特定の領域に焦点を当てた他の基準や活動とも統合することができる。

- **価値のドライバーとリスクのドライバー**—価値のドライバーとリスクのドライバーは、専門家が、特定のコントロール目標を達成するために、関連するコントロール活動を導入する際のビジネス的な判断を下す際の有用なインプットとなる。価値のドライバーは、すぐれたコントロールの結果として実現しうるビジネス上の利益の例を提供しており、一方、リスクの要因は、回避したり緩和したりする必要のあるリスクの例を提供している。これらは、保証業務の専門家とITガバナンスの導入者に対して、コントロールを導入するための議論の枠組みを提供し、それを導入しないことの影響を具体的に示している。
- **保証テストのステップ**—保証テストのステップは、IT統制の保証プロセスを行う保証業務の専門家向けに、コントロール目標レベルでのガイダンスを提供している。これらのステップはコントロール活動から導き出されており、コントロール活動はそれぞれのコントロール目標から導き出されている。保証のテストは以下のステップを踏む。
  - コントロールの設計を評価する
  - コントロールが運用されていることを確認する
  - コントロールの運用の有効性を評価する

このような異なるテストのステップについては、第6章COBITプロセスとコントロールのための保証ガイダンスにおいて、さらに詳細に説明する。汎用的な保証業務のステップは、提案されたコントロールの設計の存在と、その有効性および関連する責任をカバーしている。特定の保証業務のステップは、コントロールの運用の有効性をテストし、コントロール目標のレベルで記述される。さらに、コントロールの欠陥や不備の結果をテストするための保証業務のステップを提供する。

保証テストのステップは、内部または外部の保証業務の専門家による保証プログラム策定の最初のレベルを提供するために設計されており、そのまま利用して実行できるような詳細な保証プログラムを提供することを目的とはしていない。むしろ、いくらかの経験を持つ保証業務の専門家が、さほど経験を持たないスタッフメンバーが利用して実行できるように、保証プログラムを効率的に策定しカスタマイズするための基礎として用いるためにある。保証業務の専門家は、保証業務の導入のための基礎としてテストのステップを踏むべきである。また、組織の実情と保証業務の目的に合わせてテストのステップを調整すべきである。なお、このステップは単なるガイダンスであって、詳細を記した手引書ではない。

保証業務の全構成要素の組み合わせは、保証の目標に対する意見の形成を支援するためのテスト方法を提供している。そのテスト方法は、以下のテストのタイプの1つまたは複数の組み合わせからなる。

- 質問と確認（異なる情報源を利用する）
- 閲覧（ウォークスルー、検索、比較、レビュー）
- 観察（言い換えれば、観察を通じた確認）
- 再実施または再計算と分析（サンプルに基づくことが多い）
- 自動化された証拠の収集（たとえばサンプル、証跡、抽出）と分析

COBIT コントロール活動 との関係

*IT統制の保証ガイド*はCOBITファミリーの一部である。保証テストのステップは、*COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition* をベースとしたものであり、保証業務の専門家がテスト活動で用いることができる形で表現してある。

COBIT Control Practices は、COBITフレームワークの能力を拡張したものであり、より詳細なレベルを提供している。COBITのITプロセス、ビジネス要件、およびコントロール目標は、有効なコントロール構造を導入するのに何をする必要があるかを定めている。*COBIT Control Practices* は、コントロール目標のレベルで、目標をどのように達成するかについてのより詳細なガイダンスを提供している。コントロール活動は、COBITのコントロール目標のそれぞれについて、以下の構成要素から成る。

- 価値のドライバーとリスクのドライバー。これは「なぜそうするのか」についてのガイダンスを提供する。
- ITプロセスを評価し改善策を実施するときに考慮すべきコントロール活動

各コントロール目標に対して、該当するコントロール活動の一覧を記載している。さらに3つの汎用的なコントロール活動を定めているが、これらはすべてのコントロール目標に当てはまるものである。汎用的なコントロール活動と特定のコントロール活動の完全な集まりは、コントロール目標を達成するために必要な活動から成り、1つのコントロールアプローチを提供する。これらは、コントロール目標に基づいて、より詳細なレベルで、プロセスの成熟度を評価し、潜在的な改善策を検討し、コントロールを導入するための上位レベルかつ汎用的なガイダンスを提供する。これらは個別の解決策を提示するものではないので、ITILやPRINCE2といったような特定の関連する基準とベストプラクティスからさらなるガイダンスを入手する必要があるだろう。コントロール活動には、以下の設計基準が適用される。。

- コントロール目標の趣旨に合致している
- 適時な方法で実行できる
- 現実的で費用対効果が高い
- 測定可能である
- 関連する役割の定義、および該当する場合には役割分担を提供する
- 行動志向である
- 可能な限り常にライフサイクルに基づいている

コントロール活動によって、なぜコントロールが必要なのか、特定のコントロール目標をみたすような優れた実践方法（手法）とは何かについてのガイダンスが提供され、提案される解決策も完全かつ成功裏に導入されやすくなるだろう。

コントロール活動は、次の2種類の読者を支援するために設計されている。

- ITガバナンス導入の提唱者（たとえば経営層、業務委託先、エンドユーザ、コントロールの専門家）
- 保証業務の専門家（たとえば内部および外部の保証業務の専門家）

IT統制の保証のために、すべてのコントロール活動が、詳細な保証ステップを策定するのに用いられた。保証テストのステップは、内部または外部の保証業務の専門家による保証プログラム策定の最初のステージを提供するために設計されている。したがって、このIT統制の保証ガイドを用いる専門家は、保証業務のステップはコントロール活動から導いたものであるということを考慮に入れる必要がある。このガイドでは、コントロール活動それ自体は提供していない。

図5のテーブルは、COBITで提供されているコントロールの概要を提供しており、このガイドのIT統制の保証の基礎を示している。

図 5 コントロール目標とコントロール活動

	コントロール	
	コントロール目標	**コントロール活動**
一般	COBIT フレームワークは、それぞれのプロセスに適用される6つのプロセスコントロールを提供している。プロセスのレビューを行うときには、これらのコントロール目標とそれに関連するコントロール活動と保証のステップを、特定のコントロール目標に追加すべきである。	コントロール目標をコントロール活動に展開するときには、最初のステップは常に同じであり、目標を達成するためのアプローチの設計、記録、伝達および、それを実現するための実行責任と説明責任の割り当てが含まれる。
特定	それぞれのプロセスで、特定のコントロール目標を、COBIT フレームワークで提供している。	COBIT はそれぞれのコントロール目標で、特定の活動を提供している。汎用的なコントロール活動とともに、コントロール目標を達成するのに必要かつ十分なステップからなるコントロールの設計を提供している。

図6のテーブルは、COBITのコントロールの概要に基づきこのガイドで提供しているIT統制の保証の概要を示したものである。

図 6 汎用的および特定のアドバイスと IT 統制の保証のクラスとの関連

	保証		
	コントロールの設計のテスト	**コントロールプロセスの結果のテスト**	**コントロールの欠陥の文書化**
一般	汎用的なコントロール活動は、保証の方法論の標準的な考え方に基づいて、保証業務のステップに展開されている。	コントロールの設計に加えて、あるいはその代わりとして、コントロール目標の達成をテストすることができる。いかなるプロセスでも利用可能な、証拠を探すためのいくつかの標準的なアプローチが提供されている。	特定のアドバイスの代わりとして、あるいは特定のアドバイスに加えて、コントロールの欠陥を文書化するためのいくつかの標準的なアプローチが提供されている。主に比較可能なデータ(たとえばベンチマーク、測定結果、事例)に焦点を当てている。
特定	特定のコントロール活動もまた保証業務のステップに展開されている。一般的な保証業務のステップとともに、コントロール目標に関わるコントロール設計について完全なテストを提供している。	それぞれのプロセスで、プロセスのコントロール目標をテストするための、いくつかの保証業務のステップが提供されている。一般的なアドバイスを特定のアドバイスの代わりに、あるいは特定のアドバイスを補完するために用いることができる。	それぞれのプロセスで、プロセスの達成目標、測定指標、活動、コントロール目標に関連してコントロールの欠陥をどのように文書化するかについての特定のアドバイスが提供されている。

最後に、6つのアプリケーションコントロール(COBITで提供されている)のテストについての追加的なアドバイスが提供されており、これもまた設計、結果、影響のテストを扱っている。

COBITおよびそれを補助する著作物の多くは、広範囲のIT統制の保証活動に関する詳細なサポートを提供している。

本書の構成

本書の主だったセクションは、IT統制の保証の推奨ロードマップの構造にしたがっている。このロードマップの詳細は第2章IT統制の保証の基本原理と背景でさらに詳細に説明する。このロードマップの主たるセクションまたは章タイトルは以下のとおりである。

- 計画
- 対象範囲の決定
- 実行、これは以下を含む。
  - IT統制の保証対象の理解の精緻化
  - 主要なコントロール目標の対象範囲の精緻化
  - コントロールの設計の有効性のテスト
  - 主要なコントロール目標達成のテスト
  - コントロールの欠陥の影響の文書化
  - 結論と勧告の作成と伝達

計画については第3章保証計画で説明する。対象範囲は第4章ITの資源とコントロールの対象範囲で扱い、第5章保証業務の実行では実行のステップのすべてを扱う。

第6章COBITのプロセスとコントロールのための保証ガイドラインでは、COBITのプロセスとコントロール目標のために提供する保証ガイダンスの構造を説明する。第7章では、COBITの構成要素がIT統制の保証活動をどのようにサポートするかを説明する。付録Ⅰ からⅥでは、実際の保証のテストを提供する。

このガイドの使い方

COBITは広範囲にわたり潜在的な読者がおり、組織に属する多くの人が利用することができるが、このガイドは特に内部および外部の保証業務の専門家を意図したものである。このガイドの一番の利点は、利用者がCOBITフレームワークとその関連著作物の一貫性に依拠することができるということである。COBITフレームワークはITガバナンスのフレームワークとしてますます用いられるようになっており、ビジネスとITの管理責任者の連携を助け、ITのパフォーマンスを改善するための基礎を提供している。ITガバナンスとITのパフォーマンスを改善しているビジネスとITの管理責任者と同じフレームワークに基づいて保証業務の専門家がレビューを行えば、当事者の誰もが共通の用語を用いることになるため、必要なコントロールの改善にも同意し実施しやすくなるだろう。

このガイドは、保証業務の専門家が、以下を含む様々な目的で用いることができる。

- 保証とテストの原理について現在の優れた実践方法（手法）に関する概要を得る
- COBITの様々な構成要素とその関連する概念を用いることが、いかに保証業務の計画および対象範囲の決定において役立つかを学ぶ
- COBITのコントロール目標とそれを支えるコントロール活動のすべて、およびそれらが有効であるという保証を得るためのテスト方法についての、包括的な参考資料を利用可能にする

IT統制の保証の基本原理と背景

2. IT 統制の保証の基本原理と背景

はじめに

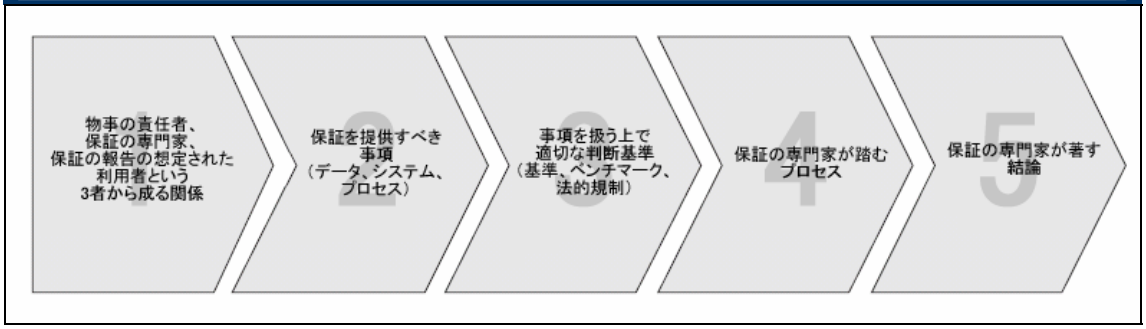
この節では、IT統制の保証の基本原理、構成要素、背景の全体像を説明し、IT統制の保証のロードマップへと進む。その際、それに伴う主要なステップに関する高レベルの説明を提供する。

IT統制の保証ガイド の目的は、詳細な保証業務のガイドラインを提供することではなく、保証業務を実施する上での高レベルのガイダンスを提供し、保証を理解するためのいくつかの基本原理と、いくつかの関連する技法および貢献活動を簡潔に説明するのが目的である。

International Auditing and Assurance Standards Board's (IAASB's) International Framework for Assurance Engagements (IAASB Assurance Framework) のような公式の基準を参照としてもよいが、このマニュアルでは、「監査」という用語よりも広い意味をもつ、「保証」という用語で通している。保証という用語はまた、内部監査基準または外部監査基準で規定していないような評価活動もカバーしている。

IAASB保証フレームワークで規定されているように、そして**図7**で示す通り、保証業務と呼ばれるためには、5つの構成要素が存在しなければならない。

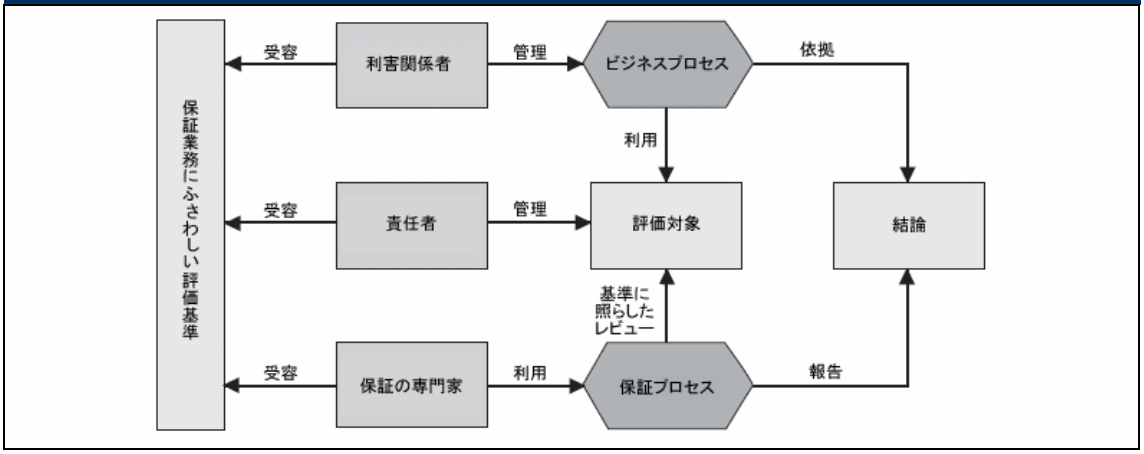
図 7 保証業務の 5 つの構成要素



保証業務の目的は、保証業務の専門家が、他者が責任のある対象事項を測定したり評価したりすることである。また、IT統制の保証業務では、一般的に評価の対象となっているものを利用する者は、その運用および管理業務を責任を担う側に委託している利害関係者である。したがって、利害関係者は評価の最終利用者であり、責任を担う者および保証業務の専門家とともに、評価基準について承認することができる。

その評価の結論として、評価対象が利害関係者のニーズに合致しているかどうかについての意見が出されることとなる。**図8**は保証業務における相互関係をまとめたものである。

図 8 保証業務における相互関係

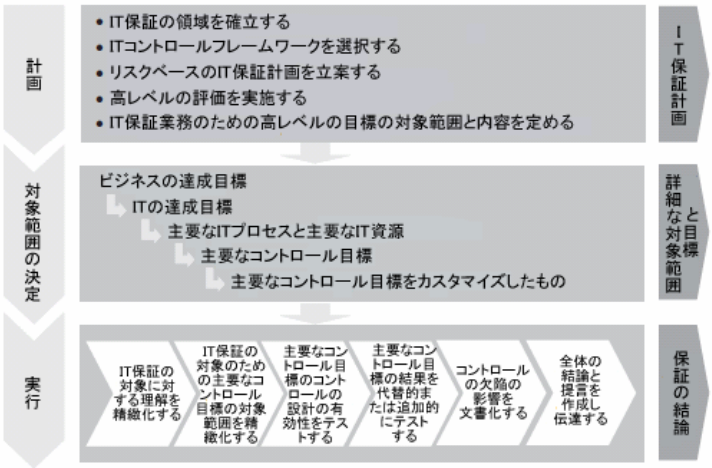


保証のアプローチとロードマップ

IT統制の保証のロードマップ

IT統制の保証を提供するためには、一貫した方法論やアプローチに従うことが大切である。それぞれの組織や保証業務のタイプに特有のアプローチがあるだろうが、このガイドの目的のために、共通するアプローチを用いる。それは計画立案、対象範囲の決定、実行という3つのステージに基づいており、最後のステージは6つのステップに細かく分類することができる。このロードマップのステージとステップを**図9**で示す。

図 9 IT 統制の保証のロードマップ



より重要な保証業務については、付録Ⅷ ITの対象範囲の決定において、その業務を目標、行動、成果物にブレークダウンするための追加的な情報を記している。このようなブレークダウンによって、IT統制の保証活動の対象範囲の決定およびITコントロールの対象範囲の決定の際に利用することのできる、より詳細なガイダンスを得ることができる。

計画

保証業務をアサインするためにIT統制の保証の領域を確立することは、あらゆる保証業務の起点となる。包括的な計画を作成するためには、保証業務の専門家が、IT統制の保証の領域を理解することと、COBITのような適切なITコントロールのフレームワークを選択することが必要である。この2つが備わって初めて、リスクベースでの保証業務の計画策定が可能になる。正しい保証目標を設定するためには、最初に高レベルの評価を実施する必要がある。このステージの最終成果物は、IT統制の保証計画である（通常は年次）。

対象範囲の決定

対象範囲を決定するプロセスは、次の3つの異なる方法で行うことができる。

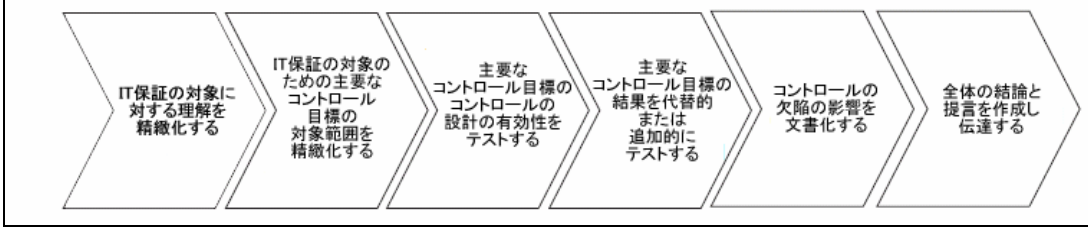
- 最も詳細な対象範囲決定アプローチは、レビュー対象となる環境でのビジネスとITの達成目標を定め、その達成目標をサポートするのに必要なITプロセスとIT資源（すなわち保証の対象領域）を識別することから始まる。IT統制の保証業務によって定まる達成目標は、さらに下位の細かな内容（その組織向けにカスタマイズした主要なコントロール目標）へと落とし込むことができる。
- 高レベルの対象範囲決定アプローチは、ITGIが実施したベンチマーク研究から始めてもよい。それらは、COBITで述べられているように、ビジネスの達成目標、ITの達成目標、ITプロセスの相互関係についての汎用的なガイドラインを提供している。この汎用的な達成目標とプロセスを段階的に示したものは、特定の環境を評価するのに必要なより詳細な対象範囲の決定の基礎として用いることができる。
- 複合型の対象範囲決定アプローチは、詳細な方法と高レベルの方法とを組み合わせたものである。このアプローチは、汎用的な達成目標とプロセスを段階的に示したものから始まるが、対象範囲の決定をより詳細なレベルにあげていく前に特定の環境に合わせて修正する。

このステージの最終成果物は、それぞれ異なるIT統制の保証業務の対象範囲と目標である。

実行

IT統制の保証のロードマップの3つ目のステージは、実行ステージである。**図10**では、保証業務の専門家が特定の保証業務を実行する際に利用できるアプローチを示している。これらのステップは、保証業務の専門家が実行する、主だったテスト活動をカバーしている。第5章保証業務の実行で、それぞれのステップをより詳細に示している。このステージの最終成果物は、それぞれのIT統制の保証業務の結論である。

図 10 実行のロードマップ



IT統制の保証活動

前節「IT統制の保証のロードマップ」で提示したアプローチは、保証サービスを提供するためのステージとステップについて示しており、このガイドの構造を規定している。このような保証アプローチのステージのそれぞれのもとで実施される典型的なIT統制の保証活動のいくつかを**図11**で列挙する。

図11では、IT統制の保証のロードマップの各ステージとステップで用いることができ、その際のアドバイスも提供されている典型的なIT統制の保証活動について紹介する。一つの活動が一つのステップになることもあれば、一つの活動をいくつかのステップで活用することができることもある。

図 11 IT 統制の保証活動

- 計画
  - 迅速にリスク評価を行う
  - 脅威、脆弱性、ビジネスへの影響を評価する
  - 業務上のリスクとプロジェクトリスクを診断する
  - リスクベースの保証活動を計画する
  - 価値の要因に基づいて重要なITプロセスを識別する
  - プロセスの成熟度を評価する
- 対象範囲の決定
  - 保証業務の対象範囲を決定し計画を立てる
  - 重要なプロセスに対するコントロール目標を選択する
  - コントロール目標をカスタマイズする
- 実行
  1. IT保証の対象に対する理解を精緻化する
     - 重要なITプロセスを識別/確認する
     - プロセスの成熟度を自己評価する
  2. IT保証の対象に対する主要なコントロール目標の対象範囲を精緻化する
     - コントロール目標の選択を改訂する
     - コントロール目標をカスタマイズする
     - 詳細な監査プログラムを策定する
  3. 主要なコントロール目標におけるコントロールの設計に有効性をテストする
     - コントロールをテストし評価する
     - プロセスの成熟度を改訂/評価する
  4. 主要なコントロール目標の結果をテストする
     - コントロールの自己評価を行う
     - コントロールをテストし評価する
  5. コントロールの欠陥の影響を文書化する
     - 業務やプロジェクトの残余リスクを診断する
     - リスクを実証する
  6. 全体の結論と提言を作成し伝達する
     - 保証の結論を報告する

このガイドでのアドバイスの大半は、実行ステージ、即ち**図12に示した**ロードマップと第7章（COBITの構成要素はどのようにIT統制の保証活動をサポートしているか）に焦点を当てているが、これらの活動に特に有益なCOBITの構成要素を明示することで、関連する保証活動に追加的なアドバイスを提供している。このような活動のほとんどはすべてのIT統制の保証業務に含まれているため、COBITの構成要素のほとんどもまた、ITに関連するすべてのタイプの保証業務に活用することができる。

図12は、保証活動と、それに対応するCOBITの構成要素との間の関係を示している。さらに、第7章「構成要素はIT統制の保証活動をどのようにサポートしているか」においては、様々なIT統制の保証活動の有効性ないし効率性を改善するために、COBITの様々な構成要素をどのように活用できるかについて提案を行なっている。

図 12 保証活動と COBIT の構成要素との対応関係

	COBITの構成要素																
IT保証活動	コントロール目標	COBITコントロール活動	価値とリスクについての記述	成熟度モデル	成熟度モデルの属性	RACI(主要な活動および責任)	達成目標と成果の測定基準	パフォーマンスの原動力	経営者の注意を引くためのツール	情報基準	プロセスリスト	Board Briefing on IT Governance, 2nd Edition	ITのリスクとコントロールの診断	COBIT Quickstart	COBIT Online—検索と閲覧	COBIT Online—ベンチマーキング	SOX法対応のためのITコントロール目標第2版
迅速にリスク評価を行う			✓	✓		✓	✓	✓	✓				✓	✓	✓		
脅威、脆弱性、ビジネスへの影響を評価する			✓			✓	✓	✓							✓		✓
業務上のリスクとプロジェクトリスクを診断する			✓			✓	✓	✓	✓				✓		✓		
リスクベースの保証イニシアチブを計画する	✓		✓	✓		✓	✓	✓	✓			✓	✓		✓	✓	✓
価値の原動力に基づいて重要なITプロセスを識別する				✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	
プロセスの成熟度を評価する				✓	✓	✓	✓		✓		✓	✓			✓	✓	
保証業務の対象範囲を決定し計画を立てる						✓	✓			✓	✓		✓		✓		✓
重要なプロセスに対するコントロール目標を選択する						✓	✓			✓	✓				✓		✓
コントロール目標をカスタマイズする	✓	✓			✓	✓	✓	✓							✓		✓
詳細な監査プログラムを策定する	✓	✓		✓		✓	✓						✓		✓		✓
コントロールをテストし評価する	✓	✓	✓		✓	✓	✓								✓		✓
リスクを実証する	✓	✓	✓			✓	✓	✓	✓	✓	✓				✓	✓	✓
保証の結論を報告する	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓				✓	✓	✓
プロセスの成熟度を自己評価する	✓	✓		✓		✓	✓	✓	✓				✓		✓		
コントロールの自己評価を行う	✓	✓				✓	✓						✓	✓	✓	✓	

他の保証モデルとの関連

保証業務の専門家は、国際会計士連盟(IFAC) の中に置かれている国際監査・保証基準審議会(IAASB)のような組織が策定した基準を熟知しているだろう。IAASBはそのInternational Standards on Auditing の中で、財務諸表監査に関連した保証業務を実施するステージを定義している。このようなステージは、特に財務諸表監査の目的で定義されたものだが、このガイドで提示するIT統制の保証プロセスとも整合する。これを**図13**で図示する。

図 13 IT 統制の保証と保証業務のステージとの相関

			保証のステージ(IAASB)						
			責任者と保証の	利用者を決定する成果物の想定された	保証の対象性質を	決定する評価基準を定め	合意する証拠を収集する	証拠を評価する	判断を下す	結論を下し報告する
ロードマップのステージ		計画	✓	✓	✓				
		対象範囲の決定			✓				
	実行	IT保証の対象に対する理解を精緻化する	✓	✓	✓				
		IT保証の対象のための主要なコントロール目標の対象範囲を精緻化する			✓				
		主要なコントロール目標のコントロールの設計の有効性をテストする				✓	✓		
		主要なコントロール目標の結果を代替的または追加的にテストする				✓	✓		
		コントロールの欠陥の影響を文書化する				✓	✓		
		全体の結論と提言を作成し伝達する						✓	✓

実行ステージの最初の2つのステップは、計画と対象範囲決定のステージの分析を精緻化したものであり、したがって、IAASBの基準に対して同じように対応している。内部の保証業務では、計画活動は年次活動だと考えられており、「計画を精緻化する」というのは個々の業務の計画立案段階のことを指す。一方、外部監査では、この2つのレベルの計画立案は同時に発生し得る。

IT統制の保証のために提案されているアプローチは、以下を明確に区別するためのものである。
- コントロール目標の設計のテスト
- コントロール目標の達成のテスト
- 識別されたコントロールの欠陥の影響の文書化

この3ステップのそれぞれでは、証拠の収集と評価を扱っているが、その内容は異なっている。

提供する保証アドバイスのタイプ

図14で示す通り、実行ステージのテストのステップのために、このガイドでは、IT統制の保証業務の専門家を支援するためのより特定的なアドバイスだけでなく汎用的なガイダンスも提供している。この図はCOBITの主要な構成要素(プロセス、コントロール目標、コントロール活動)とIT統制の保証のロードマップとの間の関係をまとめたものである。

汎用的なアドバイスというのは、アドバイスのタイプによって、いかなるプロセス、コントロール目標、コントロール活動にも適用することができるという意味である。特定のアドバイスというのは、特定のプロセス、コントロール目標、コントロール活動のために提供されているアドバイスを指す。

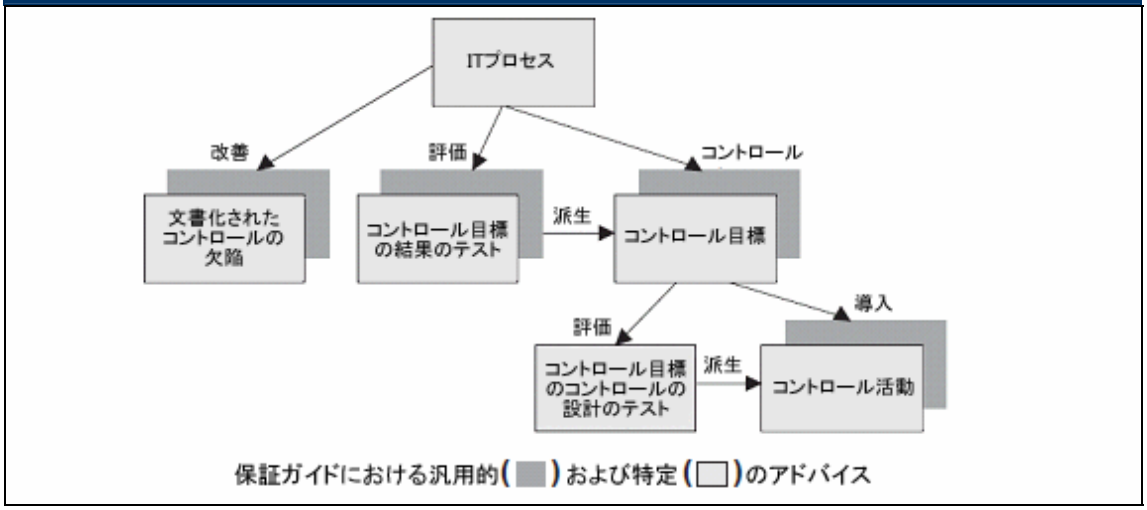
歴史的背景—財務諸表監査

歴史的には、IT統制の保証は財務諸表監査の支援のために始まったということを理解することが大切である。この種の保証は依然として強い関連性を持っており、特に米国SOX法や国際的にも同様の規制の観点からそう言える。

通常、財務諸表監査の目的は、財務諸表、特に以下のアサーションに関して意見を表明することである。

- 財務諸表に反映されている資産、負債、取引の実在性または発生
- 表示されているすべての財務情報の網羅性
- 権利、義務、関連する責任の財務諸表への適切な表示
- 公正かつ首尾一貫した基準に基づく財務諸表の各項目の評価または期間配分
- 財務諸表および、正しい解釈を確実にするための関連する会計原則や追加的な情報の適切な表示および開示

図 14 このガイドで提供するアドバイスのタイプ



これらのアサーションがすべて揃って満たされている場合に、監査人は関連する企業の財務状況についての意見を報告することができる。

関連する一般的な基準とガイダンス

財務諸表に対する外部監査プロセス向けに現在認識されているガイドラインは、International Standards on Auditing (ISA) [1]に具体化されている。

ISA 315は、保証業務の専門家が監査に関連する内部統制についての理解を得るという要件を規定しており、それは以下の構成要素を含む。

- 統制環境
- 企業のリスク評価プロセス
- 財務報告に関連するビジネスプロセスを含む情報システムおよび通信
- コントロール活動
- コントロールに対するモニタリング

[1] International Standards on Auditing (ISA)は、財務情報についての財務監査を実施するための専門的基準である。この基準はInternational Federation of Accountants (IFAC)によって公布されており、各自の責任性、監査計画立案、内部統制、監査証拠、他の専門家の成果の利用、監査の結論と監査報告、および専門化された領域をカバーしている。

ISAでは、一般的にいって、ITは企業の内部統制の有効性と効率性に潜在的なベネフィットをもたらすが、特有のリスクも引き起こすことを明らかにしている。

ITについては、財務諸表のアサーションを以下の情報処理目標に言い換えることができる。
- 網羅性
- 正確性
- 妥当性
- アクセス制限

保証業務の専門家に対して最低限求められるのは、財務報告に関連するビジネスプロセスを支える情報システムを理解し、企業がITから生じるリスクにどのように対応しているかを理解することである。ITを利用すれば、コントロール活動がビジネスおよび関連する財務報告に組み込まれる方法にも影響が及ぶため、保証業務の専門家は、企業が有効なIT全般統制と業務処理統制を確立することで、ITから生じるリスクに対して十分に対応しているかどうかを検討する必要がある。

ISAは、IT全般統制をもって、多くのアプリケーションに関連するものであり、情報システムの継続的かつ適切な運用を確実に支援することで、業務処理統制の有効な機能を支える方針および手続きであると定義している。ISAでは、IT全般統制を以下のように分類している。
- データセンタとネットワークの運用
- システムソフトウェアの調達、変更、および保守
- アクセスのセキュリティ
- アプリケーションシステムの調達、開発、および保守

ISA 330は、識別されたリスクに対応する際に適用すべき監査手続きの性質、時期、および範囲についてのガイダンスを提供している。ISAでは、以下を含む内部統制の妥当性の確認に関連していくつかの具体的な要件を規定している。
- 保証業務の専門家は、アサーションレベルでの重大な虚偽表示のリスク評価を行うにあたりコントロールが有効に運用されているという期待を抱いている場合には、監査対象期間中に適宜コントロールが有効に運用されていたという十分かつ適切な監査証拠を得るために、コントロールのテストを実施すべきである。
- 保証業務の専門家は、実証手続きからのみ得られる監査証拠によっては、アサーションレベルでの重大な虚偽表示リスクを受容可能なレベルにまで低減させることが不可能または現実的でないと決定したときには、運用の有効性についての監査証拠を得るために関連するコントロールについてテストを実施すべきである。

ISAはまた、「保証業務の専門家は、コントロールの運用の有効性をテストするために、質問と組み合わせて他の監査手続きを実施すべきである」と規定することによって、実行すべき手続きのタイプを特定している。

IT統制の保証における証拠

特にITとの関連において、ISAは、保証業務の専門家はアサーションに直接関係するコントロールだけでなく、たとえば土台にあるIT全般統制のような、そのコントロールが依拠する他の間接的なコントロールの運用の有効性もサポートするような監査証拠の入手の必要性を考慮すべき旨、規定している。この点、CobiTフレームワークは豊富なガイダンスを提供しており、本ガイドはISAガイダンスに沿った保証アプローチを提供している。

IT処理はもともと一貫性を備えているため、自動化されたアプリケーションコントロールが導入されている場合の監査証拠は、企業の全般統制（および特に変更コントロールを含むシステム開発ライフサイクルのコントロール）の運用の有効性に関して得た監査証拠と組み合わせて検討される場合、関連する期間内の運用の有効性について実証的な保証業務の証拠を提供することができる。これらの側面についてのさらなるガイダンスを、第6章COBITのプロセスとコントロールのための保証ガイダンスで提供している。

重要性

財務諸表監査を実施したり支援したりするときには、監査は金額的重要性によって測定され報告されるため、保証業務の専門家は通常は、金額的重要性を測定する。IT統制の保証業務の専門家は、非財務的な項目についても保証業務を実施することがある。その場合は代替的な測定基準が求められる。特定のコントロール目標について、重要なコントロールとは、それなしにはコントロール手続がコントロール目標に合致しているという合理的な保証を提供しないような単一のコントロールまたは複数のコントロールの組み合わせのことである。

ISACA IS Auditing Guideline G6（*www.isaca.org/standard/guideline.htm*）では、IT統制の保証目標が財務取引を処理するシステムや業務と関係ある場合には、重要性を評価する際に、システムがコントロールする資産の価値や、日次、週次、月次、年次で処理される取引の金額を検討すべきであると明確に規定している。

財務取引に影響しないようなシステムや業務については、以下のようなものが重要性を評価するために検討すべき測定基準の例となる。

- システムや業務がサポートするビジネスプロセスの重要性
- システムや業務の費用（すなわち、ハードウェア、ソフトウェア、人員、業務委託、間接費、これらの組み合わせ）
- エラーの潜在的なコスト（販売機会の喪失、保証履行の要求、回収不可能な開発費用、警告のために必要な広告費用、調整費用、健康と安全確保ためのコスト、必要以上に高い生産費用、高い廃棄率等）
- 期間当たりに処理するアクセス、取引、問い合わせの数
- 作成する報告書と維持する提出書類の性質、時期、範囲
- 取り扱う物品の性質と数量（たとえば在庫の移動が金額なしに記録されるような場合）
- サービスレベル合意（SLA）の要求事項と潜在的なペナルティのコスト
- 法的な要件や契約上の要件を遵守できないときのペナルティ

保証リスク

保証リスクとは、保証の対象に重大な虚偽表示が存在するときに保証業務の専門家が間違った意見を報告するリスクである。保証リスクは、重大なエラーのリスクと、保証業務の専門家が関連するエラーやコントロールの不備を発見できないリスクとの関数である。

重大なエラーのリスクには二つの構成要素がある。

- **固有リスク**—関連する内部統制[2]が存在しないと仮定したときに、ある虚偽表示が、単独でまたは他の虚偽表示と合わさることで、責任を持つ主体によるアサーションが重要な虚偽表示となる可能性（敏感度）
- **コントロールリスク**—アサーションに関して発生し、個別または他の虚偽表示と合わさって重大になりうるような虚偽表示が、企業の内部統制によって防止されまたは適時に発見され修正されないリスク

[2] このような定義は、International Accounting and Assurance Standards Boardからのものである。

発見リスクとは、保証業務の専門家の手続きによっても、個別または他の虚偽表示と合わさってアサーションに存在する重大な虚偽表示を発見できないリスクのことである。保証業務の計画を立てるときには、保証リスクを評価し、確実に保証目標に合致するようなアプローチを設計することが大切である。

（空白ページ）

保証計画

3. 保証計画

はじめに

IT統制の保証フレームワーク（**図9**で示されている）の最初のフェーズは計画フェーズである。IT統制の保証の専門家は、保証業務を開始する前に、保証業務の目標に合致する適切なやり方で仕事の計画を立てるべきである。内部の保証職能の場合、少なくとも年に1度は保証計画を策定/更新/レビューすべきである。計画は、保証活動のためのフレームワークとして機能し、保証基準によって設定された責務に対処できるようにすべきである。外部のIT統制の保証業務では、計画は通常は各業務ごとに作成される。それぞれのタイプの保証計画において、業務の目的を明確に文書化し、想定されているユーザの戦略と優先順位を反映すべきである。

計画立案プロセスの一環として、IT 統制の保証の専門家は、IT 統制の保証の領域、IT にとっての組織のビジネス達成目標、IT の達成目標、および IT プロセスと IT 資源を通じてそれらを実現するためにどのように計画すべきかについての十分な理解を得るべきである。要求される知識の程度は、組織、その環境、リスク、保証業務の目標によって決まる。標準化され構造化されたアプローチにしたがって保証業務と保証計画立案の作業を実行するためには、IT 統制の保証の専門家は、保証業務にとって有用な適切なコントロールフレームワーク（COSO や COBIT）や、IT 管理のフレームワークや基準（ITIL、ISO/IEC 27000）を選択すべきである。

IT統制の保証の領域

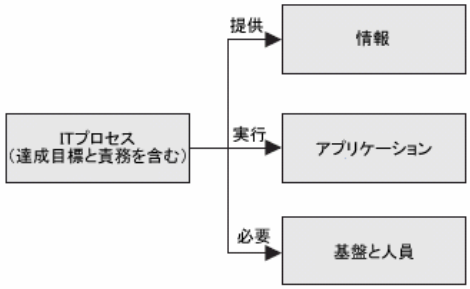
IT統制の保証の領域とは、IT統制の保証の提供者の責任範囲を定めたものである。通常これは、ITプロセス、資源、リスク、コントロールを分類し関連づけている高レベルの構造に基づいているため、これによって別々のIT統制の保証業務をリスクベースで選択することが可能になる。保証の領域を企業レベルで定義する必要があり、これは、定義して評価できるような対象、単位、プロセス、手続き、システム等から構成されていなければならない。保証の領域の最小単位は、その中で保証業務を実施できるような範囲である。*IT統制の保証ガイド*の目的のために、COBITが、4つのタイプのIT資源と、4つのドメインに分類された34のITプロセスによって構成されるIT統制の保証の領域を定義するための構造を提供している。4つのドメインは、ITにおける伝統的な役割である、計画、構築、運用、モニタリングをカバーしている。

COBITで識別するIT資源は、以下のように定義される。

- **アプリケーション**—情報を処理する自動化されたユーザシステムおよび手作業による手続きを指す。
- **情報**—ビジネスで使用される、任意の形式で情報システムに入力、処理、出力されるデータを指す。
- **インフラストラクチャ**—アプリケーションよる処理を可能にする技術および施設（ハードウェア、オペレーティングシステム、データベース管理システム、ネットワーク、マルチメディアなど、およびそれを格納しサポートする環境）を指す。
- **要員**—情報システムとサービスの計画、編成、調達、導入、提供、サポート、モニタリング、および評価に必要な要員を指す。社内の人材、アウトソーシング先の人材、および必要に応じて契約する人材が含まれる。

COBITで定義された4つのドメインは、計画と組織、調達と導入、サービス提供とサポート、モニタリングと評価である。**図15**で示すように、ITプロセスは、ビジネスに情報をもたらし、アプリケーションを実行し、基盤と人員とを必要とする。これらが一体となって、エンタープライズITアーキテクチャを構成する。

図 15 エンタープライズ IT アーキテクチャ



リスクのレベル、技術の複雑さ、直近の保証業務が実施されてからの経過時間、戦略的な重要性、技術の古さ、既知のコントロールの欠陥等によって、保証の領域の中にある保証活動のポートフォリオで優先順位をつける必要がある。そうすることによって、組織にとって最もリスクの高い部分に保証業務の資源を割り当てることができる。優先順位づけは、(機能性、俊敏性、リターン、法令遵守性、安心感についての)ビジネスとガバナンスの目標によって行われ、**図16**で図示するように、特定の価値とリスクのドライバーを示唆している。この図は、ビジネスの達成目標をITの達成目標に変換するためには、IT資源の観点(すなわち、それに必要なサービスと情報の観点で)、また、必要なサービスと情報を提供しサポートするためにはそれに必要なインフラストラクチャと要員の資源の観点で考えることが有効であることも表している。COBITは、ある状況に合わせた後に、保証の領域の中で最も注意する必要のあるものを決定する手助けになるような汎用的に適用できる企業とITの達成目標を提供している。

図 16 保証計画のドラーバーとしてのビジネスと IT の達成目標

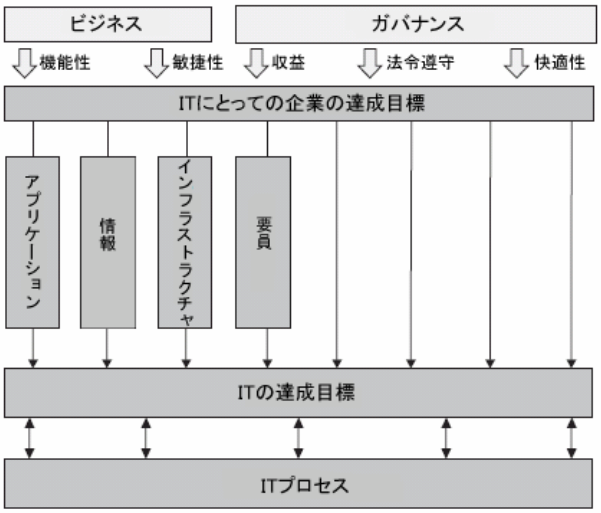
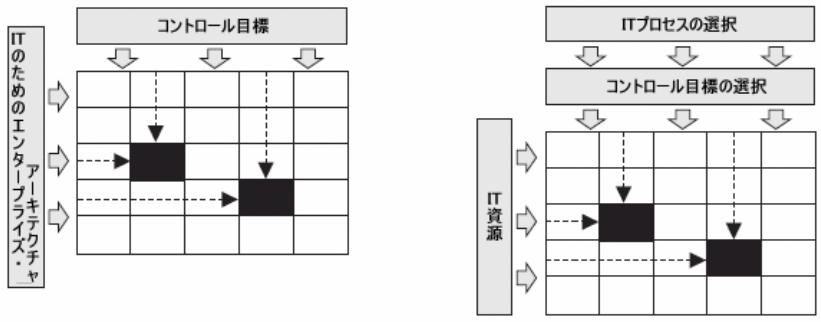


図17の左側に示すとおり、先に述べた分析作業から生じる保証領域は、大半の場合、二次元の表で表すことができる。1つの座標軸はITにとってのエンタープライズ・アーキテクチャからの関連要素であり、もう一方の座標軸はコントロール目標を示している。

図 17 エンタープライズ・アーキテクチャとコントロール目標との対応関係



推奨されるフレームワークはCOBITとそのプロセス構造であるから、保証業務の対象範囲を決定する際の最初のステップはプロセスを選択することであり、それにより横軸のコントロール目標を限定することができる。プロセスは横軸のコントロール目標に対応しているため、IT資源に注目すれば縦軸を簡略化することもできる。**図17**の右側が縦軸を簡略化したものである。他のプロセス志向でないコントロールフレームワークを用いる場合には、プロセスを縦軸にとる必要がある。しかしそうであっても、大半のフレームワークはCOBITに対応づけることができ（*www.isaca.org/cobit* を参照のこと）、対応づけした後は簡略化されたバージョンを用いることができる。

保証の領域を他の形で表すこともできる。どのような表現のしかたを選ぶにせよ、網羅性、一貫性、管理可能性との間のバランスを保たねばならない。提唱されている技法を使えば、すべての関連する単位を識別し記述することができる。 以下はその例の一部である。

- アプリケーションは、（販売、物流、管理、製造、人事といった、それがサポートする主要なビジネスプロセスに沿って）グループ分けするか、個別に列挙することができる。次に、開発フェーズやポートフォリオ管理を識別するために、アプリケーションに対するITプロセスとコントロール目標のサブセット（アプリケーションについての保証業務）を識別することができる。プロジェクトはよくプロジェクトの保証業務を通じてレビューされるが、そのようなプロジェクトは作成中のアプリケーションとみなすことができる。
- 要因とそれを組織する方法（組織単位）は保証の領域の横軸の一部であり、それにより、たとえば組織体に対する保証が可能である。
- ITインフラストラクチャの要素（データセンタ、ネットワーク、ITプラットフォーム）も横軸にあり、たとえばオペレーティングシステムとネットワークに対するセキュリティレビューの識別や、データセンタの物理的レビューの識別が可能である。
- 情報はデータベース、マスタファイル、取引ログを含む。

IT部門の多くで現在優先順位が高い特定の事項には、アウトソーシングプロジェクトや様々な法令遵守の要求事項が含まれる。保証の領域のプロセスの座標軸を通じて、保証業務の専門家は、アウトソースされたITサービスを管理するための関連ITプロセスを識別することができる（たとえばDS1サービスレベルの定義と管理およびDS2サードパーティのサービスの管理）。そうすることにより、この特定の事項を保証の領域全体の中に含めることができる。

リスクベースの保証計画

保証業務の専門家は、IT統制の保証の資源を効果的に割り当てるため、全体計画を策定する際に、適切なリスク評価の技法やアプローチを用いるべきである。リスク評価は、保証の領域の単位を調べ、最もリスクの高い領域をレビュー対象として選択するために用いる技法である。それぞれのITの層に関連するリスクは、ITに関連するリスクだけに注目してレビューしては決定できず、組織のプロセスと目標と共に検討しなければならない。
リスクには二つの主要な属性（発生可能性と影響度）があり、以下のような関連するものの属性の間に複雑な関係がある。

- **資産**—保護する価値のあるもの（有形のものも無形のものも）
- **脅威**—システムに害をなす可能性のある状況や事象
- **脅威となる作用因子**—脆弱性を利用するために用いる方法や物（決定、能力、動機、資源）
- **脅威となる対象事象**—システムが悪影響を受けるようなシステム脆弱性に対する脅威の事例
- **脆弱性**—脅威によって利用されうる弱点（開放されたファイアウォールのポート、一度も変更されたことのないパスワード、可燃性のカーペット等）。コントロールの欠如もまた脆弱性と考えられている。
- **対策**—コントロールの同義語。「対策」という用語は、いかなるタイプのコントロールを指すにも使われうるが、最もよく用いられるのは、ITサービスの回復力、耐障害性、信頼性を増す指標を指すときである。
- **リスク**—所与の脅威が資産の喪失や損害を引き起こすように、資産の脆弱性を突く可能性
- **残余リスク**—コントロールにより脅威となる対象事象の影響や発生可能性を減らしたときに、その事象に関して残っているリスク

図18は、異なる構成要素とそれぞれの主要な属性の相互関係を示している。これらの属性は、リスク分析プロセスに対するそれぞれの構成要素の貢献を分析するのに不可欠である。このプロセスで提唱されるアプローチを**図19**で示す。

本書で提唱されているリスク分析アプローチは、資産評価から始まる。これはCOBITフレームワークでは、ビジネスの目標を達成する際に役立つ、必要な判断基準がある情報（その情報を生み出すのに必要なすべての資源を含む）から成る。次のステップは、脆弱性分析である。これは、多くの情報サービスの可用性を決定する資産（データプライバシーを遵守するのに必要なビジネスプロセス、財務取引を扱う製品やインフラストラクチャの構成要素等）に当てはまる脆弱性を識別するものである。その次のフェーズでは、所与の脆弱性を突く重要な脅威（エラー、脱漏、事故といったような意図せざる事象、不正、ハッキング、盗難といった意図的な行為）を識別する。脅威の発生可能性、脆弱性の程度、影響の深刻度を組み合わせて、脅威/脆弱性のシナリオを作成し、そのリスクを評価する。次いで、対策（コントロール）を選択し、その費用と効果を評価する。選択したコントロールを導入することの影響を検討した後で、残余リスクが決定される。結果は行動計画であり、その後でそのサイクルが再び始まる。

図 18 リスク分析の構成要素の相互関係と属性

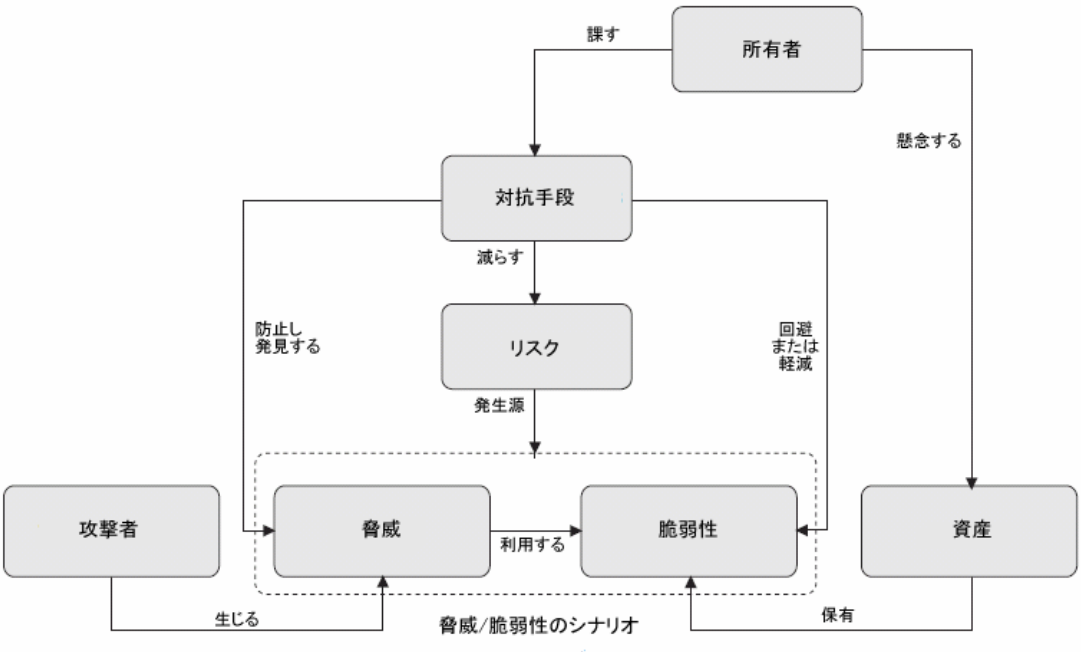
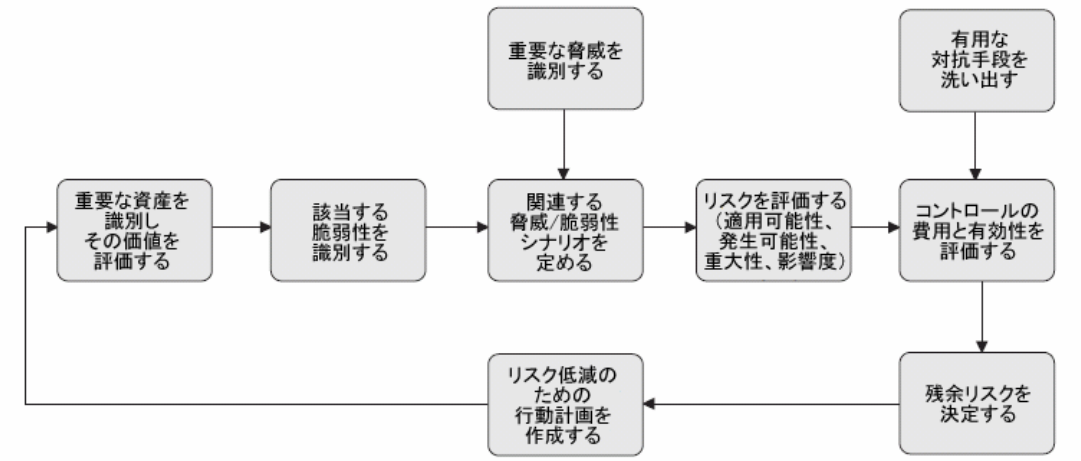


図 19 リスク分析の構成要素の相互関係と属性



高レベルでの評価

高レベルでの評価とは、成熟度/コントロールの現状とあるべき姿との間のギャップが最も重要であるようなプロセスを識別することであり、保証計画立案において有益である。いくつかの評価技法が存在し（それらはパフォーマンスとリスク属性に対する評価、プロセス成熟度の属性、コントロール目標、また成熟度の属性をカバーしている）、たとえば、**図21**で示すようなプロセスコンプライアンスプロファイルができる。

このような高レベルの評価の結果は、IT統制の保証の業務の優先順位をつける際に利用することができる。このような高レベルの評価の具体的な利点は以下の通りである。

- ITを統括する経営陣のメンバーに、ITをコントロールすることについての自らの説明責任を意識してもらい、賛同を得る

- 確立されたITコントロールの要件の遵守を高レベルでチェックする
- IT統制の保証の資源を最適化し優先順位をつける
- ITガバナンスとの橋渡しをする

保証業務の対象範囲と目標の定義づけ

また、IT統制の保証の専門家は、保証業務の期間内にすべての重要事項が十分にカバーされているという合理的な保証を提供するために、保証業務の対象範囲と目標とを明確に定義し、レビューすべき機能/活動の内部統制/成熟度の予備的な評価を実施すべきである。

高レベルの計画立案の評価を行うためには、*COBIT Quickstart* が実践的なサポートを提供している（*www.isaca.org/cobit* を参照のこと）。**図20**から**22**まで、コントロールと成熟度を高レベルで評価するために用いることができる異なったテンプレートを示している。**図20**にある最初のテンプレートは、経営者の自覚に関する診断であり、いくつかのパフォーマンスとリスクの属性に対するプロセスを評価している。あるITプロセスについてこのテンプレートを完成させることによって、関連するリスク（重要性とパフォーマンス）、責任（誰が行うか）、形式（文書化）、および保証の履歴と説明責任に関して迅速な洞察を得ることができる。

図 20 経営者の自覚診断

リスク		重要性—組織にとっての重要度を1（まったく重要でない）から5（とても重要）までの数字で評価してください。 パフォーマンス—1（とてもよい）から5（悪いまたは知らない）までの数字で評価してください。 形式—契約、サービスレベル合意、あるいは明確に文書化された手続きがありますか？（はい、いいえ、または？） 監査をうけましたか？—はい、いいえ、または？ 誰が説明責任を負いますか—名前または不明を記してください。	誰が行うか				監査	形式	誰が説明責任を負うか
重要性	パフォーマンス	COBITプロセス	IT	その他	外部	不明			
		PO1 IT戦略計画の定義							
		PO10 プロジェクト管理							
		AI6 変更管理							
		DS2 サードパーティのサービスの管理							
		DS5 システムセキュリティの保証							
		ME1 IT成果のモニタリングと評価							

次の2つのテンプレートは、成熟度の記述や成熟度の属性を用いて、プロセス成熟度の評価をどのように実行するかについての例を示している。**図21**の最初のテンプレートは、プロセス成熟度の説明から始まるが、それはいくつかの成熟度説明文に分解する必要がある。その説明文のそれぞれについて、コンプライアンスの値を定義する必要がある。これにより、IT統制の保証の専門家は「コンプライアンス・プロファイル」を算出できるようになる。

プロセス成熟度を評価する際のもう1つのアプローチは、成熟度の属性（COBITフレームワークで説明されているCOBIT成熟度モデル）を活用することである。プロセスの成熟度は、6つの成熟度の属性で評価することができる。

- 認識および周知
- ポリシー、計画、および手続
- ツールと自動化
- スキルと専門知識
- 実行責任および説明責任
- 達成目標の設定および成果測定

図 21 プロセス成熟度のコンプライアンス・プロファイル評価

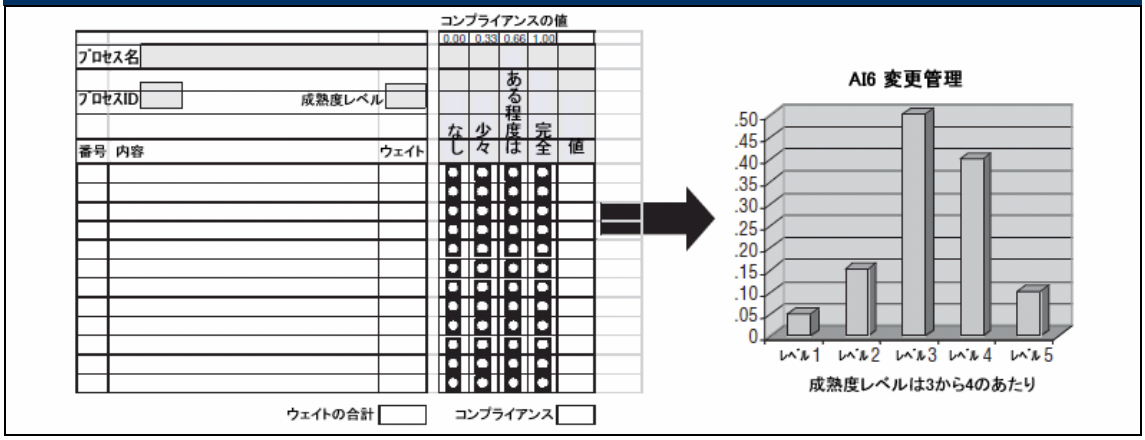


図 22 プロセス成熟度属性の評価

認識および周知	ポリシー、計画、および手続	ツールと自動化	スキルと専門知識	実行責任および説明責任	達成目標の設定および成果測定
1 プロセスの必要性が認識されつつある。 問題について散発的な周知が行われている。	プロセスと実践基準は場当たり的である。 プロセスおよびポリシーが定義されていない。	いくつかのツールが存在するものの、標準のデスクトップツールに準ずる形で使用されている。 ツールの使用については特に定められていない。	プロセスに必要なスキルが特定されていない。 研修計画が存在せず、正式な研修は行われていない。	実行責任と説明責任について定義されていない。問題が発生した場合は、要員がそれぞれの活動に基づいて事後的に対応している。	達成目標が明確でなく、成果測定は行われていない。
2 対応の必要性が意識されている。 経営層は、全体的な課題について周知している。	類似した共通のプロセスが採用され始めているが、個人の専門知識に依存しており、大部分において直感的である。 個人の専門知識により、プロセスのいくつかの局面は再現可能である。ポリシーと手続の一部が文書化されているか、非公式ではあるが認識されている場合がある。	ツールの使用に関する共通のアプローチは存在するが、主担当者が作成した対応策を基にしている。 ベンダーツールが入手されていたとしても、主担当者が作成した対応策を基に使用されている。 ベンダーツールが入手されていたとしても、正しく適用されていない場合や、使用されていない場合がある。	重要な領域に関するスキルの最小要件が特定されている。 研修は、合意済みの計画に沿った形ではなく、必要に応じて行われており、実地で非公式な研修が行われている。	責任に関する公式な合意は得られておらず、個人が各自の実行責任を想定し、説明責任も負っているものと認識されている。問題発生時には実行責任に関する混乱が生じ、責任転嫁が発生しがちである。	達成目標の設定が多少行われており、いくつかの財務対策が作成されているが、経営幹部にのみ周知されている。特定の領域のみにおいて、一貫性のないモニタリングが行われている。
3 対応の必要性が理解されている。 マネジメント層は、より正式化および構造化された方法で周知を行っている。	優れた実践基準が使用され始めている。 すべての主要なアクティビティについて、プロセス、ポリシー、および手続が定義され、文書化されている。	プロセスを自動化するため、ツールの使用方法と標準化に関する計画が定義されている。 ツールはその基本目的に合わせて使用されているが、合意済みの計画に完全には従っていない場合や、他のツールと統合されていないことがある。	すべての領域についてスキル要件が定義され、文書化されている。 正式な研修計画が作成されているが、正式な研修は依然として個人的な活動に基づいて行われている。	プロセスの実行責任と説明責任が定義されており、プロセスオーナが特定されている。実行責任を果たすために必要な全権限を、プロセスオーナが保有していない可能性が高い。	有効性の達成目標および測定指標がいくつか設定されているが、周知されていない。ビジネス達成目標との明確な関連付けは存在する。成果測定プロセスが作成され始めているが、一貫して適用されていない。ITバランススコアの手法が採用されており、根本原因の分析が時折、直感的に適用されている。
4 要件全体が理解されている。 成熟した周知技法が適用され、標準的な周知ツールが使用されている。	プロセスが完全な形で確立されている。内部のベストプラクティスが適用されている。 プロセスの全側面が文書化されており、再現性がある。ポリシーがマネジメント層によって承認され、受け入れられている。プロセスと手続の作成と管理が標準化され、遵守されている。	ツールは、標準化された計画に従って導入されており、一部のツールは関連する他のツールと統合されている。 プロセスの管理を自動化し、重要なアクティビティとコントロールをモニタリングするため、ツールが主要な領域で使用されている。	すべての領域についてスキル要件が定期的に更新されている。すべての重要領域についてスキル向上が保証され、資格取得が奨励されている。 研修計画に従って成熟した研修技術が適用され、知識の共有が奨励されている。社内の各領域の専門家が研修に関与しており、研修計画の有効性が評価されている。	プロセスの実行責任と説明責任が定着して、広く理解されており、プロセスオーナが各自の責任を完全に果たせるようになっている。成果に報いる報酬の文化が定着しており、積極的な対応が意欲的に取り組まれている。	効率性と有効性が測定および周知され、ビジネス達成目標およびIT戦略計画と関連付けられている。IT バランススコアカードが一部の領域に導入されており、例外があればマネジメント層により発見される。また、根本原因の分析が標準化されている。継続的な改善が行われ始めている。
5 要件が先進的かつ先見的に認識されている。 動向を踏まえ、先を見越した周知が行われ、成熟した周知技法が適用されて、統合された周知ツールが使用されている。	外部のベストプラクティスと標準が適用されている。 文書化されたプロセスを基に、ワークフローが自動化されている。プロセス、ポリシー、手続が標準化および統合されており、全体的な管理および改善が可能になっている。	標準化されたツールセットが企業全体で使用されている。 プロセスを完全にサポートできるように、ツールは、関連する他のツールと完全に統合されている。 ツールを使用して、プロセスの改善とコントロール例外の自動検知がサポートされている。	組織は、明確に定義された個人および組織の達成目標を基に、スキルの継続的な向上を正式に推奨している。 研修と教育は、外部のベストプラクティスと、最先端のコンセプトと技術の使用に対応している。知識の共有は企業文化となっており、ナレッジベースシステムが提供されている。外部の専門家や業界リーダーの指導を受けている。	プロセスオーナは、決定および対処に必要な権限を与えられている。実行責任の理解は、組織全体に一貫して浸透している。	IT バランススコアカードを全領域において適用することにより、IT 成果をビジネス達成目標に関連付けた、統合された成果測定システムが存在する。例外があれば、いずれの領域であってもマネジメント層により一貫して発見される。また、根本原因の分析が適用されている。継続的な改善が日常化されている。

図22で示すように、このような属性のテンプレート上での評価は、現状とあるべき姿との間の重要なギャップ、注意する必要のある領域、即効性のありそうな領域を示すことによって、IT統制の保証の専門家に、「道しるべ」となるスキームを提供する。

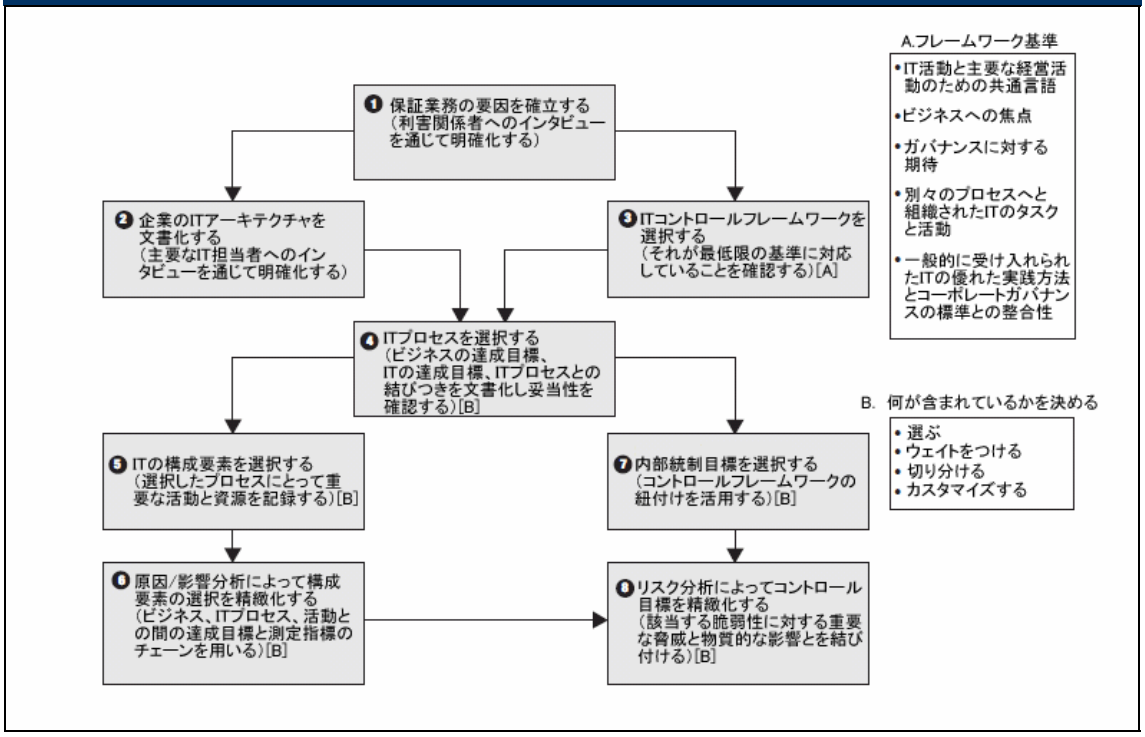
ITの資源とコントロールの対象範囲の決定

4. ITの資源とコントロールの対象範囲の決定

はじめに

IT統制の保証フレームワーク（**図23**で示されている）の2番目のフェーズは対象範囲の決定フェーズである。このステージでは、保証業務の実行ステージでの所与のITコントロールフレームワークの中で、ITの資源とコントロール目標のどれをカバーするかを決定する。対象範囲の決定は、該当するIT資源（アプリケーション、情報、インフラストラクチャ、要員）と該当するITコントロール目標とを結びつけ、それから特定のコントロール目標を達成できない場合の影響の重大さを評価することである。**図23**では、8段階の対象範囲決定プロセスを示している。

図 23 IT の対象範囲の決定のロードマップ



保証業務の対象範囲をあまりに狭く取ると、重要な要因を見落としかねない。保証業務の対象範囲をあまりに広く取ると、資源と時間の制約のために、非効率的で間違った結論がもたらされかねない。付録Ⅷ ITの対象範囲の決定では、IT統制の保証業務に適用できる汎用的な対象範囲の決定方法と他の様々なITガバナンスプログラムを提示する。

ITの資源とコントロール目標の対象範囲を決定するためのステップ

図24では、IT統制の保証業務の実施における対象範囲決定フェーズの中の8つのステップについて説明している。このステップを、以下に、さらに詳細に説明する。

ステップ1—保証業務のドライバーを確立する

最初のステップでは、保証業務のドライバーとそれに対応する保証の目標を識別する。第1章で述べたように、プロセスの改善をするとか、財務諸表監査のためにコンプライアンスの要請を満たすといったことを含む、保証のための多くのドライバーが存在する。保証業務のドライバーを確認することは、主要な利害関係者にインタビューしたり、保証の計画や憲章を調べたりすることによって達成することができる。

より具体的には、レビュー対象の企業の明確化されたビジネスの必要性をサポートするために、現在の役割と責任やITに要する資源とともに、レビュー対象の企業の境界を曖昧さなしに記述する必要がある。

保証業務の専門家は、以下についての理解を得るために、しかるべき経営陣と担当者にインタビューする必要がある。
- ビジネスの要件と関連するリスク
- 組織構造
- 役割と責任
- 方針と手続き
- 法律と規制
- 現在用いられているコントロール手法
- 経営者への報告（現状、パフォーマンス、行動）
- 過去の問題点とそれに対する是正活動
- 現在の問題点と懸念事項
- 経営者が保証業務の結果として得ようと望んでいるもの

ステップ2—エンタープライズITアーキテクチャを文書化する

2番目のステップでは、エンタープライズITアーキテクチャを文書化する。アーキテクチャの概念と要素については第3章で説明している。エンタープライズITアーキテクチャは、主要なIT担当者へのインタビューによっても検証することができる。

ステップ3—コントロールフレームワークを選択する

3番目のステップでは、適切なコントロールフレームワークを選ぶ。これは通常はCOBITだが、業務によってはCOSOだったり、類似した全社レベルのコントロールフレームワークだったり、関連するISOの基準といったような、より詳細なフレームワークや基準だったりする。

ステップ4—ITプロセスを識別する

適切なコントロールフレームワークを選んだら、次のステップで、適切なITプロセスを選び、適切なIT資源と結びつける。対象範囲内のITプロセスは、ビジネスの達成目標、ITの達成目標、ITプロセス相互間の関係を分析することを通じて識別することができる。

ステップ5—ITの構成要素を選択する

ステップ5については第2章で述べている。IT資源は以下から構成されている。
- アプリケーション
- 情報
- インフラストラクチャ
- 要員

保証業務に関連するIT資源を決定するために利用できるインプットは数多くある。後で行うリスク分析においてその業務の対象範囲から除外できる項目を決定するので、ここでは網羅性を優先すべきである。しかし、一覧表を合理的/実現可能な大きさに維持するためには、効率性も考慮する必要がある。以下のような異なる種類のインプットがある。
- 保証**業務のドライバー**—保証業務のドライバーは、レビューすべきITの構成要素とコントロール目標を決定するための最も重要な要因である。その典型例は、主要なサービスの中断、組織の変更、法令の遵守である。
- **ビジネスコントロールの要件**—このガイドの重点がIT統制の保証にあることを考えれば、必要かつ適用可能なビジネスコントロールの分析が行われていることを前提に、ITコントロールの対象範囲は、ITが自動

化されたビジネスコントロールをどのようにサポートするかに限定される。

- **エンタープライズITアーキテクチャ**—エンタープライズアーキテクチャは、情報サービスを提供するためのプロセス、組織が用いているアプリケーションとシステムのポートフォリオ、それを実行するのに用いる技術、およびアプリケーションを計画、構築、運用、サポートするのに必要な要員を含む。関連するIT資源やIT資源のグループについては、アーキテクチャから演繹することができる。

ステップ6—ITの構成要素の選択を精緻化する

プロセスと資源とを最初に結びつけるときには、保証業務の専門家はむしろ大きなポートフォリオ、おそらく保証業務の観点から費用対効果の高いものよりも広いポートフォリオを導き出すだろう。6番目のステップでは、保証業務の専門家は、資源を確実に業務に関連するプロセスに直接関係を持たせることによって、IT資源の選択を精緻化すべきである。

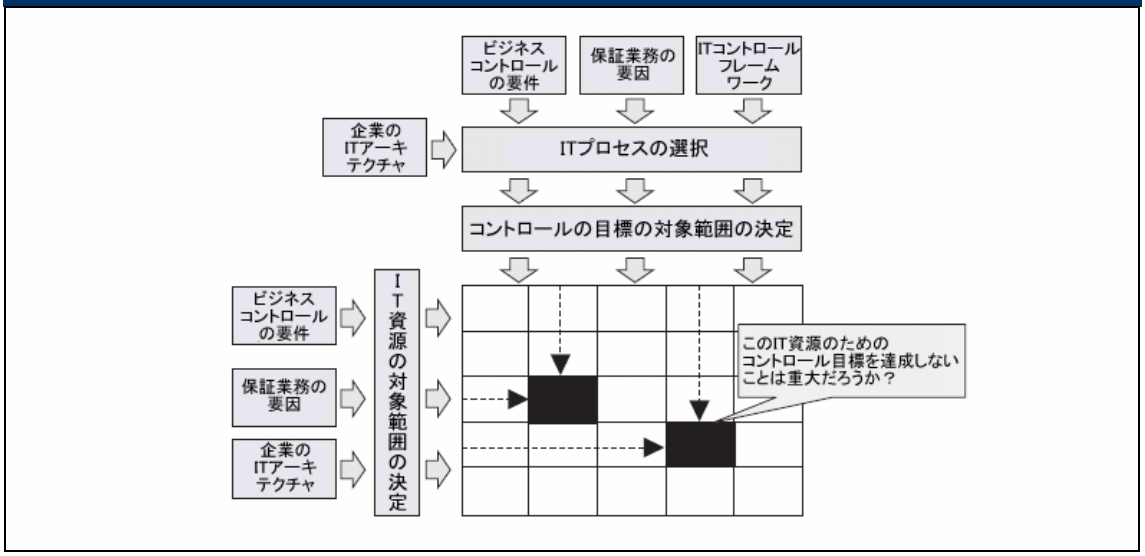
ステップ7—コントロール目標を選択する

保証業務の専門家は、まず、保証業務の対象範囲に含まれるITプロセスにとって関係のあるCOBITコントロール目標を選択する。企業の特殊な状況に即してコントロール目標をカスタマイズする必要のあることがよくある。ほとんどの業務において、IT資源の対象範囲の決定は企業の特殊な状況から始めるため、実証分析は必要ない。逆に、コントロール目標の対象範囲を決定する際には、1つまたは複数の汎用的なフレームワークから始めるため、さらなる分析が必要となる。COBITは、それぞれのコントロール目標で「リスクと価値」を明文化し、なぜ特定のコントロールが必要なのかを示すことによって、後のステップをサポートすることのできる材料を提供している。 選択されたコントロール目標をカスタマイズするだけでなく、企業の環境と保証業務の目標への対応づけもある程度必要である。

ステップ8—コントロール目標の選択を精緻化する

最後に、8番目のステップでは、保証業務の専門家はステップ6で詳述したIT資源の精緻化されたポートフォリオと、7番目のステップで選んだコントロール目標を最初に切り出したものとを関連づける。保証業務の専門家は、このプロセスを繰り返しながら、この特定の保証業務にとって関係あるコントロール目標のリストを精緻化し、しばしば体系化して小さくまとめていく。IT資源とコントロール目標とを結びつけるプロセスは、**図24**で示してある。

図 24 リスクベースの IT の資源とコントロールの対象範囲の決定



このステップでは、保証業務の専門家は、選択されたIT資源のために選択されたコントロール目標を達成できない場合のリスクを分析し、もしコントロール目標が達成されなかった場合重大な影響をもたらすようなIT資源とコントロール目標のみを残すべきである。

保証業務の専門家は以下を行うべきである。
- 対象範囲にあるIT資源を保つのに十分なリスクがあるかどうかを決定し、さらにレビューとテストを必要とするリスクの高い資源を識別するために、（**図24**の）表の横の行をレビューする。
- リスクの低いコントロール目標を取り除き、部分的な解決策ではなく企業全体の解決策を要する目標を識別するために、（**図24**の）縦の列をレビューする。

図24で示しているこのステップの重要な結論は、「このクラスのIT資源でこのコントロール目標を達成できないことは、この特定の保証業務にとって重大だろうか」という問いに答えるということである。「はい」と答えたマス目のみを最終的なITコントロールの対象範囲として残すべきである。

ITに関連するビジネスの達成目標とITの達成目標

IT統制の保証業務の専門家が保証の計画を立案する際に手助けとなるように、COBITは、ITに関連するビジネスの達成目標からIT達成目標そしてITプロセスに至る展開を、詳細に段階的に示している。COBITは17の汎用的なビジネス達成目標を定義しており、これらはITに直接影響するビジネスドライバーとサービスとを包含している。これらビジネス達成目標は、それを実現するためのIT達成目標に展開され、そしてそれがITプロセス達成目標へとつながっていく（COBIT4.1の付録1を参照のこと）。ビジネス達成目標、IT達成目標、プロセス達成目標を段階的に示したこの図は特に、保証業務のドライバーと、それが保証の領域にどのように影響するかを分析するときに有用である。

この段階的な達成目標の図は、保証計画立案の作業の手助けとなる。**図25**で示すように、保証業務が特定のビジネス機能に焦点を当てている場合、ITに関連するビジネス達成目標とIT達成目標は、保証計画立案時の価値あるインプットとなり得る。特定の組織の構成要素（たとえばプロセス）に焦点を当てた保証業務は、IT達成目標とITプロセス達成目標を、保証計画立案のための情報源として用いることができる。

図 25 IT 統制の保証計画のための、IT に関連するビジネス達成目標、IT 達成目標、および IT プロセス達成目標

		保証の主題				
		ビジネスの機能	主要なアプリケーション	重要な基盤の構成要素	組織の構成要素	主要な変更
達成目標についての情報	ビジネスの達成目標	P	S			P
	ITの達成目標	S	P	P	S	S
	ITプロセスの達成目標		S	S	P	S

(P=主要 S=副次的)

（空白ページ）

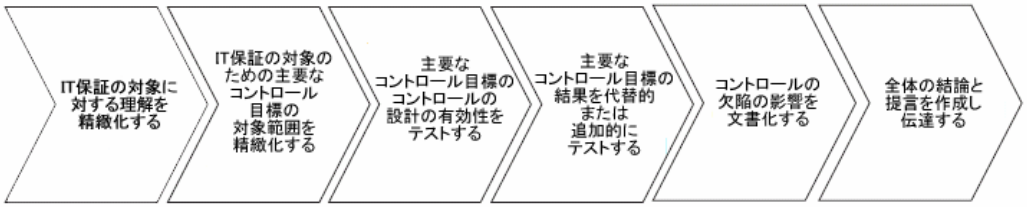
保証業務の実行

5. 保証業務の実行

はじめに

IT統制の保証フレームワーク（先に**図10**で示した）の3番目のステージは実行ステージである。**図10**では、保証業務の専門家が特定の保証業務を実行する上で従うことのできるロードマップを示している。この節の残りではこのロードマップを詳細に分析する。

図 10 実行のロードマップ



ステップ1—理解の内容を精緻化する

これから実施する保証業務のステップでは、コントロール目標を達成するためのアクティビティを文書化し、既に規定され運用されているコントロール手法/手続きを識別する。

実行ステージの最初のステップは、テストを実施する環境についての理解を精緻化することである。 これは、保証の正しい対象範囲と目標を選択するために、組織を理解するということである。保証の対象範囲と目標をすべての利害関係者に伝達して合意を得る必要がある。

このステップのアウトプットは、以下についての証拠を文書化することである。
- いつどこで誰がその作業を実施するのか
- 作業を実施するのに要するインプットと、その作業によって得られるアウトプット
- その作業を実施するための規定された手続き

保証業務の専門家は、以下の項目に沿ってこのステップを構築することができる。
- インタビューの実施、アクティビティリストとRACIチャートを利用する
- プロセスの記述書、方針、インプット/アウトプット、問題点、議事録、過去の保証業務報告書、過去の保証業務で出された勧告事項、ビジネスレポート等を収集して理解する。
- 対象範囲の決定作業の準備をする（プロセスの目的、レビューするプロセスの達成目標と評価指標）
- エンタープライズITアーキテクチャについての理解を培う

ステップ2—対象範囲を精緻化する

これから実施する保証業務のステップでは、保証プロジェクトの対象範囲を決定する。

IT環境についての最新かつ詳細な理解、ビジネスないし保証の目標に対してなされたあらゆる見直しをもとに、そして費用対効果の高いテスト計画を立てながら、対象範囲を適切に調節する。

したがって、保証の領域の最終的な範囲（たとえば、プロセス、システム、アプリケーション等）とレビューすべきコントロールの集合を決定するために、先に実施した対象範囲決定フェーズの成果を精緻化する必要がある。

ビジネスとITの達成目標を分析する

保証の目標と現状のビジネス目標に対するアプローチとを再調整し、ビジネスプロセス、ビジネスの達成目標、ITとそのプロセスや目標との関連についての理解を、最新のものにしておくべきである。最新の保証要件とIT組織とを念頭に置きながら、ITの達成目標を調節する必要があるだろう。

プロセスとコントロールを選択する

保証範囲の境界を確立するために、対象範囲に入れるITプロセス、ITコントロール目標、IT資源（アプリケーション、情報、インフラストラクチャ、要員等）の選択を精緻化すべきである。ITの構成要素のためのコントロール目標を達成しなかった場合に重大な影響が生じる可能性があるかどうかを評価することによって、プロセス、目標、関連する資源を選ぶことができる。

リスクを分析する

重要なコントロール目標が達成できないという固有リスクの評価に基づいて、対象範囲をさらに調整する必要があるだろう。このリスクに合わせて調整した対象範囲によって、保証業務でのレビューとそれに要するテストの分量が決まる。

対象範囲を最終決定する

すでに述べたように、保証戦略を設定し、目標、最適なテストアプローチ、評価したリスクについての最新の理解に基づいて保証のアプローチの対象範囲と焦点とを最終決定すべきである。ITプロセス、IT資源、ITコントロール目標の選択を、規定した戦略上、必要に応じて調整すべきである。保証の目標を最も有効かつ効率的に確実にカバーするために、何を文書化する必要があり、テストでどのようなアプローチを用いるかを決定すべきである。

ステップ3—コントロールの設計をテストする

この節では、詳細な保証業務のステップで用いる様々な技法を列挙する。

以下の主要なテスト目標（SAS70[1]やSysTrust™[2]保証にもある）をカバーしながらテストを実施する。
- コントロールの設計を評価する。
- コントロールが運用されていることを確認する。
- コントロールの運用の有効性を評価する。

加えて、コントロールの効率性もテストすることがある。

テストのフェーズでは、異なるタイプのテストを適用することができる。5つの汎用的なテスト方法は次の通りである。
- 質問および確認：
  - 例外/逸脱を探し、それを検証する。
  - 通常と異なったり定型的でなかったりする取引/事象を調査する。
  - 何かが起きたか（起きなかったか）どうか（サンプル）をチェック/決定する。
  - 独立した情報源から経営者の発言内容を確認する。
  - 担当者にインタビューして、その人の知識と意識を評価する。
  - 取引を照合する（たとえば取引を銀行明細書と照合する）

[1]監査基準書第70号「サービス・オーガニゼーション」は、米国公認会計士協会（AICPA）によって作成された、国際的に認知された一つの監査の基準である。

[2]SysTrustは、AICPAとカナダ勅許会計士協会（CICA）が作成した保証サービスである。

  - 発見事項を確認するために、経営者に質問して回答を得る。
- 閲覧
  - レビュー計画、方針、手続き。
  - 監査証跡や問題のログ等を調査する。
  - プロセス/システムを通じて取引を追跡する。
  - （文書や資産等の）存在を物理的に閲覧して確認する。
  - 導入物や計画書等のウォークスルーを行う。
  - 設計書やコードのウォークスルーを実施する。
  - 予測していた事項と実際の発見事項とを比較する。
- 観察：
  - プロセスを観察し記述する。
  - 手続きを観察し記述する。
  - 予測された行動と実際の行動とを比較する。
- 再実施ないし再計算：
  - 予想される結果を独自に作り出したり見積もる。
  - 何が防止されるかを試す。
  - 発見的コントロールによって何が発見されるかを再実施する。
  - 取引やコントロール手続き等を再実施する。
  - 独自に再計算を行う。
  - 期待値と実際値を比較する。
  - 予測された行動と実際の行動とを比較する。
  - プロセス/システムを通じて取引を追跡する。
- 自動的に収集した証拠のレビュー：
  - サンプルデータを収集する。
  - システムに組み込まれた監査モジュールを利用する。
  - コンピュータ支援監査技法（CAAT）を用いてデータを分析する。
  - 例外や重要な取引を抽出する。

次に、実施する保証業務のステップでは、コントロールの設計の妥当性を評価する。以下の3つの保証業務のステップを実施すべきである。
- コントロールに対するアプローチを観察/調査してレビューし、網羅性、関連性、適時性、測定可能性をテストする。
- コントロールプラクティスの責任と全体の説明責任が割り当てられているかどうか質問し、それらがきちんと割り当てられていることを確認する。説明責任と実行責任が理解され受け入れられているかどうかをテストする。適切な技能と必要な資源が利用可能であることを確認する。
- 関与している主要な担当者へのインタビューで、コントロールメカニズム、その目的、およびその説明責任と実行責任を理解しているかどうか質問する。

つまり、保証業務の専門家は以下を決定しなければならない。
- 文書化されたコントロールプロセスが存在するかどうか
- コントロールプロセスの適切な証拠が存在するかどうか
- 実行責任と説明責任とが明確かつ有効であるかどうか
- 必要に応じた補完的なコントロールが存在するかどうか

さらに、特に内部監査業務では、コントロールの設計が費用対効果の高いものであることを、以下の保証ステップによって確認すべきである。
- 設定されているコントロールプラクティスの設計が有効なら、ステップを最適化し、他のコントロールメカニズムとの相乗効果を模索し、予防対発見および修正とのバランスを再検討することによって、もっと効率的にできないかを調査する。コントロールプラクティスを維持するのに費やす労力を考慮する。
- 設定されているコントロールプラクティスが有効に運用されているなら、それをさらに費用対効果の高いも

のにすることができないかを調査する。設定されているコントロールプラクティスに関連するアクティビティの成果の測定指標、自動化の可能性、ないし技能レベルを分析することを検討する。

ステップ4—コントロール目標の運用状況（達成度）をテストする

これから実施する保証業務のステップでは、確立したコントロール手法が規定通りに一貫して継続的に機能していることを確かにし、コントロール環境が適切かどうかについて結論を下す。

コントロールの結果や有効性をテストするためには、保証業務の専門家はコントロールがプロセスのアウトプットの品質に及ぼす影響についての直接的および間接的な証拠を求める必要がある。これは、IT、プロセス、アクティビティのそれぞれの達成目標に対するコントロールの貢献を測定可能な形で直接的および間接的に具体化し、それによってCOBITで文書化したような結果を実際に達成した直接的および間接的な証拠を記録するということである。

保証業務の専門家は、ステップ3で提示したようなテスト技法の選択を適用することによって、レビュー対象のコントロールが有効に機能していることを保証するために、選択した項目/期間についての直接的または間接的な証拠を入手すべきである。保証業務の専門家は、プロセスの成果物の十分性に関する限定的なレビューも実施し、ITプロセスが十分であるという保証を提供するのに必要な、実証テストと追加的な作業のレベルを決定すべきである。

ステップ5—コントロールの欠陥の影響を文書化する

これから実施する保証業務のステップでは、分析的な技法を用いたり、代替的な情報源を検討したりすることにより、コントロール目標に合致しないことのリスクを具体化する。

コントロールの欠陥が見つかったときには、その重要性と機密性を考慮しながら、適切に文書化しなければならない。加えて、観察された欠陥の重要性と、ビジネスへの潜在的な影響を正しく分析し評価するために、特に注意を要する。

このステップの目的は、所与のビジネスプロセスとそれに関連するコントロール目標の達成についての保証（あるいは保証できないこと）を経営者に提供するのに必要なテストを実施することである。以下の場合にはさらに詳細な分析をすべきである。
- コントロールの手法が存在しない
- コントロールが期待通りに機能していない
- コントロールが一貫して適用されていない

こうすることによって、コントロールの欠陥とその結果として生じる脅威と脆弱性について完全に理解し、またコントロールの欠陥の潜在的な影響も理解することができるはずである。

コントロール目標を達成できない場合の影響を文書化するために、以下の保証業務のステップを実施することができる。
- コントロール目標が達成できない場合の影響を、同じ業界での実際のケースと関連づけ、業界のベンチマークを活用する。
- 既知の成果の指標と既知の結果とを結びつける。結果が存在しないときには、その原因と影響とを結びつける（原因/影響分析）。
- 何に影響を及ぼすかをわかりやすく例示する（ビジネスのゴールと目標、エンタープライズアーキテクチャの構成要素、能力、資源等）。
- コントロールの欠陥の影響を、エラー、非効率、誤用の数とシナリオによりわかりやすく例示する。

- コントロールが有効に運用されていないときによくある脆弱性と脅威を明確化する。
- 損益への影響、財務報告の完全性、無駄になった労働時間、販売機会の喪失、市場、消費者、利害関係者の要求に対処して応じる能力といった観点から、実際のコントロールの欠陥の影響を文書化する。
- 規制の要件や契約上の合意を遵守しない場合の影響を指摘する。
- 中断と停止とが実際にビジネスプロセスとビジネスの目標に及ぼす影響および顧客への実際の影響を測定する（数値、労力、作業中断時間、顧客満足度、費用等）
- 有効なコントロールによって防ぐことができたエラーのコスト（顧客と財務への影響）を文書にする。
- コントロールの欠陥によって影響を受ける効率性の指標として手戻りの費用を測定し文書にする（正常作業に対する手戻りの割合）。
- 有効なコントロールがある場合、事後的に、実際のビジネスへの利益を測定し、費用の節約をわかりやすく例示する。
- ベンチマーキングとアンケート調査の結果を用いて企業のパフォーマンスを他社と比較する。
- 問題点を示すために図を多用する。

COBITは以下の方法でサポートを提供している。

- プロセスの説明の中にある、ビジネス、ITおよびプロセスの達成目標、および情報要請規準は、もしコントロールを適切に導入しないとどのようなビジネスの価値がリスクにさらされるかを示す。
  コントロール目標ごとに、コントロールを改善することによって獲得できる利益と避けることのできるリスクとを示す、価値ドライバーとリスクドライバーについての記述がある。
- RACIチャートは、どの役割がリスクによって影響を受け、それゆえ実証テストの結果を誰に知らせるべきかを示している。
- 成熟度モデルは手軽で利用しやすく理解しやすいやり方で、社内だけでなく、他の業界や競合企業に対するベンチマークを行うために活用することができ、経営者のアクションを促す手助けともなる。ベンチマーキングデータはCOBITオンラインで入手できる。

ステップ6—全体の結論と提言を作成し報告する

これから実施する保証業務ステップでは、保証業務の様々な利害関係者に、コントロールの欠陥の具体的なリスクを伝達する。

保証業務の専門家はあらゆるコントロールの欠陥とそれによって生じる脅威と脆弱性を文書化し、（たとえば根本的原因の分析を通じて）実際の影響と潜在的な影響を識別し文書化すべきである。加えて、保証業務の専門家は、テスト結果を評価する際に用いる参考フレームワークを確立するために、（ベンチマークを通じて）比較可能な情報を提供することがある。これに対する潜在的なガイダンスとして、第7章「内部統制のための成熟度モデル」において内部統制のための汎用的な成熟度モデルを提示し、企業内での内部統制環境と内部統制の確立の状況を示している。この成熟度モデルは、内部統制の管理とより優れた内部統制を確立する必要性の認識を、その場対応のレベルから最適化レベルへ発展させる過程を示す。

その目的は、推奨される行動とその行動を取るべき理由を利害関係者に明確に伝えられるように、重要な項目を識別することである。 このフェーズでは、先のフェーズの結果を集約し、識別されたコントロールの欠陥についての結論を作成し、以下の項目を伝える

- コントロールの欠陥の影響を緩和するために推奨される行動
- 結果を相対的に見るための、現行パフォーマンスの標準的な活動およびベストプラクティスとの比較
- プロセスについてのリスクポジション

最終的に確定した保証業務の結論と勧告事項によって、責任当事者はさらなるステップを踏み、修復行動を取ることができるはずである。

保証業務の実行

保証業務が保証の付与を目的に実施される場合、保証業務の専門家は、正式な保証の伝達が求められ、ならびに保証報告基準・ガイドライン（*www.isaca.org*で入手できる）を遵守する必要がある。

（空白ページ）

COBITのプロセスとコントロールのための保証ガイダンス

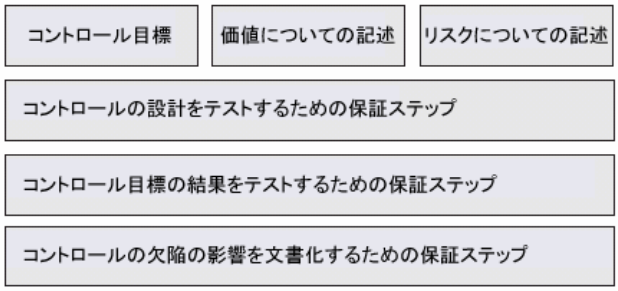
6. COBITのプロセスとコントロールのための保証ガイダンス

はじめに

この節では、COBITに基づく詳細なテスト実施ガイダンスの構造を述べ、すべてのITプロセスに当てはまる6つの汎用的なコントロール、COBITの34のITプロセスに基づくIT全般統制、6つのアプリケーションコントロールをカバーする。

コントロール設計のテスト、コントロールの結果のテスト、その影響の文書化のためのガイダンスを、付録 I からVIまでで、**図26**のレイアウトに沿って提供する。

図 26 付録 I からVIまでの詳細な保証アドバイスの構造



汎用的なプロセスコントロール

プロセスのそれぞれには汎用的なコントロール要件があり、それはプロセスコントロール（PC）のドメイン（付録 I を参照のこと）の中で汎用的なプロセスコントロールによって識別することができる。これは、すべてのCOBITプロセスに適用することができ、COBITのコントロール要件の全貌を把握するために、詳細なコントロール目標と共に検討すべきである。

詳細は付録 I で述べるが、6つの汎用的なプロセスコントロールは以下の通りである。
- PC1 プロセス達成目標とプロセス目標
- PC2 プロセスオーナーシップ
- PC3 繰り返し可能なプロセス
- PC4 役割と責任
- PC5 ポリシー、計画、手続き
- PC6 プロセスの成果の改善

汎用的なコントロールプラクティス

3つの汎用的なコントロールプラクティスと、それに起因する3つの汎用的な保証業務のステップが定義される。それは以下の通りである。
- アプローチ
- 説明責任と実行責任
- 伝達と理解

汎用的なコントロールの仕組みと特定のコントロールの仕組みを合わせることによって、既述のコントロール目標を達成するのに必要かつ十分な一貫したコントロールアプローチを得ることができる。異なった仕組みを組み合わせた他のコントロールアプローチも存在するので、コントロールの導入の手始めまたは保証活動の手始めに、コントロールの設計が適切かどうかを常に確認する必要がある。

アプローチ

アプローチについての汎用的なコントロールプラクティスは以下から成る。

- **汎用的なコントロールプラクティス**—このコントロール目標を達成するためのコントロールアプローチを設計し、この設計を実装するコントロールプラクティスを定義して維持する。
- **保証のステップ**—プラクティスの集合が目標を達成するように定義されたかどうか質問し、確認する。コントロールアプローチを観察/閲覧して、レビューする。網羅性、関連性、適時性、測定可能性について設計をテストする。

説明責任と実行責任

説明責任と実行責任についての汎用的なコントロールプラクティスは以下から成る。

- **汎用的なコントロールプラクティス**—コントロール目標全体のための説明責任と実行責任および異なるコントロールプラクティスの実行責任（COBITのRACIチャートを参照のこと）を定義して割り当てる。このような実行責任を果たすのにふさわしい技能と必要な資源を人員が持つようにする。
- **保証業務のステップ**—全体的な説明責任に加え、コントロールプラクティスのための実行責任を費用対効果が高く効率的なやり方で割り当てたかどうか質問して、確認する。説明責任と実行責任が理解され受け入れられているかどうかをテストする。ふさわしい技能と必要な資源が利用可能であることを確認する。

伝達と理解

伝達と理解についての汎用的なコントロールプラクティスは以下から成る。

- **汎用的なコントロールプラクティス**—コントロールプラクティスが、導入されたままの状態でコントロール目標に対処しており、伝達され理解されていることを確実にする。
- **保証のステップ**—関与している主要な担当者へのインタビューを通じて、コントロールのメカニズム、その目的、およびその説明責任と実行責任が伝達され理解されているかどうか質問する。

IT全般統制

全般統制は、自動化されたアプリケーションシステムが開発、維持、運用され、したがってすべてのアプリケーションに適用される環境と関係している。全般統制によって、すべての自動化アプリケーションを適切に開発、導入、維持することと、プログラム、データファイル、コンピュータ運用のインテグリティを確実にする。

COBITの34のITプロセスをどのようにテストするかについてのガイダンスを、COBITの4つのドメインに基づいて、4つの付録（付録ⅡからⅤまでを参照のこと）として構成し、提供している。

アプリケーションコントロール

アプリケーションコントロールは、自動化されたアプリケーションシステムのそれぞれに付随する取引と常設のデータと関係しており、アプリケーションによってそれぞれ特有である。アプリケーションコントロールは、手作業の処理と自動化された処理の両方からなり、記録の網羅性と正確性および取引とマスターデータでの入力の妥当性を保証する。これは、付録Ⅵのアプリケーションコントロール（AC）のドメインでさらに詳細に定義する。

IT統制の保証に関しても、アプリケーションコントロールと全般統制とが区別される。全般統制とはIT組織、そのプロセス、そのサービスに組み込まれているコントロールのことである。以下は、その例である。

- システム開発
- 変更管理

・セキュリティ
・コンピュータ運用

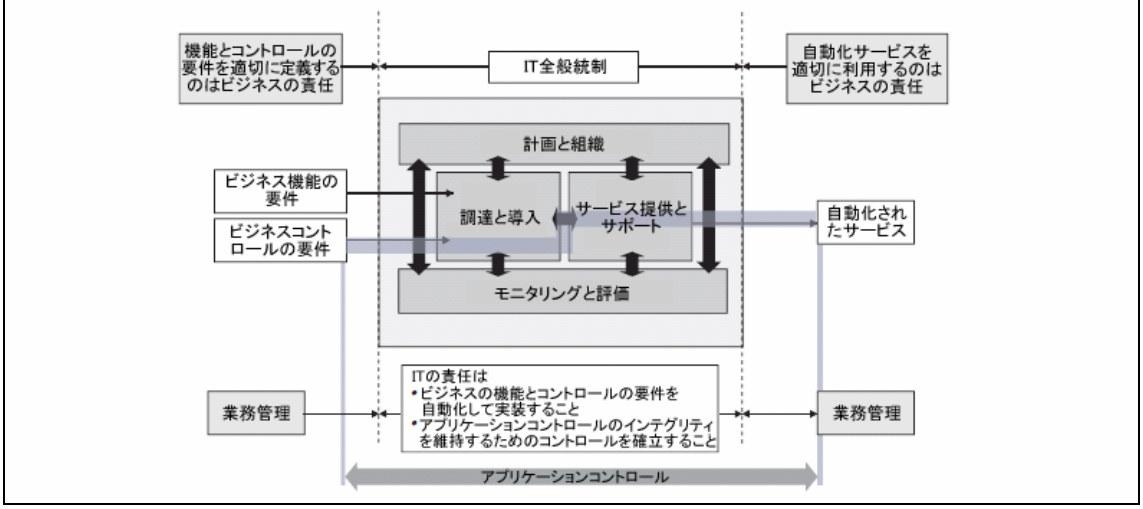
他方、ビジネスプロセスアプリケーションに組み込まれているコントロールは、通例、アプリケーションコントロールと呼ばれている。以下は、その例である。
・網羅性
・正確性
・妥当性
・承認
・職務の分離

したがって、アプリケーションコントロールの目標は、一般に、以下のことを確実にすることである。
・入力のために準備されたデータが網羅的で妥当で信頼できる
・データは自動処理可能な形式に変換され、正確、完全、かつ適時にアプリケーションに入力される
・データはアプリケーションによって、かつ確立された要件に沿って、完全かつ適時に処理される
・承認されていない改変や破損から出力が保護されており、規定された方針に沿って配布される

COBITでは、自動化アプリケーションコントロールの設計と導入はIT部門の責任であると想定しており、これはCOBITの情報要請規準を用いて定義したビジネスの要件に基づいて、調達と導入（AI）のドメインでカバーしている。アプリケーションコントロールの運用管理とコントロールの実行責任は、IT部門ではなくビジネスプロセスオーナにある。IT部門はアプリケーションのサービスとそれをサポートする情報のデータベース、インフラストラクチャを提供しサポートする。したがって、COBITのITプロセスは、アプリケーションコントロールではなくIT全般統制をカバーしている。これは、先に述べたように、アプリケーションコントロールはビジネスプロセスオーナに責任があり、ビジネスプロセスに統合されているからである。

ビジネスコントロールはCobiTやIT統制の保証ガイドの対象範囲外である。図27は、IT全般統制とアプリケーションコントロールとの境界線を設定しており、同時に、COBITがビジネスコントロールを扱う範囲にも線引きを行っている。

図 27 IT 全般統制と IT アプリケーションコントロール



自動化されたサービスでは、ビジネス部門の側に、そのアプリケーションがサポートするすべてのビジネスプロセスに対する機能要件とコントロール要件を定義する責任がある。従って、IT部門の責任は、ビジネスの機能要件とコントロール要件を自動化し、ビジネスアプリケーションのインテグリティを維持するためのコントロールを確立することを含む。

IT全般統制と汎用的なプロセスコントロールと同様に、COBITの6つのアプリケーションコントロールのそれぞれについて、設計と結果とをテストし影響を文書化するためのガイダンスを提供し、その詳細は付録VIアプリケーションコントロールで以下のように述べる。
- AC1 ソースドキュメントの準備と承認
- AC2 ソースドキュメントの収集とデータ入力
- AC3 正確性、網羅性、認証のチェック
- AC4 データ処理のインテグリティと妥当性
- AC5 出力のレビュー、照合、およびエラー処理
- AC6 トランザクションの認証とインテグリティ

アプリケーションコントロールの欠陥は、ビジネスプロセスとアプリケーションへの影響を通じて、企業がビジネストランザクションを処理する能力に影響するだろう。アプリケーションコントロールは企業のビジネスコントロールの一部である。アプリケーションコントロールの欠陥は、ビジネスと組織による補完的な手作業のコントロール活動によって軽減することができることがある。アプリケーションコントロールの欠陥の影響は、そのアプリケーションを使うビジネスプロセスの性質と、関連するトランザクションおよび他のビジネスプロセスコントロールの影響の観点で検討すべきであり、したがって、ビジネスプロセスの保証の提供者と相談することを検討すべきである。

詳細な保証業務のステップの利用例

保証のテストのステップをどのように適用するかについてのいくつかの具体例を以下に示す。

例1—コントロール設計のテスト

状況

AI6 変更管理のプロセスの AI6.2影響度の評価、優先順位付け、承認のコントロール目標を評価することによって、トランザクションを処理している部門でのIT全般統制をレビューする。

観察結果

選択したシステム（アプリケーション、プラットフォーム、ネットワーク）について、保証業務の専門家が、実施することのできる変更のタイプ、現在運用されている手続き（正式なものもそうでないものも）、変更管理プロセスに関与するすべての当事者、用いているツール等の棚卸を行った。これは、関係者へのインタビューと、文書化された手続きについての質問を通じて行われた。この作業の結果は、変更管理プロセスの包括的で正しいフローチャートとして示されていた。

保証業務の専門家は、「能力のある人やグループが変更の影響を評価する」という手続きで定義されているステップが存在するかどうかを決定するため、識別されたプロセスフローをレビューした。保証業務の専門家は、変更を要求し承認するためのテンプレートが、影響度の評価の部分を含んでいることを観察した。しかし、変更管理手続きでは、この情報が必須だと述べておらず、この情報が欠如していても変更要求を拒否するようになっていなかった。加えて、その手続きでは、いかなる文書化された基準も影響度の評価のために要求される検証と承認のステップを述べていなかった。

結論

このコントロールの設計には欠点がある。これは、コントロールの基礎的な構成要素（影響度の評価）が、どんなに良いとしても不完全だからである。適切なリスク評価を行わずに変更が実施されるということが可能であり、それによって、抑止の困難な計画外停止や機能不全が生じうる。

例2—コントロールの有効性のテスト

状況

AI6 変更管理のプロセスの AI6.3 緊急変更のコントロール目標を評価することにより、トランザクションを処理している部門でのIT全般統制をレビューする。

観察結果
コントロール設計の評価の一環として、保証業務の専門家は、関連する全ての主要な変更管理手続きで、緊急変更要求についても、再び通常の変更管理サイクルを確実に通すというコントロールが存在するということを識別した。加えて、保証業務の専門家は、すべての緊急変更が変更管理ツールに適切に記録されることを確かにするような手続きが存在することを発見した。
コントロールの有効性のテストの一環として、変更管理ツールから緊急変更要求のサンプルを選択し、それが通常の変更として再び処理されているかを追跡した。この追跡は、緊急変更が通常の変更として実際に再び処理されたかどうか、それが通常の変更管理手続きにしたがって処理されたかどうかを含んでいた。
保証業務の専門家は、選択した25の緊急変更のサンプルから、そのうちの3つが引き続き通常の変更として再び処理されなかったことを観察した。加えて、保証業務の専門家は、正規に再び処理された22の緊急変更のうち、10の変更のみが変更管理委員会で議論された、あるいは少なくとも、10の変更が議論されたことを示している利用可能な証憑が存在することを発見した（証跡は変更管理ツールに保存されている情報を含んでいた）。

結論
緊急変更手続きは以下の2つの理由により有効でない。
- すべての緊急変更がシステム変更管理で再び処理されているわけではなく、緊急変更が見えなくなり、それからの教訓も得られないというリスクがある。
- 再び処理された緊急変更も、十分に議論されず、文書化されていない可能性があり、上記と同様のリスクがある。

ステップ3—コントロールの欠陥の影響を文書化する

状況
AI6 変更管理のプロセスの AI6.3 緊急変更のコントロール目標を評価することによって、トランザクションを処理している部門でのIT全般統制をレビューする。

観察結果
先に述べたような状況により、保証業務の専門家は、コントロールの欠陥の影響を評価して文書化するために、追加的な情報を得てさらに分析する必要があった。先に述べた例では、保証業務の専門家は、コントロールの欠陥によって影響を受けた変更のタイプと数を検討する必要があった。

要求される情報のいくつかは、計画のステージですでに収集されているはずであるが、収集されていないものもあるかもしれない。記述された欠陥の重大性を評価するために、この情報を用いるべきである。とりわけ、影響を受けた変更を、関連するインフラストラクチャの構成要素とそれがサポート/処理するアプリケーション/情報へと対応づけるべきである。加えて、SLAに基づくペナルティが適用されるだろう。さらに、過去の問題の分析により、記述された欠陥の現実的な潜在影響を確定することができる。

このケースでは、変更管理の責任者との議論と他の変更管理委員会のメンバーとの確認の結果、重要でないシステムに関連する緊急変更の記録漏れと文書化の欠如は、単なる文書化の問題でしかなく、実際の変更とその原因と結果が議論されたものの、正式に文書化されてはいなかったということが判明した。

結論
コントロールの欠陥が観察されたままで残っているものの、追加的な分析と文書によれば、その欠陥は当初評価したほど重要ではなかったということを示していた。

CobiTの構成要素はIT統制の保証活動をどのようにサポートしているか

7. COBIT の構成要素は IT 統制の保証活動をどのようにサポートしているか

はじめに

図28は、典型的なIT統制の保証活動をCOBITの構成要素と結びつけたものであり、IT統制の保証活動をより効率的かつ効果的にするために活用することができる。これは、前の節で述べたIT統制の保証の推奨ロードマップに対するサポートをCOBITがどのように提供したかに加えて、スタンドアロンの作業として行われることの多い、保証に関連する特定の活動をCOBITがどのようにサポートしているかを示している。

IT統制の保証活動に対して特定の強いサポートがある部分のみCOBITの構成要素との対応関係を示した。しかし、すべての活動をサポートするいくつかの主要な構成要素がある。実用的には、COBITの利用者は、COBITのリソースを自らの特定の目的に応じて調整して適合させ、COBITが特定の作業にどのように価値を付加するかを発見することになる。したがって、この表はガイドに過ぎない。

最も有用な構成要素のうちの2つは、達成目標と成果測定指標、およびRACIチャート（主要な活動と実行責任）である。これらは、IT、そのプロセス、アクティビティ、目標のエッセンスを捕らえており、したがって、計画、対象範囲の決定、保証業務の実行のすべての側面をサポートしている。IT統制の保証活動にとって重要なもう1つの構成要素は、COBIT Onlineである。その検索と閲覧の機能によって、有用なベンチマーキングデータだけでなく、COBITの主要な構成要素のすべてに容易にアクセスできる。保証活動にとって重要なCOBITのこのような構成要素は、**図28**で網掛けをしてある。

図 28 IT 統制の保証活動と COBIT の構成要素との対応関係

	COBITの構成要素																
IT保証活動	コントロール目標	COBITコントロール活動	価値とリスクについての記述	成熟度モデル	成熟度モデルの属性	RACI(主要な活動で責任)	到達目標と結果の測定基準	パフォーマンスの要因	経営者の注意を引くためのツール	情報基準	プロセスリスト	Board Briefing on IT Governance, 2nd Edition	ITのリスクとコントロールの診断	COBIT Quickstart	COBIT Online—検索と閲覧	COBIT Online—ベンチマーキング	SOX法対応のためのITコントロール目標第2版
迅速にリスク評価を行う			✓	✓		✓	✓	✓	✓				✓	✓	✓		
脅威、脆弱性、ビジネスへの影響を評価する			✓			✓	✓	✓							✓		✓
業務上のリスクとプロジェクトリスクを診断する			✓			✓	✓	✓	✓				✓		✓		
リスクベースの保証イニシアチブを計画する	✓		✓	✓		✓	✓	✓	✓			✓	✓		✓	✓	✓
価値の原動力に基づいて重要なITプロセスを識別する				✓	✓	✓	✓		✓	✓	✓	✓	✓		✓	✓	
プロセスの成熟度を評価する				✓	✓	✓	✓		✓		✓	✓			✓	✓	
保証業務の対象範囲を決定し計画を立てる						✓	✓			✓	✓		✓		✓		✓
重要なプロセスに対するコントロール目標を選択する						✓	✓			✓	✓				✓		✓
コントロール目標をカスタマイズする	✓	✓			✓	✓	✓	✓							✓		✓
詳細な監査プログラムを策定する	✓	✓		✓		✓	✓						✓		✓		✓
コントロールをテストし評価する	✓	✓	✓		✓	✓	✓								✓		✓
リスクを実証する	✓	✓	✓			✓	✓	✓	✓	✓	✓				✓	✓	✓
保証の結論を報告する	✓	✓	✓	✓		✓	✓	✓	✓	✓	✓				✓	✓	✓
プロセスの成熟度を自己評価する	✓	✓		✓		✓	✓	✓	✓				✓		✓		
コントロールの自己評価を行う	✓	✓				✓	✓						✓	✓	✓	✓	

以下の節では、図28での最も重要な関係を、最初は構成要素の観点から、次いで活動の観点から要約する。その結論として、**図28**では、活動と構成要素との間の最も強い結びつきを丸で囲んである。

COBITの構成要素

コントロール目標とコントロールプラクティスは、関連するアクティビティをテストするのに最も有用であるが、コントロール目標が高レベルであり、主要な経営活動と類似しているので、活動を計画しているときにもコントロール目標を考慮することができる。保証業務のためにコントロール目標を選びカスタマイズするためにも、両者は有用である。

COBITのプロセスとドメインの一覧によって、IT部門の責任の構造を得ることができ、保証のカバー範囲の網羅性を確実にすることができる。この一覧は計画のフェーズで有用であり、また、保証業務の結論を要約するときにも有用である。同様に、情報要請規準は、ITプロセスの目標の汎用的で簡潔な高レベルの構造を提供し、保証の計画と結論を構造化するためにも同じくらい有用である。

成熟度モデルは、プロセスを評価し、主要なプロセスを識別し、保証プログラムで最も注意する必要のあるプロセスがどれかを計画するといったことを高レベルで行うために、そして保証の結論を要約するときにも、とても有用なツールである。成熟度の属性は、プロセス成熟度の評価のさらなる詳細を提供し、これはすべてのプロセスにとって汎用的なため、COBITのそれぞれのプロセスで提供されている特定のプロセス成熟度の説明の代わりにもなる。成熟度モデルは、プロセスを*どのように*管理するかを述べているので、詳細な属性は、コントロール目標をさらにカスタマイズするために用いることができる。コントロール目標は通常は*何を*する必要があるかのみを述べている。成熟度モデルは、次第により多くのIT管理責任者が自己評価のために用いるようになってきており、したがって、どこの領域に注意するかの優先順位付けについて、保証業務の専門家とITの専門家の両方が理解し合意するための共通のアプローチを提供している。

パフォーマンスドライバーは、IT統制の保証計画のロードマップと報告のフェーズでの保証活動にとって重要な役割を演じる一方で、コントロール目標をカスタマイズするためのすぐれた情報源でもある。これは、プロセスの達成目標とプロセス目標をうまく実現する確率を高めるために、何らかの行動を起こしたり、あるいは何らかの条件が存在したりすることの必要性を、パフォーマンスドライバーが示唆しているからである。

価値とリスクについての記述は、コントロールを正当化するための論旨を提供しているが、高レベルのリスク評価や詳細なリスク評価を実施するときの主要な情報も提供している。これらは、重要なプロセスとITの重要な構成要素を識別するときの起点でもある。
COBIT Onlineと*IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition* のCD-ROMで利用できるSupplemental Tools and Materialsで、経営者の意識診断のツールが提供されている。これは、通常はIT統制の保証業務の初期のステージで行われる、プロセスの重要性、重要なリスク、プロセスコントロールの状態に対する高レベルの評価を最初にするためのツールである。

COBIT Quickstart のプレゼンテーションで評価を行うことにより、効率的な自己評価だけでなく、迅速に高レベルの評価を容易に行うことができる。

COBIT Onlineで提供されているベンチマーキングデータと機能は、企業がプロセス管理とコントロールを、同業他社、同一地域の企業、同規模の企業と比較した結果を表すのに有用である。円グラフとレーダーチャートでこのような比較をサポートしている。このようなベンチマークは、保証活動の結論の信憑性を大いに高めるが、それだけでなく、保証業務のライフサイクルのより早い段階でも用いることができる（たとえば同業他社とのギャップのために、早期または詳細に保証業務のカバー範囲に含める必要のあるプロセスを識別するのに用いる）。

IT統制の保証活動

IT統制の保証活動が実施される事業体に対する深い理解を得る上で、保証業務の専門家に最高のサポートを提供するCOBITの構成要素は、プロセス構造、成熟度モデル、達成目標、成果測定指標、およびパフォーマンスドライバーである。

リスクベースのIT統制の保証の計画立案は、一般的な活動となり、最も潜在的なリスクが高いのはどこかを識別するため、COBITの成熟度モデルとCOBIT Onlineでのベンチマーキングで詳しくサポートされている。コントロール目標でのリスクと価値についての記述は、保証計画を推進するためにより詳細なリスク評価が必要な場合の追加的なサポートを提供している。意識診断のツールと同様に*Quickstart* もまた、高レベルの評価を迅速かつ効率的に行うための助けとなる。

計画と報告は—および対象範囲の決定も少々は—COBITの構成要素の大半を用いているが、通常は情報提供や参考資料に過ぎない。他方、詳細な計画と対象範囲の決定、およびテストは、COBITの構成要素をあまり広く使わない活動だが、より集中的に用いる傾向がある。計画、対象範囲の決定、およびテストは、COBITの心臓部分にあたる要素、すなわちコントロール目標を広範囲に用いるIT統制の保証活動でもある。

COBITとの密接なつながり

IT統制の保証活動とCOBITの構成要素とのつながりが最も密接な部分（どの活動がCOBITの題材から最も利益を受けているか）のいくつかは以下の通りである。
- リスクベースの保証業務の計画作成における達成目標と成果測定指標
- リスク評価とリスクの具体化におけるリスクと価値の記述
- 詳細な保証計画における主要な活動とRACIチャート
- コントロールのテストと評価におけるコントロール目標とコントロール活動
- プロセス成熟度と他の高レベルの評価における成熟度モデルと成熟度属性

ITGIの刊行物である*IT Control Objectives for Sarbanes-Oxley, 2nd Edition（サーベインズ・オクスリー法（企業改革法）遵守のためのIT 統制目標 第2 版）* もまた、COBITの構成要素とIT統制の保証活動との密接なつながりを提供している。

（空白ページ）

付録Ⅰ—プロセスコントロール（PC）

PC1　プロセス達成目標とプロセス目標
PC2　プロセスオーナーシップ
PC3　プロセスの反復性
PC4　役割と責任
PC5　ポリシー、計画、手続き
PC6　プロセスの成果の改善

付録 I —プロセスコントロール（PC）

プロセス保証のステップ

PC1 プロセス達成目標とプロセス目標

コントロール目標	価値のドライバー	リスクのドライバー
個々の IT プロセスを効果的に実行できるように、SMARRT（Specific;特有の目的、Measurable;測定可能、Actionable;実行可能、Realistic; 現実的、Results-oriented; 結果指向、Timely;タイムリー）なプロセス達成目標と目標を定義し、伝達する。IT プロセスの目標がビジネス達成目標に関連付けられ、適切な指標が定められていることを確認する。	・効率的かつ有効に測定された主要プロセス ・ビジネス目標に沿ったプロセス	・測定が困難なプロセスの有効性 ・プロセスによってサポートされないビジネス目標

コントロール設計のテスト

・達成目標と目的を伝達するための正式なプロセスが存在し、それが改訂されたときにはそのような伝達が繰り返されることを確かめる。
・プロセス達成目標とプロセス目標が定義されているかどうかを調査して、それを確認する。プロセスの利害関係者がこのような達成目標を理解していることを確認する。
・ITプロセスの達成目標がビジネスの達成目標に対応しているかどうかを調査して、それを確認する。
・プロセスの利害関係者へのインタビューを通じて、ITプロセスの達成目標がSMARRTであることを確認する。
・ITプロセスのそれぞれについて、アプトプットと関連する品質目標が定義されているかどうかを調査して、それを確認する。
・選択したプロセスの利害関係者に対してプロセス設計のウォークスルーを行い、プロセスが理解されその目標を達成しそうかどうかを確認する。

コントロール目標達成のテスト

・プロセスの測定指標、ターゲット、パフォーマンスの報告を分析して、プロセスの達成目標がSMARRTの特性を持っており、効果的かつ効率的に測定されていることを確認する。
・プロセス達成目標とプロセス目標の伝達の有効性を、様々なレベルの担当者との議論や研修教材、メモ、その他の文書の調査を通じて評価する。
・達成目標と目的の伝達の頻度が適切かどうかテストする。
・ビジネスの達成目標がITプロセスの間を追跡し、サポートされていないビジネスの達成目標を識別することによって、ビジネスの達成目標がITプロセスによってサポートされていることを確かめる。

コントロールの欠陥の影響の文書化

・プロセス達成目標とプロセス目標がビジネスの達成目標と結びついていない場合には、ビジネスへの影響を決定する。
・プロセスの達成目標がSMARRTのやり方で定義されていない場合のビジネスプロセスへの影響を評価する。

PC2 プロセスオーナーシップ

コントロール目標	価値のドライバー	リスクのドライバー
各 IT プロセスにオーナを割り当て、プロセスオーナの役割と責任を明確に定義する。たとえば、プロセス設計の責任、他のプロセスとの相互作用、最終結果に対する説明責任、プロセス成果の測定、および改善の機会の特定に伴う役割と責任を明確にする。	・ 円滑かつ信頼できる形で運用されているプロセス ・ 互いに有効に関連しているプロセス ・ 識別され解決されているプロセス上の問題や課題 ・ 継続的に改善されているプロセス	・ 信頼できない形で実施されているプロセス ・ 相互の連携が取れていないプロセス ・ プロセスの対象範囲間のギャップ ・ 修正されていないプロセスのエラー

コントロール設計のテスト

・ それぞれのITプロセスにオーナーが存在するかどうかを調査して、それを確認する。
・ プロセスの役割と責任とが定義されているかどうかを調査して、それを確認する。プロセスオーナーが自らの責任を理解し受け入れていることを確認する。
・ 役割と責任をサポートするのに十分な権限が提供されていることを、プロセスオーナーとその直接の監督者に確かめる。
・ プロセスと成果物に対するオーナーシップと説明責任を割り当てるためのプロセス（伝達を含む）が運用されていることを確かめる。

コントロール目標達成のテスト

・ 職務の割り当て、オーナーシップの理解と受け入れを確かめるために、プロセスオーナーの職務記述書と成果の査定をレビューする
・ 役割と責任が完全かつ適切であることを確かめるべく、それをレビューする。
・ 実際の権限を確認するために、組織図と報告系統をレビューする。
・ プロセス相互間の連携が取れていることを確かめる。
・ プロセスオーナーが継続的な改善を推進していることを確かめる。

コントロールの欠陥の影響の文書化

プロセスオーナーシップが、短期および長期の組織の目標に合致するためのビジネスプロセスサービスを達成することをサポートしているかどうかを評価する。

PC3 プロセスの反復性

コントロール目標	価値のドライバー	リスクのドライバー
期待される成果が一貫して得られるように重要なIT プロセスを、繰り返し可能なように設計し、確立する。期待される成果に結び付き、かつ例外や緊急事態にも即応できるような、論理的でしかも柔軟性とスケーラビリティに優れた一連のアクティビティを用意する。可能な限り一貫性のあるプロセスを採用し、不可避な場合に限り変更を加える。	・繰り返される活動で向上していく効率性と有効性 ・維持が容易であるプロセス ・有効性を監査人と規制当局に示すことができるプロセス ・IT部門の達成目標全体をサポートし、ITによる価値の提供を促進しているプロセス	・一貫性のないプロセスの結果と、プロセスのエラーの可能性 ・プロセスの専門家への強い依存 ・問題や新しい要件に対応できないプロセス

コントロール設計のテスト

・プロセスの反復性が経営目標になっているかどうかを調査して、それを確認する。
・重要でリスクの高いプロセスについて、プロセスのステップを詳細にレビューして、それが経営者のレビューのための証拠を提供していることを確かめる。
・ITプロセスを定義するときにどの(優れた)実践方法と業界標準を用いたかを確認する。
・選択したプロセスの利害関係者にインタビューして、プロセスを遵守しているかどうか決定する。
・システムが変更可能で柔軟に設計されていることを確かめる。

コントロール目標達成のテスト

・プロセスオーナーに対してプロセス設計のウォークスルーを行い、ステップが論理的で最終結果に貢献しそうかどうかを確かめる。
・プロセスの文書をレビューして、それに当てはまるプロセス標準が採用されているかどうかと、カスタマイズの度合いを確かめる。
・プロセスで用いている、サポートツールの成熟度と統合のレベルを評価する。

コントロールの欠陥の影響の文書化

プロセスの結果が目標に合致していないようなプロセスについてデータを選択し、その原因がプロセスの設計、オーナーシップ、責任と関係あるのか、あるいはその適用のしかたが一貫していないからなのかを分析する。

PC4 役割と責任

コントロール目標	価値のドライバー	リスクのドライバー
重要なアクティビティとプロセスの最終成果物を定義する。重要なアクティビティの効果的/効率的な実施をはじめ、プロセスの最終成果物に関する文書化と説明責任について明確な役割と責任を割り当て、伝達する。	・繰り返される活動で向上していく効率性と有効性 ・何をすべきであり、またそれがなぜなのかを知っていて、士気と仕事の満足度を高めている担当者	・コントロールされておらず信頼性が低いプロセス ・ビジネスの目標をサポートしていないプロセス ・意図した通りに実施されていないプロセス ・問題とエラーが解決されないで残っている可能性 ・一定しておらず信頼性が低い可能性のあるプロセスのパフォーマンス

コントロール設計のテスト

・主要な活動と成果物についての情報を定義し維持するためのプロセスが運用されていることを確かめる。プロセスが、それをサポートしているポリシー、手続き、ガイダンスの作成を含んでいることを確認する。
・達成を捕捉しそれを従業員の成果についての情報に含めるようにプロセスが設計されていることを確認する。

コントロール目標達成のテスト

・インタビューと文書のレビューを通じて、プロセスのための主要な活動と最終成果物が識別され記録されていることを確認する。
・職務記述書をレビューして、主要な活動のための役割と責任とプロセスの文書が記録され伝達されていることを確かめる。
・オーナー、経営陣、担当者へのインタビューを通じて、プロセスとそのアウトプットに対する説明責任が割り当てられ、伝達され、理解され、受け入れられていることを確認する。重要なプロセスインシデントの解決についての分析と職務の成果の評価のサンプルをレビューすることを通じて、インタビューでの知見を裏付ける。
・通常の職務成果の評価が、以下のようなプロセスの責任に対して実際の成果を評価するように実施されているかどうかを調査して、それを確認する。
  – 役割と責任を定義された通りに実行している
  – プロセスに関連する活動を達成目標と目的に沿って実施している
  – プロセスの最終成果物の品質に貢献している
・重要なプロセスインシデントの解決策をレビューし、職務成果の評価のサンプルをレビューして、実行責任と説明責任とが実施されているかどうかを確認する。
・様々な担当者に対して役割と責任のレビューを行い、彼らの理解、割り当てが適切かどうか、および報告の責任が有効かどうかを確認する。
・役割と責任が、その役割の中での様々な活動を遵守することをサポートするように設計されているかどうかを評価する。

コントロールの欠陥の影響の文書化

役割と責任が、短期および長期の組織の目標に合致するためのビジネスプロセスサービスを達成することをサポートしているかどうかを評価する。

PC5 ポリシー、計画、手続き

コントロール目標	価値のドライバー	リスクのドライバー
IT プロセスの実施のためのすべてのポリシー、計画、および手続に関する文書化、見直し、保守、承認、保管、周知、および研修について定義し、伝達する。これらのアクティビティについて適切な時期に責任を割り当て、それぞれが適切に実施されているかを見直す。ポリシー、計画、および手続が利用可能となっており、適切に定められ、理解され、最新状態に保持されているかを確認する。	・ 何をするのか、なぜそうするのかについて、高まっている担当者の意識 ・ ポリシー違反によるインシデント数の減少 ・ 最新かつ有効なポリシーとそれに関連する手続き	・ ビジネス目標と整合しないプロセス ・ 重要な作業をどのように実施するかを知らない担当者 ・ ポリシー違反

コントロール設計のテスト

・ ルールが存在し伝達され、知られており、ITプロセスを推進するような、ITプロセスに関連するすべての文書がどのように作成され、文書化され、レビューされ、維持され、承認され、保存され、伝達され、研修のために用いられているかを調査して、それを確認する。
・ 選択したポリシー、計画、手続きがルールに従って作成され、最新の状態を保っているかどうかを確認するために、それらを閲覧する。
・ プロセスに関連する文書を作成し、維持し、保存し、伝達する責任が定義されているかどうかを調査して、それを確認する。
・ 一貫したガイダンスを提供するために、ポリシーと手続きを識別し、作成し、承認し、レビューし、維持する、文書化された手続きが存在するかどうかを調査して、それを確認する。

コントロール目標達成のテスト

・ 活動を実施する人が自らの責任を理解していることを確認する。
・ 文書が最新の状態を保っており理解されていることを確認するために、選択した文書を閲覧する。
・ ITプロセスに関連する文書をレビューし、サインオフが適切なレベルで行われているかどうかを確認する。
・ ITプロセスに関連する文書が、容易にアクセスでき、的確で、理解されており、最新の状態を保っているかどうかレビューする。
・ ポリシーが意識喚起と訓練を通じて効果的に広められていることを確認する。
・ すべてのスタッフレベルでのインタビューを通じて、ポリシーと手続きが明確に理解されており、事業目標をサポートしているかどうかを評価する。

コントロールの欠陥の影響の文書化

ポリシー、計画、手続きのすべてが、短期および長期の組織の目標に合致するためのビジネスプロセスサービスを達成することをサポートしているかどうかを評価する。

PC6 プロセスの成果の改善

コントロール目標	価値のドライバー	リスクのドライバー
プロセスの結果と成果に関する洞察をもたらす一連の指標を見極める。プロセス達成目標と、目標達成に役立つ成果達成指標の目標を定める。データをどのように入手するかを定義する。実測値と目標値を比較して、逸脱がある場合は必要な対応策を講じる。IT 全体の成果モニタリングアプローチに従って、指標、目標、および方法を調整する。	・ 費用が最適化されているプロセス ・ ビジネスの必要性に対して敏捷であり対応できるプロセス	・ ITとビジネス目標全体に沿っていないプロセスの結果や成果物 ・ 費用がかかりすぎるプロセス ・ ビジネスでの必要性に対応するのが遅いプロセス

コントロール設計のテスト

・ 限られた労力による運用に対して高レベルの洞察を提供するように、主要な測定指標が設計されることを確立するためのプロセスが運用されているかどうかを調査して、それを確認する。
・ 測定指標の設計が、プロセスの達成目標の実現、資源の活用、結果の品質、プロセスのパフォーマンスと結果の改善をサポートするためのスループットタイムを測定できるようになっている。
・ 結果とパフォーマンスの測定指標との間の関係が定義され、必要に応じて企業の成果管理システム（たとえばバランススコアカード）に統合されているかどうかを調査して、それを確認する。
・ プロセスの達成目標とパフォーマンスの要因のための特定のターゲットを識別するための手続きが設計されているかどうかを調査して、それを確認する。その手続きでは、プロセスの測定を活用するためのメカニズム（たとえば自動化され統合されたツールやテンプレート）を含め、データをどのように入手するかを定義すべきである。
・ 実際の結果を入手し、確立された内部および外部のベンチマークと達成目標と比較するための手続きが存在するかどうかを調査して、それを確認する。主要なプロセスについて、経営陣がプロセスのパフォーマンスとプロセスの結果を内部および外部のベンチマークと比較し、プロセスの改善のための分析結果を検討しているかどうかを調査して、それを確認する。

コントロール目標達成のテスト

- プロセスのパフォーマンスとプロセスの達成目標の実現を評価するのに適切な測定指標が定義されているかどうかを調査して、それを確認する。
- 主要な測定指標のいくつかを分析し、他の手段を通じて、それらが達成目標に対して十分な洞察を与えているかどうかを確認する。
- プロセスの達成目標とパフォーマンスの要因のためのターゲットが定義されているかどうかを調査して、それを確認する。ターゲットをレビューし、それが達成目標と整合的であり、効率的で適切に修正行動を識別できるようになっているかどうかを評価する。
- モニタリングの有効性と効率性を確かめるために、データの収集と測定のための手続きをレビューする。
- 測定の方法とメカニズムが適切かどうかを評価するために、プロセスオーナーと利害関係者にインタビューする。
- 重要なプロセスの重要な達成目標について、データ収集とターゲットの測定を再実施する。
- 測定指標相互間の関係が適切かどうか（パフォーマンスの測定指標がプロセスの結果として達成できるものと思われるものに対する洞察を提供しているかどうか）を評価するために、プロセスの測定指標のサンプルを閲覧する。
- ターゲットからの主要な逸脱を入手してレビューし、行動を取ったことを確認する。測定の結果として取った行動の一覧を閲覧し、それが実際の改善につながったかどうかを確認する。
- 内部と外部のベンチマークが利用されているかどうかを評価し、もしそうならその関連性を評価し、ベンチマークからの重要な逸脱に対して適切な行動を取ったかどうかを識別する。

コントロールの欠陥の影響の文書化

プロセスの達成目標の実現、資源の活用、結果の品質、およびプロセスのパフォーマンスと結果の改善をサポートするためのスループットタイムを測定するための、一連の主要な測定指標が利用可能でない場合には、そのビジネスへの影響を文書化する。

付録Ⅱ—計画と組織（PO）

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プロセスと組織及び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　IT人材の管理
PO8　品質管理
PO9　ITリスクの評価と管理
PO10 プロジェクト管理

付録 II —計画と組織（PO）

プロセス保証のステップ

PO1 IT戦略計画の策定

ビジネス戦略およびビジネス上の優先順位に従ってIT資源の管理および割り当てを行うには、IT戦略計画の策定が必要である。IT部門およびビジネス部門の利害関係者は、プロジェクトおよびサービスのポートフォリオ（全体構成）から生み出される価値の最適化を実現する責任を有する。戦略計画を策定することにより、ITの利用機会および限界に対する主要な利害関係者の理解が深まり、現在の成果が評価され、必要な投資レベルが明確となる。ビジネス戦略やビジネス上の優先順位はIT戦略計画のポートフォリオに反映され、IT実行計画を通じて具体化されることになる。IT実行計画は、ビジネス部門とIT部門の双方から理解が得られ、承認を受けた簡潔な目標、計画、作業を定めたものである。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.1 IT価値の管理 ビジネス部門と連携することで、企業全体のIT関連投資のポートフォリオ（全体構成）に、ビジネス上の裏づけが確かな案件（プログラム）を確実に盛り込む。IT投資には、必須な投資、継続的に必要な投資、および選択可能な投資があり、それぞれ資金配分の多様性および自由度に違いがあることを認識する。ITプロセスでは、プログラムの推進のために必要とされるIT要素を効果的かつ効率的に提供する。また、プログラム進行にあたって、費用、日程、機能などの逸脱が認められ、かつ、プログラムに期待される結果に影響を与えるかもしれない場合には、これを早期に警告する必要がある。ITサービスは、公平かつ法的強制力のあるサービス・レベル・アグリーメント（SLA）に基づき実行されなければならない。便益の達成および費用の管理に関する責任の所在を明確にし、モニタリングする。公正で透明性が高く、再現可能かつ比較可能な評価方法を確立し、財務的な価値を含めたビジネス上の価値や計画を遂行できない場合のリスク、期待された便益が得られないリスクなどを評価する。	・ 透明性が高く、企業にとって効果的であるIT投資の便益 ・ ITに対する投資によって目に見える便益もたらすことを確実にする、効果的な意思決定プロセス ・ ビジネス目標に沿ったIT投資 ・ ITを用いた業務に関する費用、リスク、便益について共有された理解 ・ ビジネスの達成目標とITのための資源の利用との間の直接的な関係	・ 収益が十分でなかったり組織に悪影響が及んだりするようなIT投資を導く、効果的でない意思決定 ・ ビジネスと整合的でないIT ・ 上級経営陣の支援とコミットメントを欠いているIT価値の管理 ・ 未定義または混乱している説明責任と実行責任 ・ ITを用いた業務について、明確でなかったり、誤解されていたりする費用や便益、リスク ・ 経営陣と取締役会の公共的な責任に潜在的な影響があり、ガバナンス要件を満たしていないIT

コントロール設計のテスト

- ビジネスケースを作成するためのプロセスが存在するかどうかを調査して、それを確かめる（そのようなプロセスによって、ビジネスケース作成のための参入/出口基準、レビュープロセス、測定、ビジネスケースの変更管理プロセスが明らかになる）。
- ビジネスケースのモニタリングプロセスが、組織のSLAや業界標準と技術標準といったような、確立されたベンチマークに基づいているかどうかを調査して、それを確かめる。
- IT投資プログラムの成功と失敗のレビューを行い、ビジネスケース分析プロセスが要求通りに促進されているかどうかを調査して、それを確かめる（過去のデータを分析し、改善、教訓、ベストプラクティスを参照すべきである）。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.2 ビジネスとITの整合 双方向の教育と戦略計画における相互関与のプロセスを確立して、ビジネスとITの整合、および統合を実現する。ビジネスとITに関連する緊急課題を調整し、双方の合意を取り付ける。	・組織の使命と達成目標と整合的なIT ・ビジネスの戦略目標を達成できるIT ・最適化されているIT投資回収 ・識別され活用されているイノベーションの機会	・費用要因とみなされているIT ・ITによってサポートされていない企業の使命 ・ビジネスの方向性に従っていないITに関する経営陣の意思決定 ・資源の割当てと優先順位についての衝突につながる、ビジネスとITの優先順位に関する共通した理解の不足 ・新しいIT能力を活用する機会の逸失

コントロール設計のテスト

- ビジネスの機会をITマネジメント層に伝達するプロセスがレビューされ、そのプロセスの重要性がビジネスとITに伝達されていることを確認する。そのようなプロセスの更新頻度を考慮する。
- IT経営陣のメンバーに対するインタビューを通じて、IT経営陣が企業の達成目標の定義を手伝ったかどうか尋ね、それを確かめる。彼らに対して企業の達成目標の実現に関する説明責任について尋ね、what-if分析に着手したかどうかを決定し、達成目標に対する彼らのコミットメントを確かめる。
- ビジネスの経営陣とITマネジメント層に質問して、ITに依存するビジネスプロセスを識別する。ビジネスとITとで、重要性、利用、報告を含め、システムに対する同じ見方を共有しているかどうかを検討する。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.3 現在の能力と成果の評価 対応策とサービス提供にかかわる現在の能力と成果について評価を実施し、将来的な要件を比較する際に使用する基準を確立する。ITの成果について、ビジネス目標への貢献度、機能面、安定性、複雑性、コスト、長所、および短所の観点から定義する。	・高い透明性を伴って組織の使命と達成目標に貢献しているIT計画 ・ITの現在のパフォーマンスに関する費用、便益、リスクの明確さ ・識別された技術的な機会と活用された能力 ・要求されたソリューションとサービスを提供するために効率的で効果的な運用を可能にする、認知されたIT能力	・組織の使命と達成目標に貢献していないIT能力 ・遅すぎる投資の意思決定 ・活用されない機会と能力 ・効果的でない既存の資源の利用 ・現在のシステム能力とパフォーマンスや、将来の要求事項に関するベースラインを識別する能力の欠如

コントロール設計のテスト

・適切な判断基準、行動基準、成果の指標が確立しており、成果を評価してそれを経営陣と主要な利害関係者に報告するために用いていることを確認する。差異が生じた場合の行動計画と逸脱プロセスが存在すべきである。
・主要なシステムとプロセスのために確立された、成果の指標をレビューする（長所と弱点、機能性、ビジネスの自動化の度合い、安定性、複雑性、開発要件、技術の整合性と方向性、サポートと保守の要件、費用、外部者のインプット）。
・先のIT実行計画の中で定義された合意済みのターゲットの達成についてのレビューが存在することを確認する。
・周知で信頼できる産業、技術、その他の関連するベンチマークとの比較が行われ、既存のシステムと能力を評価できるようにしていることを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.4 IT戦略計画 利害関係者の協力のもと、ITがどのように企業の戦略目的（目標）の達成に貢献できるのか、そして関連コストおよびリスクにはどのようなものが考えられるのかを明確にした戦略計画を策定する。この計画では、ITが、IT関連投資のプログラム、ITサービス、IT資産の提供をどのように支援するのかを定める。またITにおいて、計画の中で目標がどのように達成されるのかに加え、使用する測定基準や利害関係者から正式な承認を得るための手続を定義する。IT戦略計画は、投資や実行予算、資金源、調達戦略、取得戦略、および法律上や規制上の要件を網羅する必要がある。またIT実行計画を定義する上で活用できるように十分に詳細である必要がある。	・目標と整合的であるIT戦略計画 ・明確ですべての要員に理解されている戦略目標と関連する説明責任 ・識別され構造化され、ビジネスの計画と統合されているIT戦略のオプション ・不要なIT業務の可能性の減少 ・完全かつ利用可能なIT戦略計画	・ITに関わる経営陣によって理解されておらず、取り組まれていないビジネス要件 ・ビジネスの上級経営陣とITに関わる経営陣との間の、定期的かつ正式な相談の欠如 ・ビジネスの必要性と整合的でないIT計画 ・不要なIT業務やIT投資 ・組織の期待や要求と整合的でないIT計画 ・正しい優先順位に焦点を当てていないIT

コントロール設計のテスト

- ITの作業を実施するのに必要な、ITの達成目標と目的を文書化するプロセスに従っているかどうかを調査して、それを確かめる。以下を含むITの作業を定義し、文書化し、伝達すべきである。
  - 利益を達成し、ITの能力のリスクを管理する
  - ビジネスの期待に応えるのに要する現在と将来のパフォーマンスを確立する
  - 透明性およびITがビジネスにどのように価値をもたらすかについての情報を提供する
- 戦略計画と実行計画を作成し実行するためのタイムフレームが存在するかどうかを調査して、それを確認する。このタイムフレームは、実行計画の実行の相互関連と依存性を含むべきである。タイムフレームは、対象範囲、予算、優先順位をもとに様々でありうる。
- ITの目標の測定指標（何を）とターゲット（どれくらい）によって表される結果の測定指標を捉えるためのプロセスが存在し、その測定指標がビジネスによって識別できる利益と戦略の方向性と関係あるかどうかを調査して、それを確かめる。
- IT戦略計画の作成プロセスを効果的にサポートするかどうかを決定する際の、構造的な計画作成アプローチを行うポリシーと手続きを確認してレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.5 IT実行計画 IT戦略計画に基づき、IT関連投資のポートフォリオの一部であるIT実行計画を作成する。 この実行計画では、IT関連のプログラム投資、ITサービス、およびIT資産への対応を検討する。 実行計画では、必要とされるIT業務、資源上の要件、および資源の利用状況と便益達成のモニタリング方法と管理方法を記載する。実行計画は、プロジェクト計画を定義する際に活用できるよう十分に詳細である必要がある。プロジェクトおよびサービスポートフォリオ(プロジェクトの結果として提供するサービスの全体構成)の分析を通じて、策定されたIT実行計画とIT業務を積極的に管理する。	・ 短期のIT実行計画によって運用可能な長期のIT戦略計画 ・ IT資源の効果的な配分 ・ 継続的にモニターし評価することができるIT計画 ・ 戦略ターゲットに対してモニターすることができるような、日々のパフォーマンスと資源の利用法 ・ IT部門とIT担当者に当てられた焦点	・ 達成されないIT長期計画 ・ 利用可能であるにもかかわらずビジネスの利益のために活用されていないIT資源 ・ IT計画における識別されない逸脱 ・ 理解されておらず、変更がありうるようなITの優先順位 ・ ITのパフォーマンスをモニターするための情報の欠如

コントロール設計のテスト
・ IT実行計画が存在し、それがIT戦略計画に基づいているかどうかを調査して、それを確かめる。 ・ 上記の事項が、確立されたプロセスに沿って、構造的な方法で行われており、IT戦略計画の更新がすぐにIT実行計画の更新に反映されることを確かめる。 ・ IT実行計画の内容が十分であり、適切なプロジェクト定義、プロジェクト計画情報、成果物、および定量的に評価できる利益を含んでいることを確認する。 ・ 実行計画がITに関連するリスクに対処しているかどうかレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
PO1.6 ITポートフォリオの管理 プログラムの検討、策定、評価、優先順位付け、選定、開始、管理、およびコントロールを通じて、戦略的ビジネス目標を達成する。そのために、IT関連投資のプログラム、すなわち、IT関連投資プロジェクトのポートフォリオを積極的に管理する。ポートフォリオ管理では、期待するビジネス成果を明確化し、その成果の達成に対して、プログラム目標の達成が貢献することを保証する。また、成果の達成に必要となる取り組みの全容を理解したうえで、指標を用いて責任範囲を明確化し、プログラム実施のためのプロジェクトを企画するとともに、資源および資金を割り当て、該当部署への権限委譲、プログラム買い指示において必要なプロジェクトの実行指示を行う。	・効率的なIT資源管理 ・継続的にモニターされ評価されているIT業務 ・リスク調整済みで、マイナスでない投資収益のためのIT業務の正しい組み合わせ ・定義されたターゲットに対してモニターされている、IT業務の成果と資源の要件	・保守的すぎるポートフォリオによるビジネスの機会の逸失 ・強気すぎるポートフォリオに起因する低い投資の収益率 ・利用可能であるにもかかわらず活用されていないIT資源 ・IT計画における識別されない逸脱

コントロール設計のテスト
・IT実行計画をサポートするITプログラムと、ITプロジェクトを識別し（ビジネスの利益をもとに）優先順位をつけることのできるようなプロセスが実施されているかどうかを調査して、それを確かめる。 ・このポートフォリオ管理のプロセスで、異なるプロジェクトとプログラムを定義して優先順位をつけるのにふさわしい判断基準を用いていることを確かめる。 ・ビジネスの達成目標と期待される成果が文書化されており合理的であるかどうかを確かめ、予算と労力に関して十分な情報が存在するかどうかを確かめる。 ・プログラム/プロジェクトの結果がすべての利害関係者に正式に伝えられていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

・運営委員会のメンバーへのインタビュー及びその他の情報源を通じて、運営委員会のメンバーがITとビジネスユニットのリーダーシップを適切に代表していることを確かめる（役割の自覚、責任、意思決定表、そのオーナーシップ）。
・承認された運営委員会規程をレビューして、その関連性（役割、実行責任、権限、説明責任、対象範囲、および目標が委員会のすべてのメンバーに伝達され理解されていること）を評価する。
・ビジネスケースを閲覧して、その文書の内容が適切であり（対象範囲、目標、費用便益分析、高レベルのロードマップ、成功の測定指標、役割と責任、既存のIT投資プログラムへの影響）、そのビジネスケースが適時に作成され承認されたことを決定する。インタビューを通じて、IT関連の投資プログラム、ITサービス、IT資産が優先順位付けの基準に対して評価されているかどうかを確かめる（文書化された優先順位付けの基準をレビューする）。
・IT経営陣のメンバーへのインタビューを通じて、将来のビジネスの方向性と達成目標、長期と短期の達成目標、使命、価値を彼らが知っていることを確かめる。
・企業の達成目標と目的がIT戦略計画とIT実行計画のプロセスに取り込まれ、戦略計画のプロセスが、ビジネスの活動と支援活動のすべてを含んでいるかどうかを調査して、それを確かめる。
・議事録やメモのような文書を調査することによって、ビジネスとITとが、新しいビジネスの機会を創出するために現在の技術を活用することに関与していることを確かめる。
・現在の情報システムについての報告（システムについてのフィードバック、システムになされた変更の改善

の利用を含む）が定期的に維持されていることを確かめる。
- 先のIT実行計画の中で定義された、合意済みのターゲットの達成をレビューする（パフォーマンス評価の結果は、現在の要件、現在の提供を要件と比較したもの、要件を達成することに対する障壁、合意済みのビジネスの達成目標と成果の要件を達成するのに要するステップと費用を含むがこれに限らない）。
- 要求されたIT能力がリスクと費用にどのような意味をもたらすかをIT戦略計画で文書化したかどうかを調査して、それを確かめる。
- ビジネスで識別された利益に関連する成果の測定指標が利害関係者によって承認されており、利害関係者からのフィードバックが検討されたことを確かめる。
- 承認されたIT戦略計画が伝達され、その計画が明確に理解されることを決定づけるようなプロセスが存在するかどうかを調査して、それを確かめる。
- インタビュー、議事録、プレゼンテーション、メモを通じて、IT戦略計画がIT運営委員会と取締役会に承認されたことを確かめる。正式な承認プロセスに従ったかどうかを調査して、それを確かめる。
- 実行計画が戦略計画と整合的であり定期的に更新されているかどうかを調査して、それを確かめる。インタビューを通じて、プロジェクト、資源の調達とスケジューリング、モニタリングの技法の実装を識別し計画するための基礎として、実行計画が用いられていることを確かめる。
- 実行計画の内容が、明確に記述されたプロジェクト定義、プロジェクトのタイムフレームと成果物、要求されている資源、モニターすべきビジネス上の利益、成果の指標の達成目標、リスク軽減計画、危機管理計画、意思伝達手続き、役割、責任を含んでいるかどうかを調査して、それを確かめる。
- 選択されたポートフォリオ/プロジェクトが、要求される労力、資源、資金、達成等に翻訳されており、ビジネスによって承認されていることを確かめる（議事録、上級経営陣のレビュー記録）
- 選択されたプログラムの中で承認されたプロジェクトを立ち上げるのに要する権限が、ビジネスとITから得られていることを確認する（議事録、正式な承認プロセス、プロジェクト承認の伝達）
- 遅延したり延期されたり継続しなかったりしたプロジェクトが、経営層とそれに関与したITスタッフメンバーに伝達されていることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- IT投資への配分が適切でないことによるリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。
- 投資の収益率がビジネスの達成目標の観点から最大化されていないことによる追加的な費用を評価する。
- IT投資が全体的なビジネスの戦略と適切に整合していないことによるリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。
- 要求に合致するために自己完結的なITシステムへビジネスの投資を行うことの影響を評価する
- ITサービスの提供に、業務側が満足していないような可能性を評価する
- IT戦略計画を実行することができないことによるリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。
- プロジェクトを開始したが、失敗したり不要な支出を要したりすることによるリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。
- 部分最適なソリューションを実装することによる追加的な費用を評価する。
- ビジネスの成果が理解されず、したがってあまり効果的でないことによるリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。

PO2 情報アーキテクチャの定義

情報システム部門は、ビジネス情報モデルの構築のみならず、これを定期的に更新し、ビジネス情報を最大限に利用できるシステムを定義する必要がある。
このビジネス情報モデルには、組織のデータ構文規則に従った企業データディクショナリ、データ分類体系、およびセキュリティレベルが含まれる。このプロセスは、安全で信頼性の高い情報を提供することを確実にすることにより、マネジメント層の意思決定の質を高める。また、情報システム資源をビジネス戦略に適切に合わせた合理的なものとする。このITプロセスにおいては、データのインテグリティおよびセキュリティに関する説明責任能力の強化のほか、アプリケーションおよび組織全体にわたる情報共有の有効性とコントロールの強化が必要である。

コントロール目標	価値のドライバー	リスクのドライバー
PO2.1 企業の情報アーキテクチャモデル 企業情報モデルを構築し維持することにより、PO1で述べたIT計画に合致した、アプリケーションの開発や意思決定支援活動を可能とする。このモデルは、ビジネス部門による情報の作成、利用、共有の最適化を促進するとともに、情報のインテグリティの維持はもちろん、柔軟性、機能性、コスト効率性、タイムリー性、安全性、障害回復性といった面でも有効に機能する。	・関連性と信頼性が高く、利用可能な情報に基づく、改善された意思決定 ・ITの俊敏性およびビジネスの要件への対応力の改善 ・正確で完全で妥当なデータを通じた、ビジネスの機能への支援 ・効率的なデータ管理、及び冗長性と重複の減少 ・データのインテグリティの改善 ・データに関するコンプライアンスレポーティング、セキュリティとプライバシーについての、受託者要件の充足	・ビジネスの機能に不十分な情報 ・情報の要件とアプリケーション開発との間の不整合 ・組織とシステムとの間でのデータの不整合 ・受託者の義務（コンプライアンスレポーティング、セキュリティ、プライバシー）を果たすのに要する多大な労力、あるいは受託者の義務を果たす能力の欠如 ・情報の欠落に起因する、ITを用いた投資プログラムの計画の非効率性 ・関連性、整合性、経済的な方法での利用可能性を欠くデータの蓄積

コントロール設計のテスト
・広く受け入れられた基準に基づく企業の情報モデルが存在するかどうか、及びそれがしかるべきビジネスとITの利害関係者に知られているかどうか確かめる。 ・そのモデルが、IT戦略計画をIT実行計画へ、そしてIT実行計画をプロジェクトへと翻訳するプロセスと並行して、効果的に利用され維持されているかどうか確かめる。 ・そのモデルで、柔軟性、機能性、費用対効果、セキュリティ、障害回復性、法令遵守等が考慮されているかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO2.2 企業データディクショナリおよびデータ構文規則 組織のデータ構文規則を組み込んだ企業データディクショナリを維持管理する。このディクショナリは、アプリケーションやシステムとの間でのデータ要素の共有を可能にする。また、IT部門とビジネス部門との間で、データに関する共通認識を促進し、互換性のないデータ要素の作成を防止する。	・ビジネスデータに対する全社共通な理解 ・すべてのアプリケーション、システム、組織で活用されるデータ共有 ・アプリケーション開発と保守の費用の減少 ・データのインテグリティの改善	・情報のインテグリティの毀損 ・互換性がなく整合的でないデータ ・有効でないアプリケーションコントロール

コントロール設計のテスト

- データ構文ガイドラインが維持管理されているかどうかを調査して、それを確かめる。
- データの冗長性や非互換性を識別するためのデータディクショナリが定義されており、データディクショナリの改変や変更のいかなる影響も効果的に伝達されているかどうかを調査して、それを確かめる。
- 様々なアプリケーションシステムとアプリケーション開発プロジェクトをレビューして、データディクショナリがデータ定義に用いられていることを確かめる。
- データ構文ルール、データ検証ルール、ビジネスルール（整合性、インテグリティ、品質）を定義するプロセスに、上級経営陣が合意しているかどうかを調査して、それを確かめる。
- データ品質プログラムの計画、ポリシー、その有効性を評価する手続きを閲覧する。

コントロール目標	価値のドライバー	リスクのドライバー
PO2.3 データ分類体系 企業データの重要性および機密性（公開可能、機密、極秘など）に基づき、企業全体で適用可能な分類スキームを確立する。分類スキームでは、データのオーナシップの詳細な内容と、適切なセキュリティレベル、および保護コントロールを定義する。また、データの保持および破棄にかかわる必要事項のほか、データの重要性と機密性に関する概要を盛り込む。この分類スキームは、アクセスコントロール、アーカイブ、暗号化などのコントロールを適用する上で使用すべき基準とする。	・意思決定を支援する情報の可用性の確保 ・重要度に応じたセキュリティ投資の焦点 ・情報のインテグリティ、可用性、セキュリティに関する定義された説明責任 ・定義されたセキュリティレベルに基づいて首尾一貫して許可されているデータアクセス	・不適切なセキュリティ要件 ・セキュリティコントロールへの不十分ないし過度の投資 ・プライバシー、データの機密性、インテグリティ、及び可用性に関するインシデントの発生 ・規制や第三者の要件の違反 ・効率性や整合性を欠く意思決定のための情報

コントロール設計のテスト

- データ分類スキームをレビューして、すべての重要な構成要素がカバーされ完成しており、そのスキームが費用とリスクとのバランスに関して合理的であることを確かめる。これには、経営層のデータオーナーシップと、分類レベルに関連する適切なセキュリティ指標を定義することが含まれる。
- 経営層と共に、定期的にセキュリティの分類に疑問をもち確認していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO2.4 インテグリティの管理 データベース、データウェアハウス、データアーカイブなど、電子的に保存されたすべてのデータのインテグリティと一貫性を確保する手続きを策定し、導入する。	・保存されているすべてのデータでのデータのインテグリティの一貫性 ・データのインテグリティの改善	・データのインテグリティのエラーやインシデント ・ビジネスの意思決定の基にするには信頼できないデータ ・規制や第三者の要件の違反 ・信頼できない外部報告

コントロール設計のテスト

・すべての情報のインテグリティと整合性の判断基準が、ビジネスの経営陣と共同で定義されているかどうかを調査して、それを確かめる。
・完全なデータプロセスとライフサイクルを通じて、データのインテグリティと整合性を維持管理するための手続きが実施されているかどうかを調査して、それを確かめる。
・データのインテグリティと整合性を検証し確かめるためのデータ品質プログラムが実施されているかどうかを調査して、それを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・情報アーキテクチャモデルの文書をレビューして、それが重要なすべてのアプリケーションとそのインターフェースと関係とを扱っているかどうかを決定する。
・情報アーキテクチャの文書を閲覧して、それが組織の戦略およびIT戦略計画、IT実行計画と整合的であることを確かめる。
・情報アーキテクチャモデルになされた変更が、IT戦略計画とIT実行計画の変更を反映しており、関連する費用とリスクが識別されていることを確かめる。
・ビジネスの経営陣とIT部門とが、情報アーキテクチャモデルでの関連する部分（データオーナーシップ、説明責任、データガバナンス）を理解しているかどうかを調査して、それを確かめる。
・情報アーキテクチャモデルの十分性、柔軟性、インテグリティ、セキュリティを定期的にチェックして、ユーザのレビュー（情報システムの変更の影響）を頻繁に受けているかどうかを調査して、それを確かめる。
・データ管理のコントロールが存在し、それが企業の情報モデルと一貫して、信頼性と関連性の高いデータの定義と実際の利用を調整しているかどうかを調査して、それを確かめる。
・データディクショナリをレビューして、重要なデータ要素が、定義されたプロセスに沿って適切に記述されていることを確かめる。
・定義されたデータ構文ルール、データ検証ルール、及びビジネスルールが定義されたプロセスの通りになっていることを確認する。
・データディクショナリのメタデータが、統合された方法でアプリケーションにおける構文を伝達するのに十分なほど詳細であり、それが、データ項目のそれぞれでデータ属性とセキュリティレベルを含んでいるかどうかを調査して、それを確かめる。
・組織のデータディクショナリとデータ構文ルールを管理するために、データ辞書管理を導入し、維持し、定期的にレビューしているかどうかを調査して、それを確かめる。
・データのリストをツールへの実装と比較することによって、システムがすべての関連するデータ要素をカバーしているかどうかを確かめる。
・データのインテグリティ、標準化、整合性、1回限りのデータ入力と保存を向上/促進するためのデータ品質プログラムが実施されているかどうかを調査して、それを確かめる（可能なときには自動化された証拠収集を用いて、サンプルデータ、内蔵監査モジュール、監査ソフトウェアやその他の統合ツールを用いたデータ分析から、データのインテグリティ、標準化、整合性、1回限りのデータ入力と保存をテストする）。自

動化されたツール（コンピュータの支援を伴う監査技法[CAAT]）を用いてデータのインテグリティを確認する。
- データ分類スキームが定義され承認されているかどうかを調査して、それを確かめる（セキュリティレベル、アクセスレベル、デフォルトが適切である）。
- 組織が情報を保護する必要性と、保護されていない情報がビジネスに及ぼす影響に基づいてデータ分類レベルが定義されているかどうかを調査して、それを確かめる。
- 情報の実際の分類を経営層がレビューしており、データに対する役割、実行責任、説明責任を意識していることを確かめる。
- 構成要素が、当初の資産の分類を引き継いでいるかどうかを調査して、それを確かめる。
- データ分類引継ぎのポリシーからのすべての逸脱事項が、データオーナーによって承認されていることを確かめる。
- 情報とデータ（データのハードコピーを含む）にラベルをつけ、取り扱い、保護する等、データ分類のカテゴリーと整合的な方法で情報とデータのセキュリティを保っているかどうかを調査して、それを確かめる。
- データに要求されているインテグリティと整合性の判断基準が定義され実施されている（データベースとデータウェアハウスにそれぞれ格納されたデータが整合的である）という証拠を閲覧する。
- 定期的にデータのインテグリティと整合性を検証し保証するためのデータ品質プログラムが実施されているかどうかを調査して、それを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- IT戦略計画で記述されているIT計画と企業の情報アーキテクチャモデルとの非整合性の影響を評価する。
- ビジネスとITとの意思決定の間のインターフェースが有効でない場合の影響を評価する。
- 取扱いに注意を要する情報の開示についての脆弱性を評価する。

PO3 技術指針の決定

情報サービス部門は、ビジネス部門を支援するために技術指針を定める必要がある。そのためには、技術インフラストラクチャを計画する必要がある。また、製品、サービス、および提供手段に関して、技術が、どのような貢献ができるかについて、明確かつ現実的な見込みを立て、これを管理するアーキテクチャ委員会を設置しなければならない。技術インフラストラクチャ計画は定期的に更新され、システムアーキテクチャ、技術指針、調達計画、標準、移行戦略、および緊急時対応などの観点を含む。これにより、プラットフォームとアプリケーションとの間の相互運用性の改善、競争的な環境における変化へのタイムリーな対応、および情報システム要因の確保と投資におけるスケールメリットを実現できる。

コントロール目標	価値のドライバー	リスクのドライバー
PO3.1 技術指針計画の策定 既存技術および将来性のある新技術を分析し、IT戦略とビジネスシステムアーキテクチャの実現に適した技術指針を計画する。また、ビジネスチャンスの創出が期待できる技術を、その計画の中で特定する。この計画では、インフラストラクチャの構成要素であるシステムアーキテクチャ、技術指針、移行戦略、および緊急時対応の側面を検討する必要がある。	・ビジネス機会のための技術の活用の改善 ・技術指針に従い定義された標準を通じて改善された、インフラストラクチャとアプリケーションとの統合 ・資源と能力の利用の改善 ・プラットフォームを減らし、投資に対する管理を増すことによる、技術獲得のための費用の減少	・戦略計画と整合的でない技術獲得 ・組織の要件にふさわしくないITインフラストラクチャ ・承認された技術指針からの逸脱 ・調達計画の調整と構造化が行われていないことによる費用の増加

コントロール設計のテスト
・長所、弱点、機会、脅威（SWOT）分析のプロセスの結果をレビューして、プロセスの有効性を確かめる（プロセスの測定と改善の結果としてプロセスになされた変更をチェックする）。 ・CIOおよび上級経営陣のその他のメンバーへのインタビューを通じて、ビジネスの戦略に基づいて、適切な技術リスクへの意欲が確立されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO3.2 技術インフラストラクチャ計画 IT戦略/実行計画に沿った技術インフラストラクチャ計画を策定および維持する。この計画は技術指針に基づいて策定し、緊急時対応策および技術資源の調達に関する指針を含める。プラットフォームとアプリケーションとの間の相互運用性の改善、競争的な環境における変化へのタイムリーな対応、および情報システム要員の確保と投資におけるスケールメリットについて考慮する。	・相互運用性の改善 ・投資と情報システム要員の確保に関するスケールメリットの改善 ・費用、要件、敏捷性、リスクとの間でバランスの取れた技術計画 ・情報の要件に対応するのに十分で、安定的で、柔軟な技術インフラストラクチャ	・システムの実装の不整合 ・承認された技術指針からの逸脱 ・獲得計画の調整と構造化が行われていないことによる費用の増加 ・ビジネスとIT能力を改善するための、新技術の機会を最大限に活用できない組織上の不備

コントロール設計のテスト

- IT戦略/実行計画に基づいた技術インフラストラクチャ計画が作成されていることを、主要な担当者に確認する。
- その計画をレビューして、それが、整合的で統合された技術、ビジネスシステムアーキテクチャ、インフラストラクチャの構成要素の緊急時対応の側面、移行費用とその他の費用、複雑性、技術的なリスク、将来の柔軟性の価値、製品/ベンダの持続可能性、IT資産調達の指針といったような要素を含んでいることを確かめる。
- 主要な担当者に尋ね、技術インフラストラクチャ計画を閲覧して、競合環境、情報システム要員の確保や投資におけるスケールメリット、プラットフォームとアプリケーションの相互運用性の改善が識別されていることを確かめる。

コントロール目標

PO3.3 将来の動向および規制のモニタリング

ビジネスの分野、業界動向、技術動向、インフラストラクチャの動向、および法規制関連の動向をモニタリングするプロセスを確立する。これらの動向の影響を考慮したIT技術インフラストラクチャ計画を作成する。

価値のドライバー

- 技術の機会への意識の改善とサービスの改善
- 技術と規制のリスクへの意識の改善
- ビジネス計画に沿った技術の変更に対する評価の改善

リスクのドライバー

- 規制上の要件の違反
- 意思決定が誤っていたり遅れたりすることで、法令遵守を達成するのに要する多大な労力
- ITインフラストラクチャの中での技術的な不整合や維持管理に関する問題
- ビジネスとIT能力を改善するための、新技術の機会を最大限に活用できない組織上の不備

コントロール設計のテスト

- 現在と将来の動向や、規制をモニターしているかどうか、誰がどのようにモニターしているか（技術開発、競合企業の活動、インフラストラクチャの問題点、法的な要件と規制環境の変化、外部の専門家）、それに関連するリスクや価値を創出する機会を評価しているかどうかを決定する。
- モニタリングの結果が適切な主体（IT運営委員会）に、そしてIT実行計画とインフラストラクチャ計画の実行プロセスへと一貫して渡されているかどうかを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO3.4 技術標準 一貫性があり、効果的かつ安全な技術的対応策を企業全体に適用するため、技術フォーラムを設置して、技術的なガイドライン、インフラストラクチャ関連製品に関する助言、および技術選択の指針を提示する。また、これらの標準やガイドラインなどの文書に対するコンプライアンス状況を測定する。このフォーラムでは、ビジネスとの関連性、リスク、および外部要件へのコンプライアンスに鑑みて、技術標準および実践方法についての指示を行う必要がある。	・情報システム資産の調達、変更、廃棄に対するコントロールの増大 ・技術指針をサポートし、技術指針との整合性を増し、リスクを減少させる標準化された調達 ・リプレースの費用を減らす、拡張可能な情報システム ・効率性を高め、サポート、ライセンス、保守の費用を減らす、企業全体を通じた技術の一貫性	・技術プラットフォームとアプリケーションとの間の不整合 ・承認された技術指針からの逸脱 ・ライセンス違反 ・サポート、リプレース、保守の費用の増加 ・サポートされていない技術による、過去データへのアクセス可能性の欠如

コントロール設計のテスト

・企業の技術標準がITアーキテクチャ委員会に承認されていることを確かめる。技術標準をIT業務担当者（プロジェクトマネージャ、情報アーキテクト）に伝達するプロセスの有効性を評価する。関連するIT担当者にインタビューして、彼らが技術標準を理解していることを決定する。
・ITマネジメント層から、確立された技術標準とガイドラインへの遵守を確かめるための、モニタリングとベンチマーキングのプロセスが運用されていることを確定する。
・選択したプロジェクトに対して技術の利用可能性の分析についての文書を評価して、企業の技術標準への遵守の度合いを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO3.5 ITアーキテクチャ委員会 ITアーキテクチャ委員会を設置し、アーキテクチャに関するガイドラインとその適用に関する助言を適用するとともに、それらに対するコンプライアンスを確認する。ビジネス戦略の実現を可能にし、法規制の遵守と継続性の要件が考慮されたITアーキテクチャの設計を委員会が指揮する。ITアーキテクチャは、PO2 情報アーキテクチャの定義に関連付けられる。	・アーキテクチャに関する意思決定に対する説明責任と実行責任の増加 ・ビジネス戦略とITの技術指針との間の整合性の増加 ・全社的な技術アーキテクチャに対する一貫性のある理解	・技術プラットフォームとアプリケーションとの間の不整合 ・承認された技術指針からの逸脱 ・情報システム資産の調達、利用および潜在的な増設に対するコントロールの欠如

コントロール設計のテスト

・ガイドライン、計画、プロセス、アーキテクチャ委員会の議事録をレビューする。これらが、ビジネスの戦略と確立された情報アーキテクチャに沿って、アーキテクチャガイドラインと関連する助言を与えているかどうかを確かめる。
・アーキテクチャ委員会が規制の遵守と事業継続性を意思決定の際に考慮したかどうかを確かめる。
・アーキテクチャ委員会の標準とガイドラインに遵守していないことを確実に発見するようなメカニズムがプロジェクト管理プロセスで運用されていることを確かめる。
・プロジェクト管理プロセスにおいて標準を遵守していないことによって発生した是正活動のフォローに関して、アーキテクチャ委員会の役割を評価する

コントロール目標の達成をテストするために以下のステップを踏む。
・SWOT分析の結果をレビューして、ビジネスシステムアーキテクチャ、技術指針、移行戦略、緊急時対応の側面が技術指針とインフラストラクチャ計画に含まれていることを確かめる。
・しかるべき文書をレビューして、市場の変化、法律と規制の条件、将来性のある新技術（技術開発、競合企業の活動、インフラストラクチャの問題、法的な要件と規制環境の変化、外部の専門家）がモニターされているかどうかを確かめる（モニタリング活動のアウトプットと結果をレビューしてその分析に基づく行動を確かめる）。
・IT戦略とIT技術インフラストラクチャ計画をレビューして、それが、ビジネスの成功に影響を及ぼす潜在的な可能性を持つようなITの近年の発展と整合的であることを確かめる。
・現状のインフラストラクチャと計画されているインフラストラクチャとの継続的な評価が行われていることを、チーフアーキテクトに確認する。識別され実行された修正行動をレビューして、これを承認された技術インフラストラクチャ計画と比較する。
・技術インフラストラクチャ計画を閲覧して、競合環境、情報システム要員の確保や投資におけるスケールメリット、プラットフォームとアプリケーションの相互運用性の改善が識別されていることを確かめる。
・技術研究の予算が効果的で効率的な方法で利用されているかどうかを調査する（研究に基づく改善の数やサービスの改善）。
・技術ガイドラインを閲覧して、それが技術的な対応策を適切にサポートし、組織の技術指針を正確に表していて、広範囲の問題に対して十分な指針を提供していることを決定する。
・ITアーキテクチャ委員会が設立され、役割、実行責任、説明責任が正式に定義されたかどうかを調査して、それを確かめる。
・ITアーキテクチャ委員会の会合が頻繁に開かれていることを（定期的かイベントベース）、委員会のメンバーに確認する。
・ITアーキテクチャ委員会からのすべての合意済みの行動が適切に記録され、追跡され、実施されていることを決定する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- ビジネスの達成目標やビジネスの機会（市場でのリーダーシップ）を達成するような適切な技術を組織が選択しないことのリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する
- 技術計画で競合環境での変化を考慮していないことのリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する。
- 情報システムの要員確保と投資のスケールメリットを達成できないことの影響を評価する。
- プラットフォームとアプリケーションを統合する機会を実現しないことによる機会費用を評価する。
- 潜在的なビジネス機会を実現しないことによる機会費用を評価する。
- IT技術インフラストラクチャ計画を策定する際に技術動向を考慮しないことによる機会費用を評価する。
- 法律と規制を遵守しないことのリスクを評価する。

PO4 ITプロセスと組織およびそのかかわりの定義

IT組織は、人材、スキル、機能、説明責任、権限、役割、実行責任、および監督に関する要件を考慮して定義する。透明性とコントロールを確保し、マネジメント層とビジネス管理部門の関与を確実にするために、ITプロセスフレームワークに、IT組織を組み込まなければならない。企業の戦略委員会は、取締役会を通してIT部門の監督を徹底し、ビジネス部門とIT部門が参加する1つ以上の推進委員会においてビジネス要件に応じたIT資源の優先順位を決定する。プロセス、管理ポリシー、および手続は、組織内のすべての機能のために、整備して運用する必要がある。その際には、コントロール、品質保証、リスクマネジメント、情報セキュリティ、データとシステムのオーナシップ、および職務の分離に、特に留意する。ビジネス要件にタイムリーに対応するため、関連する意思決定プロセスにはIT部門も参加する。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.1 ITプロセスフレームワーク IT戦略計画を実行するためのITプロセスフレームワークを定義する。このフレームワークには、ITプロセスの構造とITプロセス間のリレーションシップ(たとえば、プロセス間の差異や重複を管理する際に利用)、オーナシップ、成熟度、成果の測定、改善、コンプライアンス、品質目標、およびこれらの達成のための計画を含める。このフレームワークでは、IT特有のプロセス、企業ポートフォリオの管理、ビジネスプロセスおよびビジネス変革プロセス、の各プロセスを統合する。ITプロセスフレームワークは、品質管理システム(QMS)および内部統制のフレームワークに組み込む必要がある。	・ ITプロセスを定義するための一貫したアプローチ ・ 論理的で相互依存のプロセスへの主要な活動の組織化 ・ プロセスと主要な活動のオーナシップと実行責任に関する明確な定義 ・ 信頼性があり、反復性のある、主要な活動の実行 ・ 柔軟で対応しやすいITプロセス	・ 業務側に受け入れられていないフレームワークと、ビジネスの要件と関連していないITプロセス ・ ITプロセスの不完全なフレームワーク ・ プロセス間の相互関係の衝突と不明確さ ・ 活動相互間の重複 ・ 柔軟でないIT組織 ・ プロセス間のギャップ ・ プロセスの重複

コントロール設計のテスト

・ 以下を質問して確認する。
  - IT戦略計画を実現するための必要なITプロセスが識別され伝達されている
  - プロセスの達成目標、測定、コントロール、成熟度の定義とフォローアップを可能にするためのフレームワークが定義され実施されている
  - 関連性とタッチポイント(インプット/アウトプット、およびITプロセス、企業のポートフォリオ管理とビジネスプロセス)が定義されている

コントロール目標	価値のドライバー	リスクのドライバー
PO4.2 IT戦略委員会 取締役会レベルでIT戦略委員会を設置する。この委員会は、企業ガバナンスの一環として、ITガバナンスへの対応を確実かつ適切に行い、取締役会の代理として戦略的方針に関する助言を行うほか、主要な投資のレビューを行う。	・ 取締役会の支援 ・ ITの価値とリスクに対する取締役会の洞察 ・ 重要な投資に対する、より迅速な意思決定 ・ 戦略的な意思決定に関する明確な実行責任と説明責任 ・ ITガバナンスの企業ガバナンスへの統合 ・ うまく統治されているIT部門	・ 取締役会の議題での、ITに関する説明の欠如 ・ 取締役会レベルで知られていない、ITに関連するリスクと価値 ・ （ビジネスとITとの）合同の優先順位に基づいていない、投資や優先順位に関する意思決定 ・ 企業ガバナンスから分離したITガバナンス ・ ガバナンスの要件を遵守しておらず、経営者と取締役会の公共的な説明責任に潜在的な影響があるようなIT

コントロール設計のテスト

・ 以下を質問して確認する。
  – IT戦略委員会の規程、対象範囲、目標、メンバーシップ、役割、責任等が、企業の戦略的な意思決定の遵守を確かにするような方法で定義されている
  – IT戦略委員会が、組織のITへの依存とITが提供する機会とについて、しかるべき専門知識のある、取締役会とそれ以外のメンバーで構成されている。
・ 以下のために、IT戦略委員会の議題、文書、議事録をレビューする。
  – 委員会が定期的に会合を持ち、取締役会や組織が議題とする投資に対する主要な意思決定を含む戦略的な問題点を扱っていることを確かめる
  – 委員会が、ITガバナンスとIT戦略の問題点について取締役会に適切なガイダンスを提供していることを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.3 IT運営委員会 マネジメント層、ビジネスおよびITのマネジメント層で構成される、以下の役割を持つIT運営委員会（またはそれに準ずるもの）を設置する。 ・ 企業のビジネス戦略およびビジネス上の優先事項に沿った、IT関連の投資プログラムの優先順位の決定 ・ プロジェクト状況の追跡と資源をめぐる悩みや争いの解決 ・ サービスレベルおよびサービスの改善のモニタリング	・ 組織の戦略に沿ったIT戦略 ・ 組織の戦略に沿ったIT関連投資プログラム ・ 優先順位付けのプロセスへのビジネスとITとの双方の関与 ・ 衝突の解決へのビジネスとITとの双方の関与 ・ 成果のモニタリングへのビジネスとITとの双方の関与	・ 組織の戦略に沿っていないIT戦略 ・ 組織の達成目標と目的を支持していないIT関連投資プログラム ・ 主要な意思決定プロセスでの、ITと上級経営陣の不十分な支援と不十分な関与

コントロール設計のテスト
・ IT運営委員会の規程、対象範囲、目標、メンバーシップ、役割、責任等が、企業のIT戦略指針の実施を適切にもたらしているかどうかを調査して、それを確かめる。 ・ 議事録とIT運営委員会の規程といったような文書を閲覧して、委員会に関与している参加者、それぞれの担当業務および委員会から経営陣への報告の関係を識別する（IT関連投資の優先順位付け、プロジェクトのステータス、モニターサービスレベルとサービスの改善を決定する）。 ・ ビジネスがIT運営委員会の作業に積極的な役割を果たしており、経営陣は適切に相談を受けているかを経営陣に尋ね、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.4 組織におけるIT部門の配置 企業においてITが重要である場合には、ビジネスモデルに従って、全社的組織構造にIT部門を組み込む。企業においてITが重要であるとは、特に、ビジネス戦略上、ITを重要視していること、現場の実務においてITへの依存度が高いことである。CIOの報告先は、企業におけるITの重要性によって決定される必要がある。	・戦略的な優先順位と整合的なIT資源 ・効果的で、ビジネスの目標をサポートしているIT管理 ・適切なレベルでITに関する意思決定にコミットしている上級経営陣 ・組織レベルでのビジネスとITとの整合性	・上級経営陣からの不十分なコミットメント ・ビジネスを効果的にサポートしていないIT資源 ・十分な戦略的な重要性を与えていないIT ・ビジネスと別々のものとみなされているIT/ITと別々のものとみなさえているビジネス ・ビジネスの指針の欠如と業務間の情報伝達の欠如

コントロール設計のテスト

・IT部門が以下のようになっているかどうか質問して確認する。
- CIOまたは同様の部門によって扱われており、その権限、実行責任、説明責任、報告先は、企業内でのITの重要性に沿っている。
- 個々のユーザグループ/部門がIT部門に対して過度の影響力を行使してIT戦略委員会とIT運営委員会によって合意された優先順位を損なうことができないような方法で定義され予算が与えられている
- ビジネスを支援し、ビジネスとの関係を有効にするために適切なITソリューションとITサービスを導入し管理することができるよう、適切に資源を与えられている（人員、臨時雇用者、予算）

コントロール目標	価値のドライバー	リスクのドライバー
PO4.5 IT組織の構造 ビジネス上の必要性を踏まえて、社内のみならず、社外も含めて適切なIT組織構造を確立する。さらに、期待されるビジネス目標を達成し、かつ状況の変化に対応できるよう人員補充要件および調達戦略を調整するため、IT組織構造の定期的な見直しのプロセスを整備する。	・ビジネスに対する効果的かつ効率的なサポート ・戦略的なビジネス目標をサポートする人員補充要件および調達戦略 ・柔軟で対応しやすいIT組織構造 ・組織レベルでのビジネスとITとの整合性	・ビジネスへの不十分なサポート ・不十分な人員補充要件 ・不適切な調達戦略 ・ビジネスでの必要性の変化に柔軟に対応できないIT

コントロール設計のテスト

・以下を質問して確認する。
- 組織の変更が組織全体とIT部門それ自体の構造に影響するため、組織の変更の影響を定期的にレビューしている
- IT組織が、外部の請負業者を用いるといったように、資源を柔軟にアレンジし、外部のサービスを柔軟にアレンジすることによって、変化したビジネスでの必要性をサポートしている。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.6 役割と責任の確立 組織の要件を満たすにあたり、IT担当者とエンドユーザに伴う権限、実行責任および説明責任を明確にするために、IT担当者とエンドユーザにそれぞれ求められる役割と責任を定め、周知する。	・個人の良好なパフォーマンス ・特定のポジションに割り当てられた活動 ・適切な技能と経験を持つIT要員に対する効率的な採用 ・担当者の良好なパフォーマンス	・規制の違反 ・情報漏洩 ・意図した通りに機能しない要員採用 ・不正なシステム利用 ・対応力のないIT組織

コントロール設計のテスト

・以下を質問して確認する。
  - 文書をレビューし、IT業務の説明が適切であり必要に応じて更新されているかどうかを決定することによって、それぞれのIT業務が正式化されていることを確認する
  - 役割がそれに対応するIT業務を伴ってIT要員に割り当てられている。担当者が、自らに割り当てられている役割と作業を理解しているかどうかを評価し、その作業が実施されていることを評価する。
  - 説明責任と実行責任とが役割に対して割り当てられている。業務記述書、規程等を閲覧して、それぞれの役割に、その役割を実行するのに必要な説明責任と実行責任とが伴っていることを確かめる。
  - IT要員が自分の役割を知らされている。変更がIT要員に伝達されているかどうか、その変更が実施されているかどうかを評価する。
  - 管理職が定期的に職務記述書の正確性を確認する。職務記述書をレビューして、それがチームメンバーの役割を正確に反映しているかどうかを決定する。
  - 職務記述書が、主要な達成目標と目的のあらましを述べており、SMARRTの測定指標を含んでいる
  - SMARRTの測定指標が担当者の業績評価で用いられている
  - 組織内のすべての職務記述書が、情報システム、内部統制、セキュリティについての責任を含んでいる
  - 経営陣が、担当者に対して業務の研修を定期的に行っている。担当者にインタビューして、役割についての知識が伝達され理解されているかどうかを決定する。
・従業員に対して全社的および部門内のポリシーと手続きを提供しているかどうかを決定するために、以下をレビューする。
  - 年次のポリシー確認書
  - 採用時のオリエンテーションで従業員にポリシーについての文書を提供したかどうかを示す人事記録
  - 従業員の研修記録

コントロール目標	価値のドライバー	リスクのドライバー
PO4.7 ITの品質保証の責任 品質保証（QA）機能における成果達成の実行責任を割り当てる。同時に、適切なQAシステム、コントロール、および周知に関わる専門家から公正されるQAグループを編成する。QA部門の組織内での位置付けや責任と規模が、組織として求められる要件を満たすようにする。	・ITの実行責任の欠くことのできない部分としての品質保証 ・組織での品質に関する期待に沿ったプロセス ・ITの機能とビジネスプロセスへの改善に対する積極的な識別 ・品質上の問題点とビジネスリスクに対する積極的な識別	・評判の損失 ・ビジネス全体に影響するような品質に関する発見されないリスク ・品質管理が貧弱なことによる、費用と遅延の増大 ・一貫して有効に適用されない品質保証 ・組織間での品質の一貫性の欠如 ・ビジネスの業績の低下

コントロール設計のテスト

・QA部門が以下のようになっているかどうか質問して確認する。
- 十分な独立性を伴って運用することができ、その知見を客観的に報告することができるような報告ライン
- 組織のQAに関連するポリシー、基準、手続きを遵守すること（たとえば組織の開発方法論の遵守）を確かにするためのモニタリングプロセス
- QAに関連するポリシー（システムの開発ライフサイクルにおけるQA要件）、基準、手続きの作成の専門家の中心として振舞っている
- QAのベストプラクティスと標準を採用し、それと整合的なプロセス
- 担当者のレベルと技能が、組織の規模とQA部門の責任に即している。技能を評価し、それが品質保証、IT、コントロール、プロセス、伝達を含んでいることを確かめる。
- 上級経営陣のスポンサーからの積極的な支援
- QAプロセスで識別された問題点を識別し、エスカレートし、解決するための、定義され文書化されたプロセス
- 知見と提言を定期的に報告するプロセス

コントロール目標	価値のドライバー	リスクのドライバー
PO4.8 リスク、セキュリティ、およびコンプライアンスに関する責任 ビジネスにおけるIT関連のリスクのオーナシップおよび実行責任を、適切なマネジメント層レベルに割り当てる。情報セキュリティ、物理的セキュリティ、およびコンプライアンスに関する具体的な責任を含め、ITリスクを管理する上で重要な役割を定義し、割り当てる。組織全体の課題に対応するため、全社レベルでのリスクおよびセキュリティ管理に関する責任を定める。システム固有のセキュリティ問題に対処するため、さらにシステム別のセキュリティ管理責任の割り当てが必要となる場合もある。マネジメント層から、ITのリスク傾向に関する支持、および未対応のITリスクに関する承認を得る。	・ 情報資産の保全とインテグリティの改善 ・ リスク、セキュリティ、コンプライアンスに関する、上級マネジメント層レベルに割り当てられてた実行責任 ・ リスク、セキュリティ、コンプライアンスの問題における上級マネジメント層の支援 ・ 組織の脅威に対する効果的かつ効率的な対策としてのセキュリティメカニズム ・ リスク、セキュリティ、コンプライアンスの問題点に対する積極的な識別と解決	・ 情報資産の不適切な保全 ・ 機密情報の喪失 ・ 財務上の損失 ・ 組織全体のセキュリティに対する経営者のコミットメントの欠如 ・ コンプライアンスに違反するリスク ・ 組織のITリスク選好に対する不明確な理解

コントロール設計のテスト

・ 以下を質問して確認する。
  – マネジメント層が、組織全体にわたる、十分な人員を割り当てた、リスク管理と情報セキュリティの部署を創設し、そこにリスク管理と情報セキュリティの全体的な説明責任を割り当てている。主要な担当者にインタビューして、リスク管理と情報セキュリティの部署の報告ラインが、組織のリスク管理と情報セキュリティの、ポリシー、基準、手続きを効果的に設計し、実施し、ライン管理職と共同で、そのコンプライアンスを徹底するようになっていることを確かめる。
  – リスク管理と情報セキュリティの部署の役割と責任が正式化され文書化されている
  – 適切な技能と経験を持つ担当者に実行責任を割り当てており、情報セキュリティの場合には、情報セキュリティ責任者の指示を受けている
  – リスク管理と情報セキュリティに関連する資源の要件を経営陣が定期的に評価し、ビジネスの必要性に合致するのにふさわしい資源を提供している
  – リスクプロファイルと重要な残余リスクの受容に関するマネジメント層のガイダンスを得るためのプロセスが実施されている。最近の状況を調査して、そのプロセスが適切に機能していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.9 データおよびシステムのオーナシップ ビジネス部門がデータおよび情報システムのオーナシップに関する責任を果たせるよう、手続およびツールを提供する。オーナは、情報およびシステムの分類について決定し、その分類に沿って当該情報およびシステムを保護する必要がある。	・ 自らのデータとシステムをコントロールしているユーザ ・ データとシステムセキュリティの測定指標の維持に対する、定義された説明責任 ・ 効果的かつタイムリーな情報管理プロセス ・ 資産の盗難に起因する財務上の損失の減少	・ 適切なセキュリティを講じていないビジネスデータ ・ 情報資産の不適切な保全 ・ビジネスの要件に沿っていないような、ビジネスデータを保全するための要件 ・ データとシステムに対する不十分なセキュリティ測定指標 ・データに対する責任を負わないビジネスプロセスオーナ

コントロール設計のテスト

・ データ分類とシステムのオーナシップのポリシーが策定され伝達されているかどうかを調査して、それを確かめる。
・ 主要なアプリケーションシステムと企業のアーキテクチャ、および内部と外部のデータ通信に、ポリシーが適用されていることを確かめる。
・ データ分類とシステムのオーナシップが、情報資産の保全をサポートしており、ビジネスアプリケーションを効率的に提供し利用することができ、セキュリティに関する効果的な意思決定を活用していることを確かめる。
・ システムオーナシップとデータ分類を登録し維持するプロセスを観察し、そのプロセスが一貫して適用されているかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.10 監督 適切な監督の実践基準をIT部門に導入する。これにより、部門内における役割と責任が確実に果たされることを保証する。すべての要員がそれぞれの役割の実行と責任の行使に要する権限および資源を十分有しているかを見極める。また、KPIを全体的に見直す。	・ITの役割と責任の効果的かつ効率的な行使 ・IT部門に対する適切なコントロール ・資源調達の問題点の迅速な識別 ・パフォーマンス上の問題点の迅速な識別	・組織の達成目標と目的の不達成 ・資源調達とパフォーマンスに関する、識別されず解決されない問題点 ・ITとビジネスのプロセスの機能不全 ・コントロールと目標に対する不十分なモニタリング ・行使されない主要な役割と責任

コントロール設計のテスト

- インタビューを通じて、成果のレビューのためのガイダンスと研修を含む監督活動が確立していることを確かめる。
- 記録をレビューして、監督者のレビューと担当者の査定の頻度と程度を評価する。
- レビューが、成果に関する期待と成果の判断基準とをうまく組み合わせているかどうかを評価する。
- 監督者のレビューと担当者の査定からの知見が、適切にエスカレートされ、伝達され、フォローアップされているかどうかを調査して、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.11 職務の分離 役割と責任の分類を行う。これにより、一個人に役割と責任が集中するがために、重要なプロセスが不適切に実施される可能性を減らす。要員が、割り当てられた職務および職位に関連して許可された業務のみを遂行していることを確認する。	・業務上重要なシステムとプロセスの効果的かつ効率的な機能 ・情報資産の適切な保全 ・財務上の損失とレピュテーション(世評)ダメージのリスクの減少	・重要なプロセスに対する不適切な監督 ・財務上の損失とレピュテーション(世評)上のダメージ ・不正や意図せざるダメージ ・重大なシステムとビジネスプロセスを分離するための外部の要件の違反

コントロール設計のテスト

- 適切な職務の分離を守らせて確かなものとするための基準が確立し、このような基準が必要に応じてレビューされ変更されているかどうかを調査して、それを確かめる。
- 役割と責任を評価する際に基準が実施されているかどうかを評価する。
- 職務の分離をしなければならないような、重要な地位とプロセスを識別するためのプロセスが存在するかどうかを調査して、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.12 ITスタッフの配置 ITスタッフの配置要件について、定期的に、またはビジネス環境、運用環境、もしくはIT環境の大規模な変更に応じて評価する。これにより、IT部門がビジネスの達成目標や目標を適切に支える上で十分な人材を確保できるようにする。	・ ITスタッフがビジネスの必要性をサポートする能力 ・ コストに対するコントロール ・ 適切な規模のIT部門 ・ IT部門での適切な技能	・ ビジネスの必要性に合致できないIT要員リソース ・ ITに関する内部ないし外部の要員の過大な費用 ・ リソースに過不足のあるIT部門 ・ IT部門における適切な技能の欠如

コントロール設計のテスト

- ITに関する必要な技能と能力および利用可能な技能と能力を定期的にレビューし、そのITスタッフへの影響を分析し、エスカレートし、必要に応じて対処しているかどうかを調査して、それを確かめる。
- ビジネスと業務に関する主要な変更をレビューし、それが技能、能力、要員の要件に及ぼす影響を評価し、対処しているかどうかを評価する。
- 人員調達戦略を評価し、それが技能と能力の要件をサポートしていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.13 主要IT担当者 主要IT担当者(交代要員/バックアップ要員)を定義および特定して、重要な業務を実行する際に特定の個人に依存し過ぎないようにする。	・ 適切に訓練された主要なIT担当者 ・ 個々の主要なIT担当者への依存度の低下 ・ 知識の共有 ・ ITサービスの継続性 ・ 確実にサポートされたITに関する重要な役割 ・ 引継計画	・ 主要なIT担当者の不十分な技能 ・ 知識を持つ一人の専門家への依存 ・ 不十分な知識の共有や不十分な引継計画 ・ 実施されない重要な作業や役割

コントロール設計のテスト

- マネジメント層が、欠員補充の承認や人員不足と知らされたときに、主要なプロセスに対する担当者の補填範囲を検討するための正式な手続きを持っているかどうかを調査して、それを確かめる。
- マネジメント層が、主要な担当者への依存をレビューし、代替的な供給源、主要な知識の文書化、他の担当者への訓練、主要な担当者から他の担当者への責任の移管といったような緊急対応を検討したかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.14 契約社員に関するポリシーおよび手続き IT機能をサポートするコンサルタントや契約社員が、組織の情報資産の保護についてポリシーを認識し、遵守することにより、双方が合意した契約要件に適合できるようにする。	・ビジネスの必要性をサポートする契約社員 ・組織内での知識の共有と保持 ・情報資産の保全 ・契約社員の行動に対するコントロール	・主要な（契約）社員への依存度の増加 ・契約社員に対する期待と能力との間のギャップ ・ビジネスの要件との整合性を欠いて実施された作業 ・契約社員からの知識の獲得や技能の移転の欠如 ・効率的、効果的でない契約社員の使い方 ・情報資産の保全に関する組織のポリシーに対する、契約社員の違反 ・実行責任と説明責任に対する期待について合意できないことによる訴訟の費用

コントロール設計のテスト

・いつ、どのように、どのような仕事を外注できるのかを記述するポリシーと手続きを閲覧し、それが実施されているかどうかを決定する。
・請負業者の情報セキュリティに関する責任についてのポリシーと手続きを閲覧して、質問を通じて、それが守られているかどうかを評価する（バックグラウンドチェックを実施しているか、物理的および論理的なアクセスコントロールの要件にしたがっているか、個人の識別は安全か、電子メール、電話、すべてのプログラムとデータのファイルを含むIT資源のすべての利用をモニターし検閲する権利を経営陣が留保する旨を請負業者に通知したか）。
・請負業者選定のためのポリシーと手続きをレビューして、それを実施しているかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO4.15 リレーションシップ IT部門間、およびIT部門内外のさまざまな関係者との間で最適な連携、情報共有、および協力体制を確立し、維持する。関係者とは、具体的には、取締役会、マネジメント層、ビジネス部門、個人ユーザ、サービスプロバイダ、セキュリティ担当者、リスク管理担当者、企業のコンプライアンス担当グループ、アウトソーシング発注者、および遠隔地管理担当者などである。	・ 問題点に対する効率的な識別と解決 ・ ビジネスの達成目標と方法論、及び達成目標とアプローチとの整合性 ・ 利害関係者の積極的な関与 ・ リレーションシップ管理に対する、明確に定義されたオーナシップと説明責任	・ 問題点の識別と解決との間のギャップの拡大 ・ 改善点の不十分な識別 ・ ビジネスの目標と、ITのポリシー、ガイドライン、方法論との間のギャップ

コントロール設計のテスト
・ 利害関係者を識別するためのプロセスが定義され、伝達チャンネルと伝達計画がそれぞれに確立されたかどうかを調査して、それを確かめる。 ・ 主要な利害関係者へのインタビューを通じて、ITのコミュニケーションに満足しているか、ITのコミュニケーションは有効か、利害関係者からのフィードバックへの対処の十分かを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

・ ITプロセスフレームワークをレビューして、それがIT戦略計画をサポートしておりビジネスプロセス、ITプロセス、全社的なポートフォリオ管理と一体化しているかどうかを決定する。
・ インタビューを通じて、このフレームワークが、ビジネスとITによって、伝達され、実行され、理解されているかどうか尋ねる。
・ ITプロセスフレームワークが品質管理システムと内部統制フレームワークに統合されているかどうかを調査して、それを確かめる。
・ IT戦略委員会の対象範囲、メンバーシップ、責任等が定義され、委員会が取締役会とそれ以外のメンバーから構成され、それぞれに適切な専門知識があるかどうかを調査して、それを確かめる。
・ インタビュー、議事録、取締役会への報告書を通じて、IT戦略委員会が取締役会に、ガバナンスとIT戦略の問題点を報告していることを確かめる。
・ IT部門のパフォーマンスをモニターし、測定し、報告するためにどのようなプロセスを用いているかをITマネジメント層が理解しているかどうかを調査して、それを確かめる。
・ 役員レベル、主要な業務部門、ITと主要な間接部門から構成されるIT運営委員会が存在することを確認する。
・ IT運営委員会の役割と責任についての正式な文書が、役員レベルでの主要なスポンサーシップを含んでいるかどうかを調査して、それを確かめる。
・ 議事録とIT運営委員会の規程といった文書を閲覧して、委員会への参加者、その職務、委員会から経営陣への報告との関係を識別する。
・ CIOやそれと同等の機能によってITが指揮されており、報告ラインがITの重要性に相応しているかどうかを調査して、それを確かめる。
・ インタビューと組織図のレビューを通じて、IT部門に対していかなる個別のユーザグループ/部門も過度の影響力を行使できないことを確かめる（IT部門の報告との関係、IT部門の他の部門や部署からの独立性、プロジェクトの資金源）。
・ インタビューと文書のレビューを通じて、IT部門に、業務部門をサポートするのに十分な資源と予算が与えられていることを確かめる（資源の要件に関して、ビジネスケース、IT戦略、IT実行計画をレビューする）。
・ IT組織がビジネスの必要性を反映していることを確かめることを目的に、IT組織の構造について定期的

にレビューしているかどうかを調査して、それを確かめる。
- IT管理部門の長とともに、外部の資源へのアクセスが必要に応じて利用可能であることを確かめる。
- IT担当者へのインタビューを通じて、役割がそれに対応するITの作業のそれぞれに割り当てられていることを確かめる（担当者が自らに割り当てられた役割と作業を理解しており、その作業を実行しているかどうかを評価する）。
- 責任が役割に割り当てられているかどうかを調査して、それを確かめる（それぞれの役割に、その役割を実行するのに必要な責任があることを確かめる）。
- 職務記述書が作成され、権限と説明責任が明確に示されているかどうかを調査して、それを確かめる。
- QA部門が存在するかどうか質問して確認する。
- QA部門の役割を決定する（組織のQAに関連するポリシー、基準、手続きの遵守を確かにするためのプロセスをモニターし、QAに関連するポリシー、基準、手続きの作成の専門家の中心として振舞う）。
- QA部門に、十分な技能を持った十分な人員が配置されているかどうかを調査して、それを確かめる。
- マネジメント層のメンバーが、リスク管理と情報セキュリティの部門を創設し、それがそれぞれの分野での説明責任を果たしているかどうかを調査して、それを確かめる。
- リスク管理とセキュリティ部門の報告ラインが、組織のポリシーと手続きの遵守を効果的に設計し、実施し、ライン管理職と共に徹底することができるようになっているかどうかを調査して、それを確かめる。
- ITに関連するリスクで受容可能なレベルについての、マネジメント層のガイダンスを得るためのプロセスが実施されているかどうかを調査して、それを確かめる。
- リスク管理と情報セキュリティについての役割と責任が正式化され文書化され、その責任が適切に割り当てられているかどうかを調査して、それを確かめる。文書をレビューして、役割と責任が概要の通りに満たされているかどうかを決定する。
- 資源の要件が定期的に評価され、必要に応じて提供されているかどうかを調査して、それを確かめる。資源の要件の評価の結果に基づいて、人員配置のレベルが適切であるかどうかを評価する。
- インタビューと文書のレビューを通じて、情報資産の棚卸が作成され、追跡され、維持されていることを確かめる。
- インタビューを通じて、監督者が、監督業務を実施するのに必要な技能を持っていることを確かめる（重要な作業、KPI、担当者の業績査定、リスク評価を追跡する）。
- エスカレーション手続きをレビューして、それが実施され、一貫して適用されていることを確かめる（問題点が記録され、追跡され、定期的に分析されている）。
- 定期的な従業員のレビューの間に、監督者の技能が評価され、能力を保証するのに必要な行動が取られているかどうかを調査して、それを確かめる。
- 矛盾している機能を識別するためのプロセスが存在するかどうかを調査して、それを確かめる。
- 矛盾している機能が修復されたかどうかを調査して、それを確かめる。
- 典型的な職務担当者が存在しない場合、適切な職務の分離をどのように維持しているかを手続きで取り上げているかどうかを調査して、それを確かめる。
- 職務と職責が作成されたり更新されたりするときに職務の分離をレビューしているか、必要な場面で責任を割り当てているかどうかを調査する。変更が実施されているかどうか決定する（職務記述書で権限と責任を明確に示しているか）。
- 必要に応じて補完的なコントロールを設計し実施しているかどうかを調査して、それを確かめる（ITマネジメント層や監督者と共に、補完的なコントロールの有効性を確かめる）。マネジメント層が、ビジネス/IT環境と戦略を考慮する際に、定期的に人員配置の要件をレビューし、技能と資源のギャップを識別しているかどうかを調査して、それを確かめる。
- マネジメント層が、要員配置要件のレビューと同時に、人材資源の調達戦略（ビジネス/IT人員再配置、多職種の職能訓練とローテーション）を評価しているかどうかを調査して、それを確かめる。
- マネジメント層が定期的に、主要なプロセス、そのプロセスをサポートするのに必要な技能、職務の冗長性のない主要なエリアを識別しているかどうかを調査して、それを確かめる（重要な役割を満たすのに関連する技能、経験知識を持つ個人が利用可能かどうかを決定し、主要なプロセスとそれをサポートするために任命された人の一覧を閲覧する）。
- マネジメント層が、主要なプロセスの業務の冗長性を提供するために、外注やその他のサポートの手配を検討したかどうかを調査して、それを確かめる（外注に関する規定が存在することを識別するために、

サードパーティとの契約で入手可能なものを閲覧する）。
- 主要な連絡先の一覧が存在し維持されているか、および連絡先一覧によって適切な人と適時に連絡できるどうかを確かめる。
- バックアップ要員が相互に訓練されていることを確かめる。
- ポリシー、手続き、ルール、責任が請負業者に伝達され、IT資源のすべての利用をモニターし検閲する権利を経営者が留保しているということをその請負業者が理解しているかどうかを調査して、それを確かめる。
- 請負業者の作業をレビューし、支払いを承認する責任を、適切な個人が持っているかどうかを調査して、それを確かめる。
- ITマネジメント層が、主要な利害関係者（ユーザ、供給者、セキュリティ責任者、リスク管理者、規制当局）と関係を定義し、役割と責任を利害関係者に伝達しているかどうかを調査して、それを確かめる。
- マネジメント層に、関係を管理するのにふさわしい技能を持ったIT担当者が割り当てられていることを確認する（主要な利害関係者それぞれに対応する連絡先一覧を閲覧する）。
- 主要な利害関係者からのフィードバック（問題点、行動項目、報告）を得ているかどうかを調査して、それを確かめ、継続的な改善のためにそのフィードバックを適切に用いているかどうか評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 戦略的な達成目標を達成するためのロードマップが確立されないリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する。
- ITが、戦略的な達成目標を達成するのに最適に組織されていないことによるリスクと追加的な費用を評価する。
- IT戦略計画が効果的に実行されないことのリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する。
- 主要なIT担当者への過度の依存に対するリスクを評価する（脅威、潜在的な脆弱性、セキュリティ、内部統制）。
- 人員配置の要件と資源調達戦略が、期待されたビジネスの達成目標と環境の変化に合致するように調整されていないことによる追加的な費用を評価する。
- 担当者が、職務と地位に関連して、承認されていない職務を実施することによる追加的な費用を評価する。
- 外部の人員のコントロールされていない行動が、組織の情報資産を損なうことのリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する。

PO5 IT投資の管理

コスト、便益、予算内での優先順位、正式な予算編成プロセス、および予算に照らした管理が組み込まれたフレームワークを構築および維持し、IT関連の投資プログラムを管理する。利害関係者と協力し、IT戦略計画および実行計画の枠内で総コストと便益を特定およびコントロールし、必要に応じて是正措置を講じる。このプロセスにより、ITとビジネスの利害関係者間の協力関係が促進され、IT資源の効果的かつ効率的な使用が可能になる。さらに、総所有コスト(TCO)についての透明性と説明責任が確保され、ビジネス上の便益およびIT関連の投資からの収益の獲得が可能になる。

コントロール目標	価値のドライバー	リスクのドライバー
PO5.1 IT財務管理フレームワーク IT関連の投資、投資対効果検討、およびIT予算から成るポートフォリオを通じて、投資、IT資産のコスト、およびサービスを管理するための財務フレームワークを確立、維持する。	・標準化された投資基準を用いることによる、ITのビジネスへの貢献の価値の確認 ・IT価値への貢献度に基づくITの優先順位 ・明確で合意された予算 ・ビジネスケースに基づいて優先順位を割り当てる能力の改善	・ITプロジェクトに対する不明確な優先順位 ・財務管理の非効率的なプロセス ・ビジネスニーズを反映しないIT予算 ・IT予算に対する弱いコントロール ・マネジメント層のIT予算の不承認 ・マネジメント層の支援の欠如

コントロール設計のテスト

・コストに基づいたプロセスと責任、利益と予算の管理を含む、財務管理フレームワークが存在することを確かめる。財務フレームワークのインプットとアウトプットが定義されており、入手可能な財務情報に基づいて、マネジメント層が財務フレームワークを定期的に改善しているかどうかを調査し、それを確かめる。
・投資プログラム、サービス、資産のポートフォリオが作成され維持されていることを確かめる。ポートフォリオに対する高いレベルのレビューを行い、網羅性およびIT戦略計画とIT実行計画との整合性をチェックする。
・ポートフォリオでの関連するコストと便益の側面を、しかるべき予算の優先順位の決定（ビジネスケース）、コスト管理、利益管理のプロセスへと伝達するためのプロセスが存在するかどうかを調査し、それを確かめる。
・報告されているコストと便益のインプットが比較可能で一貫していることを確かめる。
・策定されたIT予算が、プロジェクト、資産、サービスを含んでいることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO5.2 IT予算内での優先順位の決定 運用、プロジェクト、維持管理のためのIT資源配分の優先順位付けのために、意思決定プロセスを導入する。IT資源配分の優先順位付けを通じて、IT関連投資のプログラム、その他のITサービス、資産における企業ポートフォリオから生み出される収益の最適化を図ると同時に、収益の最適化に対するITの貢献度を最大限に高める。	・ ITの達成目標とビジネス要件を反映し、すべての利害関係者にとって明確な優先順位 ・ 資源の重点的な利用法 ・ 適切な意思決定、コストバランス、継続的な改善、品質改善、将来への準備	・ 不十分な資源管理 ・ 最適化できていない達成目標と目的 ・ 優先順位が不明確なために生じる、混乱、モティベーションの低下、俊敏性の欠如 ・ IT戦略と投資の意思決定に沿っていないIT予算

コントロール設計のテスト
・ IT業務とIT資源の優先順位決定のためのプロセスと意思決定委員会が設立されているかどうかを調査し、それを確かめる。委員会の責任が、他の委員会との関連において定義されていることを確かめる。 ・ ビジネスケースと戦略計画および実行計画に基づいて、すべてのIT業務の優先順位をつけているかどうかを調査し、それを確かめる。 ・ 継続性と正確性について、予算配分と決算をレビューする。 ・ 議事録の閲覧を通じて、優先順位付けについての意思決定が伝達されていることを確かめ、インタビューを通じて、その意思決定が予算に関する利害関係者によってレビューされているかどうか尋ねる。 ・ ビジネスケース、ポートフォリオ、戦略計画に影響を及ぼす、予算に関する重要な意思決定を識別し、伝達し、解決するためのプロセスが存在するかどうかを調査し、それを確かめる。 ・ IT戦略委員会と執行役員会が、企業の戦略計画や実行計画に悪影響を及ぼす項目についてのIT予算全体に対する変更を承認し、このような影響を解決するための活動を提案したことを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO5.3 IT予算編成 IT関連投資プログラムの企業ポートフォリオにおいて確定した、優先順位を反映した予算を編成するための実践方法(手法)を確立し、導入する。予算の中には、現行のインフラストラクチャの運用、維持コストを含める。この実践方法(手法)は、総合的なIT予算の編成に加え、各プログラムの、ITコンポーネントに重点を置いたプログラム別の予算編成に対応している必要がある。また、この実践方法(手法)には、全社の予算および各プログラムの個別予算の継続的な見直し、最適化、および承認を組み込む必要がある。	・ 予算の予測と配分のための効果的な意思決定プロセス ・ IT運用のための、正式に定義された予算オプションの範囲 ・ 識別され分類されたITのコスト ・ 支出に対する明確な説明責任	・ リソースの利害衝突 ・ IT運用のための財源の不適切な配分 ・ 組織の達成目標に沿っていない財源 ・ 迅速な対応を不可能にする、権限の欠如 ・ IT予算に対するマネジメント層の支援の欠如

コントロール設計のテスト

- 正式なIT予算を確立し、変更し、承認し、伝達するための方法論が導入されているかどうかを調査し、それを確かめる。
- IT予算をレビューして、予算を編成するときに、関連する要素（財源、内部の資源のコスト、資本と業務の支出に対する承認）が考慮されているかどうか確かめる。
- 緊急的な予算が識別され、このような緊急的な予算のための根拠が承認されたかどうかを調査し、それを確かめる。
- 予算編成プロセスの有効性がモニタリングされていることを確かめ、レポートをレビューして、将来の予算編成をより正確かつ信頼性の高いものにするために、過去からの教訓が記録されていることを確かめる。
- 予算編成プロセスに関与している人（プロセス、サービス、プログラムのオーナ、資産管理者）が適切に指導を受けているかどうかを調査し、それを確かめる。
- 承認され一貫した予算編成プロセス（予算計画をレビューし、予算配分に関する意思決定を行い、IT予算、プロジェクト費用配分、サービス費用配分、予算差異分析全体をまとめて報告する）が存在するかどうかを調査し、それを確かめる。

コントロール目標

PO5.4 コスト管理

実コストと予算を比較するコスト管理プロセスを導入する。コストはモニタリングおよび報告される必要がある。予算からの逸脱がある場合は、それをタイムリーに特定し、プログラムへの影響を評価するとともに、当該プログラムのビジネス上のスポンサーと協力して適切な是正措置を講じ、必要に応じてプログラムの投資対効果検討内容を更新する必要がある。

価値のドライバー

- 予算からの逸脱に対する正確かつ適時な識別
- 費用対効果が高く最大化されたIT資源の活用
- 価格設定に一貫性のあるサービス提供
- ITの価値への貢献の明確性
- 業務側における、ITの実際のコストと便益に対する理解

リスクのドライバー

- 不適切なIT投資
- 不適切なサービス価格設定
- ITの価値への貢献の不明確さ

コントロール設計のテスト

- IT関連のコストを管理するためのフレームワークが定義されており、IT支出のカテゴリーが包括的で、適切で、適切に分類されているかどうかを調査し、それを確かめる。
- 財務情報を入手、分析、報告する個人とIT予算を持つ人との間に適切な独立性があることを確かめる。
- 確立したタイムスケールをレビューし、それが予算編成と会計の要件と合致しており、ITプロジェクトの中で、成果物のタイムテーブルにしたがって構築されているかどうかを決定する。
- 特定された逸脱を識別するためのデータを収集する方法が定義されているかどうかを調査し、それを確かめる。
- データを収集するシステムが識別されていることを確かめる。
- システムが提供する情報が、完全で正確で整合的かを判断する。
- 費用に関連する情報をどのように連結するか、それを組織内の様々なレベルや利害関係者にどのように報告するか、それによって、必要な是正措置を適時に識別できるようになっているかを判断する。

コントロール目標	価値のドライバー	リスクのドライバー
PO5.5 便益管理 適切なIT機能を提供、保守することから得られる利点を監視するためのプロセスを導入する。IT関連の投資プログラムの一部として、または通常の業務支援の一環として、業績に対するITの貢献内容を特定し、投資対効果検討書として文書化し、合意を得た上でモニタリングおよび報告を行う。報告書を検討し、IT部門による貢献に改善の余地がある場合は、適切な措置を策定、実施する必要がある。IT部門の貢献における変化、または関連プロジェクトにおける変化がプログラムに何らかの影響を与える場合、当該プログラムの投資対効果検討内容を更新する必要がある。	・投資プログラムの実施中および実施後における便益の差異の正確な識別 ・ポートフォリオについての意思決定、すなわちプログラムを継続、調整、または停止するための意思決定のための正確な情報 ・価格設定が適切なサービス提供 ・ITのビジネスへの貢献の明確性 ・ITの実コストと便益に対する業務側での理解	・不適切なIT投資への支出 ・不適切なサービス価格設定 ・ITの価値への貢献の不明確さ ・ITの価値への貢献に対する誤った認識

コントロール設計のテスト
・コスト管理プロセスが、ITソリューションを提供し、ITサービスを提供し、IT資産を監視することの便益を識別し定量化し定性化するのに十分な情報を提供しているかどうかを調査し、それを確かめる。 ・期間を通して便益の配分によって便益を有効に分析することが可能かを調査し、それを確かめる。 ・便益を測定するために必要な測定指標を作成するプロセスをレビューする（外部の専門家、業界のリーダー、比較可能なベンチマーキングデータから助言を得る）。 ・便益の逸脱が識別されたときに是正するプロセスが存在するかどうかを調査し、それを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

・IT関連のビジネスプログラムのポートフォリオへのインプットに対し、公正、明確、反復可能で、ITのコストと便益の評価の比較を可能とする財務管理のフレームワーク、プロセス、責任が定義され、維持されているかどうかを調査し、それを確かめる。
・財務管理フレームワークが、ITの投資とポートフォリオの意思決定を効果的かつ効率的にできるようにするための情報を提供し、ITのコストと便益を評価できるようしており、ITの資産とサービスのポートフォリオの維持へのインプットを提供しているかどうかを評価する。財務管理のフレームワークとプロセスが、ビジネスケースの作成を支援し、予算プロセスを遂行するのに十分な財務情報を提供しているかどうかを決定する。
・投資、ITの資産とサービスがIT予算の編成で考慮されていることを確かめる。
・現在のIT予算が実際のコストと比較されて追跡され、差異が分析されているかどうかを調査し、それを確かめる。
・予算編成プロセスによって提供される情報が、プロジェクトコストを追跡し、IT資源の配分を支援するのに十分かどうかを調査し、それを確かめる。
・ITの全ての業務に対して優先順位をつけ、それにしたがって予算を配分するための効果的な意思決定プロセスが実施されているかどうかを調査し、それを確かめる。
・正式なIT予算を確立し、維持し、その変更と承認を伝達するための方法論が導入されているかどうかを調査し、それを確かめる。
・プロセス、サービス、プログラムのオーナとプロジェクト管理者と資産管理者が、どのように予算の要件を捉え、予算を計画するかの指導を受けているかどうかを調査し、それを確かめる。
・予算編成プロセスが存在し、このプロセスが定期的にレビューされ改善されていることを確かめる。
・コスト管理フレームワークをレビューし、それがITに関連するすべてのコストを識別していることを確かめる。

コストをモニターするためのツールが効果的であり適切に用いられていることを確かめる（予算とプロジェクトの中でどのようにコストを配分しているのか、コストをどのように捉えて分析しているのか、誰にどのように報告しているのか）。
- 期間を通して予算配分がITプロジェクトと合致しており、予算の差異を有効に分析できるように活動をサポートしているかどうかを調査し、それを確かめる。
- IT財務のマネジメントメンバーが、コストのデータをどのように捉え、連結し、報告するかについて指導を受けているかどうかをを調査し、それを確かめる。
- 適切なレベルのマネジメント層が、コスト分析の結果をレビューし、是正措置を承認しているかどうかを調査し、それを確かめる。
- ビジネスケースに記録された通りに便益を達成することの実行責任と説明責任が割り当てられているかどうかを調査し、それを確かめる。
- ビジネスケースへのITとビジネスの貢献をモニターするための測定指標を、定期的に収集し、報告し、分析しているかどうかを調査し、それを確かめる。
- 識別された予算の差異がビジネスとITのマネジメント層に承認されているかどうかを調査し、それを確かめる。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。
- 以下のようなリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制）を評価する。
  - ビジネスケースへのインプットが、現在のITの資産とサービスのポートフォリオを考慮していない
  - 新規の投資と維持とが将来のIT予算に影響を及ぼさない
  - プロジェクトのコスト/便益が、予算の優先順位付け、コスト管理、便益管理のプロセスへと反映されていない
  - 投資の収益率の最大化へのITの貢献の結果として、IT資源の優先順位をつけていない
  - 予算全体および個々のプログラム予算の継続的なレビュー、改善、承認を行っていない
  - 費用の逸脱がタイムリーに識別されず、そのような逸脱の影響が評価されていない
  - ビジネスソリューションへのITの貢献を改善する機会を考慮していない
  - 費用便益分析ですべての便益を識別しておらず、その結果、プロジェクトの優先順位付けが適切でなく、実行できたはずのプロジェクトを棄却してしまう

PO6　マネジメントの意図と指針の周知

マネジメント層は、企業のITコントロールフレームワークを策定し、ポリシーを定義、周知する。継続的な周知プログラムを導入し、マネジメント層が承認および推進する使命、サービス目標、ポリシー、手続きなどを明確に表明する。情報を周知することで、IT目標の達成が促進され、さらにビジネスリスクおよびITリスクのほか、目標や指針についての認識と理解を得ることができる。このプロセスにより、関連法規へのコンプライアンスが確立される。

コントロール目標	価値のドライバー	リスクのドライバー
PO6.1 ITポリシーおよび統制環境 企業の経営理念および運営方針に合致するITの統制環境の要素を定義する。これらの要素には、IT投資による価値の実現に対する期待/要件、リスクの許容度についての考え方、インテグリティ、倫理的価値観、スタッフの能力、説明責任、および実行責任が含まれる。統制環境は、企業文化の上に構築する。企業文化は、重大なリスクへの対処の一方で、価値の提供を支援する。部門間の協力およびチームワークを促し、さらにコンプライアンスと継続的なプロセス改善を促進する。それればかりでなく、プロセスからの逸脱(失敗を含む)が適切に処理されることを支援する。	・包括的なIT統制環境 ・一連の包括的なITポリシー ・組織の使命への意識の向上 ・アプリケーションとITサービスの適切な利用	・組織の使命についての誤った情報伝達 ・誤って解釈された経営者の理念 ・組織のビジネス目標に沿っていない活動 ・明確なIT統制環境の不在 ・コンプライアンスとセキュリティの問題点

コントロール設計のテスト

- ITのリスクと統制環境を定義し管理するために設計された、「経営者の意向」を正式に伝達するものが存在し、それが組織の一般的なリスクと統制環境と合致しているかどうかを調査し、それを確かめる。
- コントロールの文化の伝達を確立し強化するため説明責任と実行責任を個人に割り当てているかどうかを判断する。
- 統制環境を支援するためのポリシーと活動(利用規程、バックグラウンドチェック)の存在を確かめる。
- このようなポリシーと活動の意識を向上するための教育を定期的に行っているかの証拠を閲覧する。
- 統制環境とリスクの許容度が環境の変化と合致しているかを確かにすべく、それらが十分かどうかを定期的に(少なくとも毎年)再評価するためのプロセスが存在するかどうかを判断する。
- 人事のポリシー(求職者に対するバックグラウンドチェック、新規採用者に対する教育、承認された行動規範、倫理に反する行動に対する適切な罰則)がIT統制環境を支援しているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO6.2 企業のITリスクおよび内部統制のフレームワーク 企業全体を対象としたITリスクとコントロールのアプローチを定義したフレームワークを作成および維持する。これにより、ITポリシーとコントロール環境、および企業リスクとコントロールフレームワークの整合が図られるようになる。	・ ITのコントロールとリスクについての包括的なフレームワーク ・ ITのリスクとコントロールに対する意識と理解 ・ 想定内および想定外の問題点が生じたときのビジネスへの悪影響の軽減	・ 企業にとって重要な情報の開示 ・ 識別されない不祥事 ・ 財務上の損失 ・ コンプライアンスとセキュリティの問題点

コントロール設計のテスト

・ 一般的に認識された業界標準/模範となる活動（COSO、COSO-ERM、COBIT）に基づいた、ITのリスクとコントロールについての正式なフレームワークが存在するかどうかを調査し、それを確かめる。
・ ITのリスクとコントロールのフレームワークが、組織全体のリスクとコントロールのフレームワークと合致しており、企業全体のリスク許容レベルを考慮しているかどうかを評価する。
・ ITのリスクとコントロールのフレームワークで、その対象範囲と目的を特定しており、経営者が何をコントロールする必要があるかの概要をまとめているかどうかを調査し、それを確かめる。
・ ITのリスクとコントロールのフレームワークが適切に定義され、責任が明確に記述され、しかるべき個人に割り当てられているかどうかを調査し、それを確かめる。
・ ITのリスクとコントロールのフレームワークの十分性と関連性を維持するために定期的にレビューするプロセスを実施しているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO6.3 ITポリシーの管理 IT戦略を支援する一連のポリシーを作成し、維持管理する。これらの一連のポリシーには、ポリシーの目的、役割と責任、例外対応プロセス、規定遵守アプローチ、および手続、標準、ガイドラインの参照情報を含める必要がある。これらのポリシーでは、その妥当性を定期的に検証および承認する必要がある。	・ 組織に適したポリシーと手続 ・ 組織内での品質 ・ アプリケーションとITサービスの適切な利用 ・ ITのコスト、便益、戦略、セキュリティレベルの明確性と理解	・ セキュリティ違反の数と影響の増大 ・ 容認されていない、または理解されていないポリシー ・ 経営者の目的と方向性に対する誤解 ・ 陳腐化していたり不完全なポリシー ・ 組織における貧弱なセキュリティ文化 ・ 明確性の欠如

コントロール設計のテスト
・ ポリシー、基準、手順書が階層構造になっており、ITの戦略と統制環境と合致しているかどうかを調査し、それを確かめる。 ・ 品質、セキュリティ、機密性、内部統制、倫理、知的所有権といった、関連する主要な表題についての具体的なポリシーが存在するかどうかを調査し、それを確かめる。 ・ ポリシー改訂プロセスが定義されており、少なくとも毎年レビューすることが要求されているかどうかを調査し、それを確かめる。 ・ コンプライアンスを追跡し、コンプライアンス違反の罰則を規定する手続が実施されているかどうかを調査して、それを確かめる。 ・ ポリシー管理プロセスのすべての要素が説明責任を持つ個人に割り当てられるよう、ポリシーを正式化、作成、文書化、承認、普及、コントロールするための説明責任が定義され文書化されているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO6.4 ポリシー、標準、および手続の展開 ITポリシーをすべての関連スタッフに確実に展開して徹底させる。これにより、ITポリシーが企業の運営に不可欠な要素として組み込まれる。	・ 組織の資産の適切な保全 ・ 組織のビジネス目標と合致した意思決定 ・ 組織の資産に対する効率的な管理 ・ ITリソースとITサービスの適切な利用	・ 容認されていない、または理解されていない、組織のポリシー、基準、手順書 ・ 経営者の目的と方向性の伝達の欠如 ・ 経営者の目的と合致していないコントロールの文化 ・ 正しく容認されていない、または理解されていないポリシー ・ ポリシーと手続に沿っていないことによるビジネスリスク

コントロール設計のテスト
・ ITのポリシーと基準を業務手順書に反映するためのプロセスを実施しているかどうかを調査し、それを確かめる。 ・ 雇用契約とインセンティブメカニズムがポリシーと合致しているかどうかを調査し、それを確かめる。 ・ 関連するITのポリシー、基準、手順書をユーザが受領し、理解し、容認することを明確に認識するプロセスが実施されているかどうかを調査し、それを確かめる。その認識を定期的に（半年おきに）新たにする。 ・ ポリシーの展開をサポートする技能が十分にある人材が利用可能かどうか確認する。

コントロール目標	価値のドライバー	リスクのドライバー
PO6.5 IT目標と指針の周知 全社的に、事業目標とIT目標、および該当する利害関係者やユーザに向けた指針に関する認識と理解を徹底する。	・明確に伝達された経営者の理念 ・組織の使命への意識の向上 ・組織内での、リスク、セキュリティ、目標などに対する意識と理解 ・組織のビジネス目標と合致した意思決定	・達成されないIT目標 ・容認または理解が不足した組織のポリシー ・タイムリーに識別されないビジネス上の脅威 ・経営者の目的と方向性に対する理解の欠如 ・ITの使命に対する確信と信頼の欠如 ・コントロールとセキュリティの文化の崩壊

コントロール設計のテスト
・経営者がITの目標と指針を定期的に伝達するプロセスが存在するかどうかを調査し、それを確かめる。 ・異なるレベルの担当者をサンプル的に選び、IT目標が明確に伝達され理解されていることを確かめる。 ・過去の伝達をレビューして、それが、使命、サービス目標、セキュリティ、内部統制、品質、倫理規範/行動規範、ポリシー、手続をカバーしていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

・「経営者の意向」を伝達する頻度、形式、内容を評価して、それがコントロール文化、リスク許容度、倫理的な価値、行動規範、経営者の誠実性の要件を効果的に定義し強化しているかどうかを判断する。

・統制環境をサポートするのに関係のあるポリシーと手続きに対する意識を高めるための定期的な研修（行動規範や倫理に関する毎年の研修、利用規定の定期的な確認）の証拠を閲覧する。従業員がITのマネジメント層のポリシーとリスク許容度を理解しているかどうか評価し、それが経営陣と合致している程度を判断する。質問と観察を通じて、IT統制環境に影響する主要なリスクと規制の要件に対する一般的な理解、または、ITのポリシーと手続に従うことの重要性に対する一般的な理解が存在するかどうかを評価する。

・ITのリスクとコントロールに対する企業全体のアプローチを規定し、ITのポリシーと統制環境を企業のリスクとコントロールのフレームワークに対応づけるような、ITのリスクとコントロールのフレームワークが存在するかどうかを決定する。

・ITのリスクとコントロールのフレームワークを導入し維持することに関連する責任が適切な担当者によって十分に実行されているかどうかを判断する。規定されたリスクとコントロールを閲覧し、それが情報システムとネットワークの機密性、インテグリティ、可用性をコントロールするのに十分かどうかを判断する。

・ITポリシーをレビューして、更新頻度および再評価が少なくとも毎年行われているかどうかを判断する。必要な調整と修正を行い、更新されたITポリシーが企業全体に適切に伝達されているかどうかを判断する。

・インタビューを通じて、ITポリシーを考案、作成、文書化、承認、普及させ、コントロールするのに適した役割と責任を果たす人に対して資源が配分されていることを確かめる。

・コンプライアンスをモニタリングし徹底することを含む、普及プロセスを支援するために、十分に技能のある人材が配置されていることを確かめる。インタビューを通じて、ITのポリシーと基準をサポートする運用手順書がしかるべき担当者によって伝達され理解され容認されているかどうか調べて確認する。

・サンプル的に選んだ従業員について、ITポリシーの認識と容認に関する文書を閲覧して、それが一貫して管理され定期的に新たにされていることを決定する。

- 証拠を閲覧して、ITの目標と指針を明確にするための伝達が行われ、経営者の支援が明確であることを確かめる。
- 伝達プロセスに、効果的な伝達に必要な資源と技能が与えられているかどうかを調査して、それを確かめる。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。
- ITポリシーを適切に管理しないことによって、IT資源に対するコントロールが十分でなかったりビジネス目標が達成されていないかを判断する。
- ITのポリシーと基準の十分な伝達、モニタリング、実施が欠如するによって、そのような基準の遵守が欠如していたり、関連するビジネスの達成目標を達成できていないかを決定する。
- ITの目標と指針を意識しないことによって、ビジネスの達成目標を達成できていないかを判断する。

PO7 IT人材の管理

ビジネス部門に対するITサービスの作成と提供のために、有能な人材を獲得し、維持する。これは、採用、研修、業績評価、昇進、および解雇を支援するために、文書化され合意された行動基準を遵守することで達成される。要員は重要な資産であり、ガバナンスおよび内部統制環境は要員の意欲と能力に大きく依拠するため、このプロセスは非常に重要である。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.1 要員の募集および保持 IT要員の募集プロセスを、組織全体の人事ポリシーおよび手続(採用、望ましい職場環境、新人研修などの手続)に従って維持する。組織の目標達成に必要なスキルを有するIT人材が適材適所に確実に配置されるプロセスを導入する。	・最適化され、組織の達成目標と合致したITスキル ・将来のビジネス要件を支援するのに適したITスキルを持つ人材の募集と維持の改善	・十分に支援されていない、ビジネスにとって重要なプロセスのためのITサービス ・効果的でないITソリューション ・IT人材管理が市場の状況と合致していないことによる、適切なIT人材の欠如

コントロール設計のテスト
・組織での戦略的および戦術的なITニーズに合致する技能の要件と、望ましい専門的な能力の定義を反映するIT人事管理計画が存在するかどうかを調査し、それを確かめる。その計画は、少なくとも毎年更新し、現在と将来の要件に対処するための具体的な採用と維持の行動計画を含めるべきである。長期休暇ポリシーの手続を規定どおりに実施するポリシーも含めるべきである。 ・IT人材の採用と維持のための文書化されたプロセスが実施されており、IT人事計画で識別された必要性を反映しているかどうかを調査し、それを確かめる。 ・人事の専門家が、IT人材の募集と保持のプロセスが組織のポリシーと合致していることを確かめるために、それらを定期的にレビューし承認していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.2 要員の能力 要員がそれぞれの役割を果たす上で必要な能力を有しているかどうか、学歴や研修内容、経験などを基に定期的に検証する。資格および認証プログラムを適宜取り入れて、中核となるIT能力要件を定義し、継続的に維持されているか検証する。	・特定の職責のための適切な能力と経験のあるスタッフ ・人員のキャリア開発、貢献、職務満足度の改善 ・ビジネスニーズに沿ったスキルの継続的な開発	・重要なビジネス要件で求められているような技能を有さないIT要員 ・昇進に満足していないIT要員 ・より大きな影響を与えるインシデントとエラーの増加

コントロール設計のテスト

- 要求されている技能、能力、資格を完全かつ適切に記述してかるかどうか、職務記述書のサンプルを閲覧する。
- 定期的に職務記述書をレビューし新規作成するためのプロセスが存在し実施されていることを確かめる。
- 組織での特定の要件に対処するのに適した教育、クロス・トレーニング、認定資格を含む技能の必要性をマネジメント層が識別しているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.3 役割に応じた人材配置 要員の役割、責任と報酬のフレームワークを定義し、モニタリングおよび監督する。同時に、管理ポリシーと管理手続、倫理規定と専門家としての行動基準を遵守することを要求する。監督の度合いは、職位に求められる機密性および付与される責任の範囲に応じて定める必要がある。	・組織のポリシー、行動、倫理の伝達と遵守 ・主要な機能についての明確な説明責任と実行責任 ・ビジネスの達成目標へ要員の貢献の向上	・不明確な指示に基づく、誤った行動と意思決定 ・監督が行き届かないことに起因するエラーとインシデントの増加 ・管理と監督が不十分であることに起因する要員の不満

コントロール設計のテスト

- 職務記述書のサンプルを閲覧し、責任、能力、および重要なセキュリティと遵守の要件を十分に定義してあることを確かめる。
- IT要員が職務の記述内容と責任を容認したことを認める書類のサンプルを閲覧する。
- 雇用契約条件をレビューして、機密保持、知的所有権、情報セキュリティの責任、内部統制、該当する法律と規制についての条項が存在するかどうか確かめる。これらは、機密情報の保持に関する組織の要件と合致しなければならない。
- リスクの高い職位での職務記述書のサンプルを閲覧し、コントロールと要求される監督の範囲がそれぞれの役割で適切かどうかを判断する。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.4 要員の研修 IT従業員の採用時に適切なオリエンテーションを行い、その後も継続的に研修を実施し、組織の目標達成に必要なレベルの知識、スキル、能力、内部統制とセキュリティへの意識を身に付けさせる。	・組織の成功へ向けての要員の貢献と成果の向上 ・従業員の各々の役割の効果的かつ効率的な割当て ・技術開発とマネジメント層の育成への支援と、それによる要員の維持 ・企業にとっての従業員の価値の増加	・不十分なセキュリティ意識と、それによるエラーやインシデント ・製品、サービス、活動に関する知識のギャップ ・不十分な技能と、それによるサービスの質の低下、及びエラーとインシデントの増加

コントロール設計のテスト

・研修の有効性を測定するプロセスのウォークスルーを行い、重要な研修と認識要件が含まれていることを確かめる。
・研修プログラムの内容が完全で適切かどうか閲覧する。研修を提供するメカニズムを確認し、コンサルタント、請負業者、期間契約社員、該当する場合には顧客と販売業者を含むIT人材のすべての利用者に情報が提供されているかどうかを判断する。
・研修プログラムの内容を閲覧し、組織のセキュリティポリシーと内部統制に基づいて、内部統制フレームワークとセキュリティ要件のすべてが含まれているかどうかを判断する（セキュリティ要件を遵守しないことの影響、企業の資源と設備の適切な使用、インシデントの取り扱い、情報セキュリティに対する従業員の責任）。
・研修の教材とプログラムが十分かどうかを定期的にレビューしているかどうかを調査し、それを確かめる。
・研修要件を決定するためにポリシーを閲覧する。研修要件のポリシーによって、研修と認識向上のプログラムに組織の重要な要件が反映されることを確実にしていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.5 個人に対する依存 知識の記録（文書化）、知識の共有、後任者育成、および予備要員の確保により、主要な要員に対する極度の依存を最小限に抑える。	・十分に支援され、継続的に目標と合致している、重要なIT活動 ・主要な人員がいない場合に備えたコンティンジェンシープラン ・内部IT要員によるインシデントのリスクの低下	・重要な役割を果たすのに不可欠な技能が利用できないことによる、インシデントの数と影響の増加 ・引継計画と昇進の機会の欠如による担当者の不満 ・重要なIT活動を実施する能力の欠如

コントロール設計のテスト

・主要な役割を果たす人についての文書を閲覧し、IT組織内で重要なプロセスで一人の担当者に依存していないか確かめる。
・主要な人材に過度に依存することのリスクを低減するための技法を研修プログラムで取り入れているかどうかを調査する。クロス・トレーニング、主要な作業の文書化、ジョブローテーション、知識の共有、組織内で重要な役割の引継計画をプログラムに含めるべきである。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.6 要員の人事認可手続 IT人材の募集プロセスには、経歴調査を含める。身元調査は、従業員、契約社員、およびベンダーに対して実施し、そのレビューの範囲および頻度は担当業務の機密性や重要性に応じて決定する。	・適切な人材採用 ・情報漏洩の積極的な防止と機密性の基準	・IT組織内から生じる脅威のリスクの増加 ・顧客や企業の情報漏洩と、企業の資産が脅威に晒される度合いの増加

コントロール設計のテスト
・機密情報取扱者の人物調査を実施するための選択基準を閲覧する。 ・機密情報取扱者の人物調査を要するような重要な役割が適切に定義されているかどうかレビューする。これは、従業員、契約社員、ベンダーに適用すべきである。 ・採用プロセスが経歴調査を含んでいるかどうかを調査し、それを確かめる。IT担当者の採用文書のサンプルを閲覧して、経歴調査が完了し評価されたかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.7 従業員の業績評価 組織の達成目標に向けた各従業員の目標、確立された標準、各職務固有の責任、これらの関連する成果については、タイムリーな評価を定期的に実施する。また、従業員に対して、成果および勤務態度に関する指導を適宜行う。	・個人および部門のパフォーマンスの、組織の達成目標への貢献における改善 ・従業員の満足度の改善 ・従業員からのフィードバックとレビューのプロセスからの、マネジメント層のパフォーマンスの改善 ・IT要員の効果的な活用	・非効率的な業務を識別する能力の欠如 ・効果的でない研修プログラム ・従業員の不満と、それによる人員維持の問題、及びインシデント発生の可能性 ・有能な担当者とその担当者が保持していた企業の知識の喪失

コントロール設計のテスト
・従業員の業績評価のサンプルを閲覧し、目標設定の基準がSMARRTの目標を含んでいるかどうかを判断する。これらは、中核となる能力、企業の価値、それぞれの役割で要求される技能を反映すべきである。業績評価プロセスのウォークスルーを行い、個人情報の利用に関するポリシーと手続が明確で該当する規制を遵守しているかどうかを判断する。 ・給与/評価プロセスを閲覧し、それが業績目標と組織のポリシーに沿っているかどうかを判断する。 ・業績改善計画を閲覧し、組織のポリシーと合致しており、IT組織を通じて一貫して適用されているかどうかを判断する。業績改善計画には、具体的に定義された達成目標、完了期限、改善を達成できない場合の是正措置の適切なレベルを含めるべきである。

コントロール目標	価値のドライバー	リスクのドライバー
PO7.8 職務の変更および解雇 職務の変更、特に解雇に際しては、臨機応変な対応を行う。知識の引継ぎ、責任の再割り当て、およびアクセス権の取り消しにより、リスクを最小限の押さえ、当該職務が確実に継続されるようにする。	・ビジネスにとって重要な業務の効率的かつ効果的な継続 ・従業員維持の改善 ・適時な適切なアクセス制限による、情報環境の安全性の向上	・従業員が解雇されたときの承認されていないアクセス ・ビジネスにとって重要な業務の円滑な継続の欠如

コントロール設計のテスト

- 従業員の自主退職のための退出手続が文書化されており、必要な知識の引継ぎ、適時な論理的および物理的なアクセスのセキュリティ、組織の資産の返却、退職者面接といったような、すべての必要な要素を含んでいるかどうかを調査し、文書を閲覧する。
- 職務の変更の手続が文書化されており、ビジネスプロセスの途絶を最小化するために必要なすべての要素を含んでいるかどうかを調査する。例えば、職務の指導、職務の引継ぎ手続、正式な事前研修といったようなものを含む。職務変更手続を閲覧して、その手続に一貫して従っているかどうかを判断する。
- 人事部を通じて、(過去6ヶ月から1年間に)退職/異動したユーザの一覧を入手する。

コントロール目標の達成をテストするために以下のステップを踏む。

- IT人材計画を閲覧して、組織でのITニーズが定義されていることを確かめる。IT人材計画は、組織の目標に基づいており、戦略的業務、該当する規制の要件、それに関連して必要なITの技能を含むべきである。
- 現在と将来のニーズが現在利用可能な技能に対して評価され、ギャップが行動計画へ反映されていることを確かめる。
- IT人事管理計画を閲覧し、それが、重要かつ不足している技能、個人評価の検討、報酬とインセンティブ、開発計画、個人の研修の必要性を含む、IT組織内での維持活動に言及しているかどうかを判断する。
- 職務記述書が定期的にレビューされ、職務記述書が、現在の人員のスキルセットの能力と資質を含んでいることを確かめる。現在の従業員のスキルセットを職務記述書の要件と比較する。サンプル的に選らんだ従業員の専門的な技能の開発計画を閲覧して、キャリア計画が十分かどうか判断する。開発計画には、能力開発の促進、個人の昇格の機会、主要な個人への依存を減らすための測定指標を含めるべきである。
- 職務記述書をレビューして、それぞれが最新かつ関連性があることを確かめる。サードパーティの従業員の義務が明確に記述され、所定の役割に適していることを確かめるために、従業員のハンドブック/サードパーティの合意を含める。情報セキュリティ、内部統制、法令遵守、知的財産権の保護、機密情報の保全の責任を含む、雇用条件を従業員が承認したことを示す書類を閲覧する。リスクの高い役割に適用される監督の度合いが適切であるかどうかを観察する。リスクの高い役割の活動についての手順書をレビューして、重要な意思決定に際して監督者の承認が要求され、実施されたかどうかを判断する。
- 人材管理活動の適切なベンチマーキングが同様の組織、該当する国際標準、業界のベストプラクティスに対して定期的に実施されたかどうかを判断する。監督のレベルが、割り当てられている職位と責任の重要さに適していることを確かめる。
- 自動化コントロールを調査して、特権ユーザの許可権限の変更を追跡する。
- アクセス権の提供に先立って、すべての新規ユーザに人材研修プロセスが提供され、毎年際提供されていることを確かめる。人材研修プログラムの内容が完全かつ適切かどうか閲覧する(内部統制と倫理規定に関する組織の要件についての教育など)。
- 研修提供メカニズムを閲覧して、コンサルタント、請負業者、期間契約社員を含む、IT資源のすべての利用者に情報が提供されているかどうかを決定する。該当する場合には、顧客と納入業者も含めるべきである。

- 人材研修プログラムが、適切な役割の認証および再認証のプロセスを含んでいることを確かめる。
- 研修の教材とプログラムが十分かどうか定期的にレビューされ、すべての必要な技能への影響を含んでいるかどうかを調査し、それを確かめる。
- 重要な従業員の訓練、認識を高めるプログラムと要件の、完了と有効性を測定するためのプロセスが存在することを確かめる。
- 重要な役割において、一担当者への依存を減らすための文書化された戦略をレビューする。職務分掌を含んでいるかどうか確かめる。ローテーションに適した役割を識別するためのプロセスを閲覧し、ローテーションが発生していることを確かめる。従業員に質問して、知識の共有を行っているかどうかを判断する。
- 保存されている業績評価情報を閲覧して、それが完全かつ正確に保存されたかどうかを評価する。その情報が適切な方法で利用されていることを検証する。業績評価の間およびその後に、マネジメント層が業績について適切なフィードバックを提供しているかどうかを従業員に質問する。個人の目標とその地位のために確立された業績基準に対して業績が評価されていることを判断する。業績評価プロセスが一貫して適用されており、それが業績目標と組織のポリシーに沿っているかどうかを判断する。
- 退職時の手続とプロセスを閲覧して、組織を通じて一貫して適用されているという証拠を得る。
- 職務の変更に関連して、アクセス権（論理的および物理的なアクセス）が適切かどうかをレビューする。古いアクセス権が異動期間中に保持されている場合には、職務分掌と代替的なコントロールへの影響を判断する。
- 解雇されたユーザのユーザアカウントが無効化され、異動したユーザに適切なアクセスが適用されていることを確かめる。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。

- 組織が主要な担当者に依存する度合いを評価し、能力と蓄積された知識の喪失が発生しないことを確かめる。
- 経営者のポリシーと手続、倫理規定、専門家の行動規定、雇用契約の条件、内部統制、情報セキュリティのポリシーと手続、規制の要件を遵守することを確実にするための、適切なモニタリングと監督が存在するかどうかを評価する。
- セキュリティ要件の認識レベルを評価して、規制の要件、知的財産、組織の評判、戦略的な地位を遵守していることを確かめる。
- 組織が資質のある人材を引きつけて維持する能力を確実にするための人材研修プログラムが、十分かどうかを判断する。
- 主要な担当者への依存と、IT組織がビジネスプロセスの継続的な支援を効率的かつ効果的な方法で提供する能力とを評価する。重要なコントロールが意図した通りに機能することを確実にするための、主要な役割での適切な職務分掌が存在するかどうかを判断する。
- 盗難、情報漏洩、重要な企業資産の侵害といったような組織内での脅威に対するコントロールに適切に対処することを確実にするための、主要な従業員に対するセキュリティチェックのメカニズムが適切かどうかを評価する。
- 適切に定義され、適時に一貫して適用される、業績評価プロセスが存在し、それによって、IT資源を効率的かつ効果的に利用できるようになっているかどうかを判断する。
- ビジネスにとって重要な業務の途絶と、安全な環境と組織の資産に対する承認されていないアクセスが生じないことを確実にするための、職務変更のポリシーと手続の適切さと一貫性のレベルを評価する。

PO8 品質管理

実績のある開発プロセス、調達プロセス、および標準が組み込まれたQMSが作成、維持されている。これは、明確な品質要件、手続、およびポリシーを提示し、QMSを計画、導入、維持することで実現できる。品質要件は、数値化された達成可能な指標として表し、周知する。モニタリング、分析、逸脱への対応、および利害関係者への結果報告を常時行うことにより、継続的な改善を実現する。品質管理は、ITによるビジネスへの価値提供と継続的な改善および利害関係者に対する透明性を確実に確保する上で不可欠である。

コントロール目標	価値のドライバー	リスクのドライバー
PO8.1 品質管理システム ビジネス要件に沿った品質管理に関して、標準化された、正式で、かつ継続的なアプローチを提供するQMSを確立し、維持する。QMSは、品質要件と品質基準、主要ITプロセスとその順序および相互関係を特定し、さらに不適合の定義、発見、是正、および防止に関するポリシー、基準、方法を特定する。QMSでは、役割、任務、および実行責任を含む品質管理の組織構造を定義する必要がある。すべての主要分野において、基準およびポリシーに沿った品質計画を作成し、品質データを記録する。QMSの効果および適用レベルのモニタリングと測定を行い、必要に応じて改善を行う。	・ ITに対するビジネス要件との合致および達成 ・ 利害関係者の満足の確保 ・ すべての担当者が理解し遵守する一貫したQA環境 ・ ITプロセスの効率的、効果的かつ標準化された運用	・ サービスとソリューションの不十分な品質、およびそれに起因する失敗、手戻り、コストの増加 ・ 場当たり的で信頼性のないQA活動 ・ 業界の優れた実践方法とビジネスの目標に対する整合性の欠如 ・ 品質に対する責任の所在の曖昧さと、それによる品質の低下

コントロール設計のテスト
・ ITマネジメント層、その他の利害関係者、関連する企業全体のフレームワークからのインプットによってQMSが作成されているかどうかを調査する。 ・ それぞれの品質レビューからの知見がITマネジメント層とその他の利害関係者にタイムリーに伝達され、是正措置を取れるようにしているかどうかを調査する。 ・ IT品質計画が企業全体の品質管理の基準とポリシーと合致しているかどうかを判断する。

コントロール目標	価値のドライバー	リスクのドライバー
PO8.2 IT標準および品質の実践基準 組織がQMSの目的を達成できるよう、主要なITプロセスについて、標準、手続、および実践基準を特定し、維持する。組織における品質の実践基準を改善、調整する際は、業界のベストプラクティスを参照する。	・ ビジネス要件及びポリシーとQMSとの合致 ・ 一貫性があり信頼できる一般的な品質計画 ・ 効果的かつ効率的なQMS運用 ・ ITの基準、ポリシー、手続、実践基準、リスク管理が効果的かつ効率的であるということに関する、企業全体のマネジメント層にとっての、確信度の増加	・ プロジェクトとサービスの中での定義されていない実行責任 ・ 主要なITプロセスでの品質の不足 ・ 定義された基準と手続に対する違反 ・ ITのポリシー、基準、プロセス、実践基準と、現在の優れた実践手法との不整合 ・ ITのポリシー、基準、プロセス、実践基準と企業全体の目標との不一致

コントロール設計のテスト

- ITの基準とフレームワークをレビューして、それがその環境でのシステム、データ、情報にふさわしいかどうかを判断する。
- ITの基準からの逸脱の承認を閲覧して、義務化または、承認された基準を遵守しているか否かを検証する。
- 主要なプロジェクトの主要なマイルストーンを閲覧して、QMSが適用されていることを確かめる。
- 組織内で義務化または、承認された基準を変更するプロセスを確かめる。

コントロール目標

PO8.3 開発および調達標準

最終成果物のライフサイクルを通じてすべての開発および調達に関する標準を導入および維持し、主要な肯定ごとに、合意された承認基準に基づいて承認を得る。ソフトウェアコーディング標準、命名規則、ファイル形式、スキーマとデータディクショナリの設計標準、ユーザインターフェース標準、相互運用性、システムパフォーマンス効率、拡張性、開発標準、およびテスト標準、要件に照らした評価、テスト計画、単体テスト、回帰テスト、および統合テストを検討する。

価値のドライバー

- ビジネスの目標を適時に達成するための、効率的かつ効果的な技術の利用
- 主要な調達活動及び開発活動に関する、適切な識別、文書化、実行
- 調達と開発を管理するための、正式に定義され、標準化され、繰り返し可能なアプローチの採用

リスクのドライバー

- プロジェクトのタイムスケールと予算に対する不正確な見積り
- プロジェクト内での不明確な責任分担
- 開発と導入におけるエラーと、それに起因する遅延、手戻り、コストの増大
- 相互運用性と統合における問題
- サポートと保守における問題
- 本番環境での識別されないエラー

コントロール設計のテスト

- 既存のIT資源に対する変更に、開発標準と調達標準が適用されているかどうかを調査する（エラーのないコーディング、ソフトウェアコーディング標準、命名規則、ファイル形式、スキーマとデータディクショナリの設計標準、ユーザインターフェース標準、相互運用性、システムパフォーマンス効率、拡張性、開発標準、およびテスト標準、要件の妥当性評価、テスト計画、単体テスト、回帰テスト、および統合テストなど）。
- 開発標準と調達標準によって、既存のIT資源への変更のためのコントロールが適切なレベルかどうか尋ねるか調査する。
- 開発と調達の指導がITの標準とフレームワークに取り込まれているかどうかを調査する。

コントロール目標	価値のドライバー	リスクのドライバー
PO8.4 顧客中心 顧客の要求事項を特定し、それらとIT標準およびITの実施内容との調整を図ることにより、顧客に焦点を当てた品質管理を行う。ユーザ/顧客とIT組織の間に生じる対立の解決に関する役割と実行責任を定義する。	・顧客満足度の改善 ・品質管理と顧客の期待との合致 ・明確な役割と責任	・期待とサービス提供との間のギャップ ・顧客の期待に対する不十分な理解 ・顧客との係争や顧客からのフィードバックに対する不十分な対応 ・顧客との係争を解決するための不適切ないし効果的でないプロセス ・提供されている異なるサービスに対する不適切な優先順位付け ・成果物と品質の不備に関する係争

コントロール設計のテスト

・品質管理プロセスに対する顧客側の評価を把握しているかどうかを調査する。プロセスをレビューして、顧客側の評価を定期的に把握していることを確かめる。
・顧客からの質問、アンケート調査、フィードバックフォーム、インタビューを閲覧して有効性を確かめる。
・フォローアッププロセスからのアウトプットを閲覧して、そのフィードバックが、組織され、苦情対応プロセスを改善するのに有用であるかどうかを判断する。
・役割と責任の文書を閲覧して、顧客の不満による係争を有効に解決できるようになっているかどうかを判断する。
・顧客とのやり取りの側面が研修プログラムに含まれているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO8.5 継続的改善 継続的な改善を促進する総合的な品質計画を維持し、定期的に周知する。	・サービスとソリューションの品質の改善 ・サービス提供の効率性と有効性の改善 ・従業員の士気と労働満足度の改善	・コントロールが有効でなく効果的でないようなサービス提供 ・不十分なサービス ・開発における不備

コントロール設計のテスト

・それぞれの品質レビューからの結果がITマネジメント層とその他の利害関係者に適時に伝達され、是正措置を取れるようにしているかどうかを調査する。
・従業員研修プログラムが継続的な改善のための効果的な方法論を含んでいることを確かめる。
・継続的な改善の活動を積極的に促進し、効果的に管理し、品質の基準書、ポリシー、実践基準、手順書の中に導入しているかどうかを調査する。
・品質管理計画が定義されているかどうかを調査して、それを確認する。計画と文書を閲覧して、学習と知識の共有のプロセスが適切かどうか検証する。

コントロール目標	価値のドライバー	リスクのドライバー
PO8.6 品質の測定、モニタリング、およびレビュー QMSへの継続的なコンプライアンスおよびQMSが提供する価値をモニタリングするための測定項目を定義し、計画して導入する。プロセスオーナは、適切な是正措置および予防措置を講じるために、情報を測定、モニタリング、および記録する必要がある。	・品質の成果を意識している従業員 ・一貫した報告 ・組織のQMSへと統合されており、組織のQMSを活用している品質報告 ・測定可能で明確なQMSの価値 ・QMSの遵守と有用性に関するフィードバック	・明確で一貫した品質目標の欠如 ・識別されていない防止活動と是正活動 ・一貫しない品質報告 ・企業全体のQMSに貢献しない報告 ・明確化された目標の欠如 ・一貫しない品質報告 ・組織の目標を促進しないQMS ・QMSを重視していなかったり遵守していなかったりする組織 ・QMS内で認識されない長所と短所 ・識別されないコンプライアンス違反 ・納期に遅延し予算を超過し、十分でない品質で提供されるリスクがあるプロジェクト

コントロール設計のテスト

・品質の成果についての役員レベルの報告（ダッシュボードレポーティングやバランススコアカード）をレビューして、長所と短所の傾向を識別する。
・品質の測定指標が、ビジネスとITの戦略の達成、財務上のコスト、リスクレート、入手可能な業界でのデータを盛り込んでいるかどうかを調べる。モニタリングプロセスによって、是正活動や防止活動を実施することができるかをレビューする。
・品質管理プロセスに対してウォークスルーを実施して、それが妥当性、適用性、最新の業界データ、組織内での継続的な改善のプログラムへの貢献の価値を考慮していることを確かめる。

コントロール目標の成果をテストするために以下のステップを踏む。
・QMSを閲覧して、それが品質管理のための標準化された継続的なアプローチを提供していることを確かめる。
・ITマネジメント層がQMSを承認していることを確かめる。
・定期的な成果のレビューをして、そのレビュープログラムがすべての必要な要素を含んでいるかどうかを判断する。
・QMSの成果に対する定期的に第三者が実施したレビューの結果を閲覧する。
・重要な知見が生じた場合の品質保証計画でのフォローアップレビューが存在するかどうかを調査し、そのフォローアップレビューを閲覧して是正措置が有効であることを確かめる。
・QMSベンチマークの結果を閲覧して、業界での適切なガイドライン、標準、組織が比較の際に含まれているかどうかを判断する。
・ITの基準からの逸脱の承認を閲覧して、利害関係者の要件を遵守しているか、あるいは遵守していないかを検証する。
・主要なマイルストーンを閲覧して、QMSが運用されていることを確かめる。
・顧客の品質基準と測定指標の要件を閲覧してその網羅性を確かめる（質問、アンケート調査、フィード

バックフォーム、インタビュー）。
- QMSフォローアッププロセスからのアウトプットを閲覧して、そのフィードバックが整理され、苦情対応プロセスを改善するのに有用であるかどうかを判断する。
- 役割と責任の文書を閲覧して、顧客の不満による係争を有効に解決できるようになっているかどうかを決定する。
- 研修プログラムを閲覧して、顧客ケアの内容が存在するかどうかを確かめる。
- 定期的な成果のレビューに対するウォークスルーを実施して、そのレビュープログラムがQMSの必要な要素を含んでいるかどうかを決定する。
- QMSの成果に対する定期的に第三者が実施したレビューの結果を閲覧する。
- 品質の測定指標が、ビジネスとITの戦略の達成、財務上の費用、リスクレート、入手可能な業界でのデータを盛り込んでいるかどうかを調べる。
- モニタリングプロセスによって、是正活動や防止活動を実施することができているかどうかをレビューする。
- QMSプロセスに対してウォークスルーを実施して、それが妥当性、適用性、最新の業界データ、組織内での継続的な改善のプログラムへの貢献の価値を考慮していることを確かめる。
- 業界のベストプラクティスとの整合性と、現在の手続とビジネスでの期待との間のギャップを評価することによって、品質保証活動の信頼性を判断する。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。
- 組織のIT標準と品質活動の遵守のレベルを判断し、合致しないシステムアーキテクチャをもたらし、コストが増大し、プロジェクトが達成目標と目的に合致しなくなるような逸脱を評価する。
- 開発標準と調達標準が、ITとビジネスの資源を効率的かつ効果的に利用し、戦略的な達成目標と目的を達成できるようにするために、プロジェクトのタイムスケールと予算の正確な評価のためのプロセスを含んでいるかどうかを判断する。
- 品質管理プロセスが、利害衝突を解決し、顧客の期待と製品/処理能力についての理解の一貫性を測定するためのメカニズムを含んでいることを確かめる。
- 顧客の要求がITの標準と合致しているかどうかを評価する。
- 継続的な改善のポリシーと手続によって、組織が競争優位を維持できているかどうかを判断する。
- 品質測定プロセスと報告メカニズムによって、是正措置を適時に実施できるようになっているかどうかを評価する。

PO9 ITリスクの評価と管理

リスクマネジメントフレームワークが構築され、維持されている。フレームワークでは、合意された一般的なITリスクレベル、リスク軽減戦略、および未解決のリスクについて文書化する。すべての計画外のイベントが組織の達成目標に与える潜在的な影響を特定、分析、評価する。未解決のリスクを許容レベルまで軽減するために、リスク軽減戦略が導入されている。利害関係者が理解可能なように評価結果をとりまとめると同時に、財務的な観点でもとりまとめる。これにより、利害関係者から見ても、リスクが許容範囲に収まるようにする。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.1 ITリスクマネジメントフレームワーク 組織の（企業の）リスク管理フレームワークと整合的なITリスク管理フレームワークを確立する。	・ ITリスク管理のための一貫したアプローチ ・ ITリスクの効果的な管理 ・ 現在のITリスクと組織にとっての脅威に関する継続的な評価 ・ 広範なITリスク管理アプローチ	・ 別々に管理されているITリスクとビジネスリスク ・ ITリスクがビジネスに及ぼす、発見されない影響 ・ リスク管理のためのコストのコントロールの欠如 ・ 全体の中ではなく単一の脅威としてみなされているそれぞれのリスク ・ リスク評価の際のマネジメント層による支援不足

コントロール設計のテスト
・ ITリスク管理フレームワークが組織（企業）のリスク管理フレームワーク合致しており、戦略、プログラム、プロジェクト、業務のためのビジネス主導の構成要素を含んでいるかどうか調査する。ITリスクの分類をレビューして、それが、全社的なリスク管理フレームワークの共通した特性に基づいていることを確かめる。ITリスクの測定が標準化され優先順位がつけられているかどうか、それが、企業全体のリスク管理フレームワークと合致しており、影響、残存リスクの許容、発生可能性を含んでいるかどうかを調査する。 ・ IT戦略計画の策定とレビューでITリスクが考慮されているかどうかを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.2 リスクをめぐる状況の明確化 リスク評価フレームワークの適用背景を明確化し、確実に適正な結果が得られるようにする。これには、個々のリスク評価の社内外における背景、評価の達成目標、およびリスクが評価される基準の確定が含まれる。	・ リスク管理のための効果的かつ効率的なリソースの利用 ・ リスク管理の優先順位のビジネスニーズとの合致 ・ 関連性があり、重要なリスクへの焦点 ・ リスクの優先順位づけ	・ 関連性が少ないのに重要だと考えられているリスク ・ 重要なのに適切な注意を払われていないリスク ・ リスク評価に対する不適切なアプローチ

コントロール設計のテスト
・ 企業全体のリスク管理のポリシーと原則に沿って、適切なリスク状況を定義してあり、それが、システム、プロジェクト管理、アプリケーションソフトウェアのライフサイクル、ITの運用とサービス管理のようなプロセスを含んでいるかどうかを調査し、それを確かめる。内部と外部のリスク要因を含めるべきである。 ・ ITリスクの状況が伝達され理解されているかどうかを判断する。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.3 イベントの特定 ビジネス、法規制、法律、技術、取引先、人材、および運用面において、企業目標または企業運営に悪影響を与える可能性のあるイベント(該当する深刻な脆弱性を悪用する重大で現実的な脅威)をすべて特定する。影響の特徴を特定し、この情報を保持する。該当するリスクをリスクレジストリに記録し、維持する。	・ リスクイベントの識別に対する一貫性のあるアプローチ ・ 重要なリスクイベントへの焦点	・ より重要なイベントが見過ごされている中での、関連性の乏しいリスクイベントの識別と重視

コントロール設計のテスト
・ 潜在的なイベントを識別するために用いているプロセスを閲覧して、すべてのITプロセスが分析に含まれているかどうかを判断する。プロセスの設計は、内部と外部のイベントをカバーすべきである。潜在的なイベントの識別は、前回の監査、調査、および、チェックリスト、ワークショップ、プロセスフロー分析を用いて識別されたインシデントの結果を含む可能性がある。識別された影響をリスクレジストリで追跡して、そのレジストリが完全であり、最新であり、企業全体のリスク管理フレームワークの用語と合致しているかどうかを判断する。 ・ 適切な機能横断的なチームが、イベントと影響を識別する様々な活動に関与しているかどうかを調査する。リスクレジストリのサンプルが脅威、脆弱性の重要性、影響の重要性と関連しているかどうかをレビューし、そのプロセスがリスクを識別し、記録し、判断する上で効果的かどうかを分析する。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.4 リスク評価 特定されたすべてのリスクの発生可能性と影響を、定性的および定量的な方法を用いて繰り返し評価する。内在しているリスクおよび残存リスクの発生可能性と影響は、種類別、およびポートフォリオに基づいて、それぞれ判断する必要がある。	・ ITリスク管理に関する技能とリソースの利用及び計画の改善 ・ ITリスク評価機能チームに対する、組織からの信頼 ・ リスク管理者の間での知識の引継ぎ ・ IT資産の価値への意識づけ	・ 関連性が少ないのに重要だと考えられているリスク ・ 全体の中ではなく単一のイベントとしてみなされているそれぞれのリスク ・ 重要なリスクをマネジメント層に説明する能力の欠如 ・ 重要なリスクを見逃す可能性 ・ IT資産の喪失 ・ IT資産の機密性やインテグリティへの違反

コントロール設計のテスト

- リスク管理プロセスに対するウォークスルーを実施して、固有リスクと残存リスクが定義され文書化されているかどうかを決定する。
- リスク管理プロセスで、識別されたリスクを定性的ないし定量的に評価しているかどうかを調査し、それを確かめる。
- プロジェクトとその他の文書を閲覧して、定性的ないし定量的なリスク評価が適切かどうかを評価する。
- プロセスに対するウォークスルーを実施して、分析で用いている情報源が合理的かどうかを判断する。
- 発生可能性を定性的または定量的に測定するための統計分析の利用と発生可能性の測定を調査する。
- リスク相互間のいかなる相関も識別されているかどうかを質問または調査する。すべての相関をレビューして、それが、明確に異なる発生可能性を示しており、そのような関係から生じる結果に影響を及ぼすことを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.5 リスクへの対応 コスト効率に優れたコントロールによって、リスクの発現を継続的に軽減できるように考案したリスク対応プロセスを作成し、維持する。リスク対応プロセスでは、回避、軽減、共有、および受容などのリスク対応戦略を明確化する。これに伴う実行責任を特定し、リスク許容レベルについて検討する。	・効果的なリスク管理 ・リスク軽減のための一貫したアプローチ ・費用対効果の高いリスク対応	・効果的でないリスク対応 ・識別されていない残存ビジネスリスク ・リスクに対処するための効果的でないリソースの利用 ・十分でない既存コントロールへの過度の依存

コントロール設計のテスト

リスク評価の結果が、それぞれのリスクを回避、移転、軽減、または受容するための軽減対応に割り当てられており、組織全体でリスクを軽減するためのメカニズムと合致しているかを調査する。

コントロール目標	価値のドライバー	リスクのドライバー
PO9.6 リスク対応実行計画の維持およびモニタリング 必要とされたリスク対応策の導入に向け、コントロール活動をすべてのレベルにわたり優先順位付けし、計画を策定する。活動計画には、コスト、便益、および実行責任の明確化が含まれる。推奨される実行策および残存リスクの受容に関する承認を求め、約束した実行策を、影響を受けるプロセスのオーナに、確実に自らのものとして認めさせる。計画の実行を監視し、何らかの逸脱があった場合は経営層に報告する。	・効果的なリスク管理 ・現在のリスクと組織にとっての脅威に関する継続的評価	・意図した通りに機能しない、リスク軽減のためのコントロール ・識別されたリスクから逸脱している代替的コントロール

コントロール設計のテスト

- 受容されたリスクがリスク行動計画で正式に認識され記録されているかどうかを調査する。
- リスク管理計画の要素が適切かどうか評価する。
- 実行、報告、逸脱がモニタリングされているかどうか尋ねるか、調査する。
- リスク対応が適切な承認を得ているかを調査する。
- 活動をレビューして、オーナシップが割り当てられ、文書化されているかどうかを確かめる。
- リスク行動計画が効果的に維持され、調整されているかどうかを調査する。

コントロール目標の成果をテストするために以下のステップを踏む。

- ITリスク管理の許容レベルが企業全体のリスク許容レベルと合致しているかどうかを調査する。組織のリスク許容度が、ビジネスとITの戦略策定の両方のインプットとして用いられているかどうかを判断する。
- 企業全体のリスク許容レベルをITリスク管理の意思決定に適用するプロセスが存在するかを調査する。同様の組織、適切な国際標準、業界のベストプラクティスに対して、リスク評価フレームワークのベンチマーキングを実施したかどうか検討する。
- リスクに関連する説明責任と実行責任が理解され受容されられているかどうかをテストする。適切な技能と必要な資源がリスク管理のために利用可能であることを確認する。
- 関与している主要な担当者へのインタビューを通じて、コントロールメカニズム、その目的、およびその説明責任と実行責任を理解し、適用しているかどうかを調査する。
- 活動がITマネジメントプロセスへと効果的に統合されているかどうかを調査する。
- 識別された影響が、企業にとって関連があり重要であるかどうか、それが過大評価または過小評価されていないかどうかを調査する。機能横断的なチームがイベント分析プロセスに貢献しているかどうかを判断する。インタビューと影響に関する報告を通じて、イベント識別ワークグループが、企業全体のリスク管理フレームワークについて適切な研修を受けているかどうか確かめる。影響度の評価のときに、相互依存と発生確率を正確に識別したかどうか確かめる。すべての相関をレビューして、それが、明確に異なる発生可能性を示しており、そのような関係から生じる結果に影響を及ぼすことを確かめる。
- リスク管理プロセスを閲覧して、分析で用いている情報源が合理的かどうかを判断する。
- リスクの発生可能性を定性的または定量的に測定するための統計分析の利用と発生可能性の測定を調査する。
- プロセスに対するウォークスルーを実施して、固有リスクと残存リスクが定義され文書化されているかどうかを判断する。
- リスク行動計画を閲覧して、優先順位、スケジュール、期待される結果、リスクの軽減、費用、便益、成果の測定指標および確立すべきレビュープロセスを特定しているかどうかを判断する。
- リスク対応が適切な承認を得ているか調査する。活動をレビューして、オーナシップが割り当てられ文書化されているかどうかを確かめる。
- リスク管理計画が効果的に維持/調整されているかどうか調査する。
- 行動計画の結果を閲覧しレビューして、それがリスクフレームワークのガイドラインと合致し、実施され、ビジネス目標への変更を反映しているかどうかをを判断する。計画をレビューして、それがリスクの回避、軽減、共有の観点から設計されていることを確かめる。コストと便益を考慮する際にリスク対応が含まれ、選択されているかどうか調査する。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。

- ITリスク管理戦略を評価して、それが企業全体のリスク管理戦略と組織のリスク許容度と合致しているかどうかを判断する。識別されていないリスク、IT資源の間違った適用、規制の要件と組織の達成目標への遵守違反の可能性に対処していることを確かめる。
- 未発見のリスク、非効率的で効果的でないコスト制約、軽減されていないリスク、コントロールされていないまとまったリスクレベル、組織の資産の紛失、評判の失墜、戦略目標からの逸脱、法令違反を含む、イベントの識別の正確性と網羅性を評価する。
- 企業全体でのリスク軽減におけるリスク行動計画の有効性を評価し、リスクと軽減との相関を調査する。

- リスク行動計画の結果をレビューして、その有効性を評価し、オーナが軽減活動の際に適時に対応したかどうかを確かめる。
- 高リスクの脅威に適用されるリスク軽減活動をレビューして、優先順位付けの有効性を評価する。

PO10 プロジェクト管理

すべてのITプロジェクトの管理を目的とするプログラムおよびプロジェクト管理フレームワークが確立されている。このフレームワークでは、すべてのプロジェクトを適正に優先順位付けし、プロジェクト間の調整を行う。プロジェクトのリスクマネジメントおよびビジネスへの価値の提供を実現するため、フレームワークには、基本計画、資源の割り当て、成果物の定義、ユーザによる承認、サービスの提供に対する段階的なアプローチ、QA、正式なテスト計画、テストの実施と導入後レビューの実施が含まれる。このアプローチにより、予想外のコストやプロジェクトの中止によって生じるリスクが軽減され、ビジネス部門およびエンドユーザへの情報伝達および両者の関与が促進される。さらに、プロジェクト成果物の価値と品質が保証され、IT関連の投資プログラムに対するそれらの貢献度を最大化できる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.1 プログラム管理フレームワーク プロジェクトの特定、定義、評価、優先順位付け、選択、開始、管理、およびコントロールにより、IT関連の投資プログラムのポートフォリオに関連する、プロジェクトのプログラムを維持する。各プロジェクトが確実にプログラムの目標の達成を後押しするようにする。複数のプロジェクトのアクティビティおよび相互依存を調整し、プログラム内のすべてのプロジェクトが期待される成果の達成に貢献するよう管理し、資源要件や資源にかかわる問題に対処する。	・プログラム管理のために最適化されたアプローチ ・組織をまたぐプログラム管理のための、標準化され、信頼でき、効率的なアプローチ ・プログラム内で主要なプロジェクトに焦点を当てる能力の向上	・プロジェクトへの不適切な優先順位付け ・プロジェクトプログラムへの組織的でなく効果的でないアプローチ ・プロジェクトとプログラムの目標との不整合

コントロール設計のテスト

- プログラム管理フレームワークをレビューして、以下を確かめる。
  - フレームワークが、ITプロジェクトの集計されたポートフォリオをプログラムの目標に照らし合わせて評価可能なように設計されている
  - 資金、プロジェクト管理者、プロジェクトチーム、該当する場合にはITの資源とビジネスの資源を含む要求された資源をプログラムで特定しており、プログラム管理チームが各プロジェクトに、利益の達成、コストのコントロール、リスクの管理、プロジェクト活動の調整を含む説明責任を明確かつ曖昧さなしに割り当てている
  - 説明責任が割り当てられている場合には、そのような説明責任が受け入れられている。義務と範囲が明確である。説明責任を持つ人が、行動するのに十分な権限と裁量、必須の能力、十分に見合った資源、説明責任の明確な区別、権利と義務の明確な理解、関連する成果の測定指標を持っている
- 計画、ポリシー、手続をレビューして、プログラム管理チームが以下を行っていることを確かめる。
  - プログラム内の複数のプロジェクトの相互依存を判断する
  - プログラム全体のスケジュールに間に合うように、完了までのスケジュールを作成する
  - 企業の内外にいるプログラムの利害関係者を特定する
  - プログラムの利害関係者と、適切なレベルの協力、意思伝達、連絡を確立する
  - プログラムの利害関係者とプログラムの継続のための意思伝達を維持する
- プログラム管理チームが以下を行っていることを定期的に確かめる。
  - 現在のプログラムが設計された通りであり、ビジネスの要件に合致するということをビジネスのマネジメント層と共に確かめ、必要に応じて調整を行う
  - 個々のプロジェクトの進捗をレビューし、スケジュールのマイルストーンに合わせるために、必要に応じて、資源の利用可能性を調整する
  - 技術とIT市場の変化を評価し、新たに生じるリスクを避けるために、プログラムの調整を行うか、新しくより効率的な技術ソリューションを利用するか、コストを下げることのできるような市場の変化を活用すべきかどうかを判断する

コントロール目標

PO10.2 プロジェクト管理フレームワーク

各実施プロジェクトに導入、適用する方法論に加え、プロジェクト管理の範囲と境界を定義するプロジェクト管理フレームワークを確立し、維持する。フレームワークおよびフレームワークを支える手法は、プログラム管理プロセスに統合されている必要がある。

価値のドライバー

- プロジェクトの成功の可能性の増加
- プロジェクト管理の活動と規律の確立に関連するコストの減少
- プロジェクトの目標、プロジェクト管理活動、プロジェクトの進捗に関する効果的な伝達
- 一貫性のあるアプローチ、ツール、及びプロセス

リスクのドライバー

- 組織内でのプロジェクト管理のための異なるアプローチ
- 組織の報告体制の遵守の欠如
- 一貫性のないプロジェクト管理ツール

コントロール設計のテスト

- 計画、ポリシー、手続きをレビューして、プロジェクト管理フレームワークが以下のようであることを確かめる。
  - 組織のプログラム管理フレームワークと合致しており、不可欠な構成要素である
  - プロジェクトの対象範囲の変更を記録し、評価し、伝達し、承認するための変更コントロールプロセスを含んでいる
  - 状況が変化しても適切であり続けるよう、定期的に評価されている
  - 既存のプログラムやプロジェクトのオフィスの役割と利用法についての助言や、プロジェクトのためにそのような機能を設けることについての助言を含んでいる

コントロール目標

PO10.3 プロジェクト管理のアプローチ
各プロジェクトの規模、複雑度、および法的要件に応じたプロジェクト管理のアプローチを確立する。プロジェクトガバナンスの体制には、プログラムのスポンサー、プロジェクトのスポンサー、運営委員会、プロジェクトオフィス(project office)、およびプロジェクト管理者の役割、実行責任、および説明責任のほか、それぞれが定められた責務(報告、段階ごとのレビューなど)を果たすための手段となる仕組みを組み込むことができる。すべてのITプロジェクトに対し、総合的な戦略プログラム内でのプロジェクトの実行に必要な権限を持つスポンサーを確実に割り当てる。

価値のドライバー

- プロジェクト管理のための最適化されたリソースの利用
- 明確な役割と責任、それによる主要な意思決定と作業に対する明確な説明責任とコミットメント
- プロジェクト目標とビジネス目標との整合性の向上
- プロジェクトの問題点に対する適時かつ迅速な対応と処理を行う能力

リスクのドライバー

- 組織内で異なるプロジェクト管理のアプローチを用いていることによる混乱と不確実性
- 組織の報告体制の遵守の欠如
- プロジェクトの問題点に対しての、最適かつ承認された意思決定による対応の不在

コントロール設計のテスト

- 計画、ポリシー、手続きをレビューして、以下を確かめる。
  - それぞれのプロジェクトの開始に先立って、プログラム管理チームが、プロジェクトの規模、複雑さ、リスク(法的リスク、規制のリスク、評判のリスクを含む)に適したプロジェクト管理ガバナンス体制を確立する。プロジェクト管理ガバナンス体制は、プログラムスポンサー、プロジェクト管理者、そして必要に応じて運営委員会の人やプロジェクトマネジメントオフィスの人の実行責任と説明責任を割り当てるべきである。
  - プログラム管理チームがそれぞれのITプロジェクトに、戦略プログラム全体の中でプロジェクトの実行を管理するのに十分な権限を持つ、一人または複数のスポンサーを割り当てる。この任命は、明確に行われ、役割と責任が簡潔であり、責任が被任命者に容認されられている。
- プロジェクトの実行を追跡するのに効果的なメカニズム(定期的な報告、段階ごとのレビューなど)が実施されているかどうかを調査して、それを確かめる。計画、ポリシー、手続、報告をレビューして、プログラム管理チームによってメカニズムが効果的に設計されており、逸脱を適時に識別し管理するために用いていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.4 利害関係者の関与 IT関連の投資プログラム全体の枠内におけるプロジェクトの定義と実行において、影響を受ける利害関係者の関与と協力を得る。	・プロジェクトがビジネスの便益を原動力とし、かつビジネスの便益を提供する可能性の増加 ・ビジネス、エンドユーザ、ITで共有された、プロジェクトの目的に対する理解 ・プロジェクトに対するユーザのコミットメントと関与	・コストのコントロールとプロジェクトの成功を確実にするには不明確な実行責任と説明責任 ・要件定義と成果物のレビューに際しての利害関係者の不十分な参加 ・ビジネスの便益に対する理解と、ビジネスの便益の提供の減少

コントロール設計のテスト

・以下を質問して確認する。
  – プロジェクト管理フレームワークのもとで、プロジェクトの開始、定義、承認に際して、影響を受けるユーザ部門の統括責任者と主要なエンドユーザを含む主要な利害関係者のコミットメントと参加が得られている
  – プロジェクトの開始時に主要な利害関係者とエンドユーザの参加を求めており、プロジェクトのライフサイクルの間に改善されている
・プロジェクト報告をレビューして、プロジェクトの承認、プロジェクトフェーズの承認、プロジェクトのチェックポイントでの報告、プロジェクト委員会への代表者の選出、プロジェクト計画、製品のテスト、ユーザの研修、ユーザの手順書の作成、プロジェクト伝達書類の作成において継続的に関与しているを確かめる。
・主要な利害関係者とエンドユーザにインタビューし、導入後のレビューの結果を閲覧して、プロジェクト成果物の品質と受入れの向上のために、利害関係者とエンドユーザが関与したことを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.5 プロジェクト範囲の記述 プロジェクトの性質および範囲を定義および文書化し、プロジェクトの範囲およびIT関連の投資プログラム全体の枠内における他のプロジェクトとのリレーションシップについて、すべての利害関係者が共通の認識を持つようにし、その体制を促進する。この定義については、プロジェクトの開始前に、プログラムおよびプロジェクトのスポンサーから正式な承認を得なければならない。	・プロジェクトの進捗と最終的な成功を測定できるよう提供された基準 ・主要なビジネスの利害関係者を含む説明責任の割り当てと明確化 ・プロジェクトのための効果的なリソースの利用 ・プロジェクトのマスタープラン作成の促進	・プロジェクトの目的と要件に対する誤解 ・ビジネスとユーザの要件へのプロジェクトの不適合 ・プロジェクトに関連する他のプロジェクトへの影響に対する誤解

コントロール設計のテスト

・計画、ポリシー、手続をレビューして、以下を確かめる。
  - プロジェクト管理フレームワークでは、利害関係者に対して、プロジェクトでの作業が始まる前に、プロジェクトの対象範囲への理解を利害関係者が共有できるように、各プロジェクトの目的、対象範囲、ビジネスでの価値を定義した、明確な書面を提供している
  - 高レベルでの主要成功要因と重要な成果指標を初期に検討することを含め、プロジェクトの要件が、主要な利害関係者および組織内でのプログラムとプロジェクトのスポンサーによって、合意され容認されている
  - プロジェクトの対象範囲に対するすべての変更が適切に文書化され、利害関係者によって承認されている

コントロール目標	価値のドライバー	リスクのドライバー
PO10.6 プロジェクトの各フェーズの開始 プロジェクトの主要フェーズの開始を承認し、すべての利害関係者に周知させる。第一フェーズの承認は、プログラムのガバナンスに関する決定に基づいて行う。以降の各フェーズの承認は、前フェーズの成果物のレビューとして受け入れ、また、プログラムの次回の主要なレビューにおける最新のビジネスケースの承認に基づいて行われなければならない。プロジェクトのあるフェーズが他のフェーズと並行する場合、プログラムおよびプロジェクトのスポンサーは、プロジェクトの進行を許可する承認手続の時期を定める必要がある。	・組織のビジョンと合致した、プロジェクトの達成目標 ・優先順位をつけたプロジェクト実行 ・プロジェクトのフェーズとプロジェクトの定義との一致 ・プロジェクトの進捗をモニタリングし伝達する能力	・プロジェクトと組織のビジョンとの不一致 ・間違ったプロジェクトの優先順位付け ・プロジェクトの全体計画からの発見されない逸脱 ・不十分なリソース活用

コントロール設計のテスト

- 計画、ポリシー、手続をレビューして、プロジェクト管理フレームワークによって影響を受けるビジネスとITの部門の任命された管理者とエンドユーザが、次のフェーズが始まる前に、システム開発ライフサイクルのプロジェクトの各フェーズ（要件分析、設計、開発、テスト、本番移行など）で作成された成果物を承認し容認されることが可能になっていることを確かめる。
- 承認プロセスが、プロジェクトフェーズの成果物を開始する作業に先立って、あるいは最低限、あるフェーズでの成果物の完成に先立って、主要な利害関係者と合意され、明確に定義された受入れ基準に基づいているかどうかを調査し、それを確かめる。
- 計画、ポリシー、手続をレビューして、フェーズの開始と承認において、そのフェーズでの実際のコスト、時間、進捗を予算された値と比較し、検討されていることを確かめる。
- 計画、ポリシー、手続をレビューして、プロジェクトで期待された便益に対する重要な逸脱が評価され、適切なプログラムガバナンス部門によって承認され、プログラムのビジネスケースに反映されていることを確かめる。
- 計画、ポリシー、手続をレビューして、導入に先立って、システムの品質およびビジネスとシステムを利用、維持するための支援部門の準備を判断することを目的に、事前に決定された主要成功要因に基づいて正式に実施される「進めるか否か」の評価を通じてプロジェクトを本番に移行してよいかどうかが、承認されていることを確かめる。

コントロール目標

PO10.7 統合プロジェクト計画

プロジェクトの開始から終了にいたるまで、その実行とコントロールの指針となる、承認済みの正式な統合プロジェクト計画（ビジネスおよび情報システムの資源についても扱う）を策定する。同一プログラム内の複数のプロジェクトにおけるアクティビティおよび相互依存について理解し、文書化する必要がある。プロジェクト計画は、プロジェクトの存続期間中保守されなければならない。プロジェクト計画および計画に対する変更は、プログラムおよびプロジェクトのガバナンスフレームワークに沿って承認される必要がある。

価値のドライバー

- プロジェクトの時間、予算、対象範囲がマイルストーンに合致している可能性の増加
- 潜在的なプロジェクトの遅延に対する経営者の認識と適時に対応する能力の増加
- プロジェクトの内外で一貫した方法でプロジェクト計画と進捗状況の詳細を共有するためのメカニズム
- 管理され伝達されたプロジェクト進捗

リスクのドライバー

- プロジェクトの計画と予算策定における、発見されないエラー
- 組織の目標や相互依存のある他のプロジェクトとの、プロジェクトの不整合
- プロジェクト計画からの発見されない逸脱

コントロール設計のテスト

- 計画、ポリシー、手続をレビューして、統合されたプロジェクト計画が、プロジェクトの進捗を経営陣がコントロールすることができるための情報を提供しており、その計画が、対象範囲についての記述、プロジェクトの製品と成果物の詳細、必要な資源と責任、明確なWBSと作業パッケージ、必要な資源の見積もり、マイルストーン、主要な依存関係、クリティカルパスの識別を含んでいることを確かめる。
- 統合的なプロジェクト計画とそれに依存するすべての計画が、合意された計画のオーナによって更新され、プロジェクトのマスタープランのチェックポイントからの実際の進捗と構成要素の変化を反映させているかどうかを調査し、それを確かめる。
- 主要な利害関係者へ変更と状況の報告を行う伝達計画がプロジェクト計画に含まれているかどうか調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.8 プロジェクトの資源 プロジェクトチームメンバーの実行責任、リレーションシップ、権限、および成果基準を定義し、有能なスタッフや受託業者の確保およびプロジェクトへのアサインの基本的な考え方を明確化する。プロジェクト目標の達成に向け、各プロジェクトに必要な製品およびサービスの調達について、組織におきえる調達の実践基準に基づき計画および管理する必要がある。	・プロジェクト内で効率的かつ効果的に配分され割り当てられた技能とリソース ・リソースに関するギャップの適時な発見 ・企業の調達ポリシーに沿ったプロジェクトのリソース配分	・プロジェクトでの重要な作業に悪影響を与える、技能とリソースにおけるギャップ ・非効率的なリソースの利用 ・アウトソースしたリソースに関する契約上の係争

コントロール設計のテスト
・資源の必要性がプロジェクトで識別されている。そして、合意され理解されるエスカレーションと意思決定の権限とともに、適切な役割と責任が明確に策定されているかどうかを調査し、それを確かめる。 ・役割が識別され適切な人員を配置しているかどうかを調査し、それを確かめる。 ・着手しようとしているプロジェクトの規模、複雑性、リスクに適した技能を持つ経験豊富なプロジェクト管理要員とチームリーダーが活用されているかどうかを調査し、それを確かめる。 ・計画、ポリシー、手続を閲覧して、他の利害関係者の役割と責任が考慮され明確に定義されていることを確かめる（他の利害関係者というのは内部監査、コンプライアンス、財務、法務、購買、人事を含むがこれに限らない）。 ・サードパーティのプロジェクトとシステムサポートリレーションシップの調達と管理か明確に定義されているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.9 プロジェクトのリスクマネジメント プロジェクトに付随する固有のリスクを排除または極小化するため、不要な変更の原因となり得る領域とイベントに関する計画、特定、分析、対応、モニタリング、およびコントロールの体系化されたプロセスを適用する。プロジェクト管理プロセスおよびプロジェクトの成果物が抱えるリスクを把握し、一元的に記録する必要がある。	・プロジェクトの実現可能性と承認を検討する際の、潜在的な阻害要因の早期の識別 ・リスクの影響を軽減するため、偶発事象や対策を識別し計画することができるマネジメント層 ・明確に識別できるリスクと問題点の責任者 ・モニタリングされたリスク軽減活動 ・組織のリスク管理フレームワークと整合的な、プロジェクト内でのリスク管理のための一貫性があり効率的なアプローチ	・発見されないプロジェクトリスク ・識別されたリスクに対する軽減活動の欠如 ・プロジェクトの発見されない阻害要因

コントロール設計のテスト
・ 正式なプロジェクトリスク管理フレームワークが確立されているかどうかを調査し、それを確かめる。 ・ 計画、ポリシー、手続をレビューして、組織でのプロジェクトリスク管理フレームワークをプロジェクト内で実行する責任が、適切な技能を持つ人に明確に割り当てられていることを確かめる。 ・ 計画、ポリシー、手続をレビューして、この役割が、プロジェクト管理者によって実施されているか、プロジェクト管理者によってプロジェクトチームの他のメンバーに委任されていることを確かめる。 ・ プロジェクトのリスクと問題点を識別するために、プロジェクトのリスク評価を実施しているかどうかを調査し、それを確かめる。 ・ プロジェクトリスクが、プロジェクトでの主要なフェーズに入るときを含め定期的に、そして主要な変更依頼の評価の部分として再評価されているかどうかを調査し、それを確かめる。 ・ 文書を閲覧して、リスクと問題点のオーナが識別され、リスクの回避、受容、軽減のための活動（コンティンジェンシープランなど）がリスクで識別され、是正措置がオーナに割り当てられており、コストへの影響が考慮され、活動が合意されたの期限内に行われていることを確かめる。 ・ プロジェクトリスクのログとプロジェクトの問題点のログが維持管理され定期的にレビューされているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.10 プロジェクトの品質計画 プロジェクトの品質システムおよびその導入方法が記載された、品質管理計画を作成する。この計画は正式にレビューし、関係者全員の合意を得た上で、統合プロジェクト計画に組み込む必要がある。	・ プロジェクト品質計画と企業全体の品質フレームワークとの合致 ・ 導入されたシステムやシステムの変更がビジネスとユーザの要件に合致する度合いの増加 ・ サードパーティを含むプロジェクト全体での、一貫したレベルでの品質保証活動	・ 業務要件及びユーザ要件と、プロジェクトの成果物との不適合 ・ プロジェクト内で期待された品質と提供している品質とのギャップ ・ 非効率的で断片化された、品質保証へのアプローチ ・ 既存のシステムとインフラストラクチャに悪影響を及ぼす、システム導入やシステム変更

コントロール設計のテスト
・ 計画、ポリシー、手続をレビューして、品質計画が明確にオーナシップ/責任、プロセス、測定指標を特定しており、プロジェクト品質システムを構成するプロジェクト成果物に品質保証を与えていることを確かめる。 ・ 計画、ポリシー、手続をレビューして、品質計画が、必要に応じて、ビジネスと技術のソリューションに対して独立した妥当性チェックと検証のための要件の概要を記述していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.11 プロジェクト変更コントロール 各プロジェクトについて、変更コントロールの仕組みを確立する。これにより、プロジェクトのベースラインにかかわるすべての変更(コスト、日程、範囲、品質など)を、プログラムおよびプロジェクトのガバナンスフレームワークに沿って適切にレビューおよび承認し、統合プロジェクト計画に組み込む。	・リソース競合を管理するための明確な優先順位 ・プロジェクトの対象範囲を追跡する能力 ・プロジェクトでの変更の際に、支障なく、効率的になされる意思決定	・プロジェクトの対象範囲、コスト、スケジュールに対するコントロールの欠如 ・ビジネス上の焦点の欠如 ・リソース管理能力の欠如

コントロール設計のテスト

・プロジェクトの変更を管理、評価、正当化、承認するための変更コントロールプロセスが存在するかどうかを調査して、それを確かめる。プロセスの一部としての変更要求が適切かどうかを評価する。
・プロジェクト変更要求のサンプルを閲覧して、それが任命された担当者によって開始され、変更、関連するリスク、期待される便益についての完全な説明を含んでいるかどうかを判断する。
・プログラムとプロジェクトの計画と文書が承認された変更に基づいて更新されているかどうかを調査し、それを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.12 保証方法に関するプロジェクト計画 プロジェクト計画の策定過程において、新規または修正されたシステムを認可する前提として必要とされる保証作業を明確にし、それらを統合プロジェクト計画に含める。この保証作業によって、内部統制およびセキュリティ機能が定められた要件を満たすことが保証されなくてはならない。	・適時かつ費用対効果の高い方法で満たされた、保証（外部監査など）に対する外部要求 ・システムやシステムの変更に対する外部認定の活用 ・プロジェクトがコントロール下におかれ、ビジネスの便益の実現を追求しているという、主要な利害関係者の確信度の増加	・信頼できない保証活動 ・効果的ないし効率的でない保証活動 ・認定と導入の遅延

コントロール設計のテスト

・プロジェクト管理の基準と手順書が、コンプライアンスの要件を検討するステップ（内部統制とセキュリティ要件のテストなど）を含んでいるかどうかを調査し、それを確かめる。
・プロジェクト管理の基準と手順書を閲覧して、それがコンプライアンスの要件を検討するステップを含んでいるかどうかを判断する。コンプライアンスに影響するプロジェクトに対する要求文書を閲覧して、適切なコンプライアンスの利害関係者が関与しており、要求が承認されていることを判断する。
・認定、保証、認証要求を伴うシステムを含むプロジェクトの文書を閲覧して、その事項に関する適切な専門家が要求されているテストと承認結果に関与しているかどうかを判断する。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.13 プロジェクトの成果の測定、報告、およびモニタリング プロジェクトの成果指標(範囲、日程、品質、コスト、リスクなど)に照らして、プロジェクトの成果を測定する。計画からの逸脱を特定する。逸脱によるプロジェクトおよびプログラム全体への影響を評価して、主要な利害関係者にその評価結果を報告する。必要に応じて、プログラムおよびプロジェクトのガバナンスフレームワークに沿った是正措置を提案、実施、およびモニタリングする。	・顧客満足と顧客への焦点の改善 ・すべてのITプロジェクトにおける、IT組織の文化での強い顧客志向 ・迅速に識別される計画からの逸脱 ・良好な結果が伝達され、組み込まれることによる、利害関係者の信頼とコミットメントの促進	・プロジェクトの進捗に関する、有効でない報告と識別されていない問題点 ・プロジェクトの進捗に対するコントロールの欠如 ・顧客の期待とビジネスニーズに対する焦点の喪失

コントロール設計のテスト
・ITプログラム、プロジェクトのガバナンスと管理のフレームワークが、対象範囲、スケジュール、品質、コスト、リスクのレベルを含む、ITでの重要成果測定指標から成っているかどうかを調査し、それを確かめる。 ・プロジェクト計画基準をレビューして、ITプログラム管理チームが、必要に応じて是正措置を提言し、実施し、モニタリングしているかどうかを判断する。プロジェクト計画は、プログラムとプロジェクトのガバナンスフレームワークに沿っているべきである。

コントロール目標	価値のドライバー	リスクのドライバー
PO10.14 プロジェクトの終了 各プロジェクトの終了時に、プロジェクトが計画どおりの成果および便益をもたらしたかどうか、プロジェクトの利害関係者が必ず確認できるようにする。計画されたプロジェクトの成果およびプログラムの便益の達成に必要な事項のうち、未完了のものがあればそれを特定し、周知する。また、プロジェクトの実行により得られた教訓や知識を、将来のプロジェクトおよびプログラムにおいて活用できるよう、特定して文書化する。	・プロジェクトが期待され合意されたビジネス便益を実現する可能性の増加 ・将来のプロジェクトのために、プロジェクト管理とシステム開発で識別された改善点 ・約束された便益の提供のため、残っている活動を実行することへの、より強い集中	・プロジェクト管理の発見されない欠陥 ・過去からの教訓から学習する機会の逸失

コントロール設計のテスト
・ITのポリシーと手続が、効果的な導入後のレビューを含む、プロジェクト終了のための主要なステップを含んでいるかどうかを調査し、それを確かめる。 ・導入後のレビューのサンプルの文書を閲覧して、そのレビューが効果的に計画され実行されたかどうかを判断する。 ・プロジェクトプログラムの便益を達成するのに要求される活動のうち完了していないものすべてを識別し、伝達し、追跡するプロセスに対してウォークスルーを実施する。導入後の文書を閲覧して、未完了の活動が識別され、伝達され、解決されたかどうかを判断する。 ・過去からの教訓を収集するプロセスに対してウォークスルーを実施して、そのプロセスが将来のプロジェクトを改善する上で効果的かどうかを判断する。レビューと分析のプロセスに顧客がどの程度関与しているのかを評価する。

コントロール目標の達成をテストするために以下のステップを踏む。

- プログラム管理フレームワークの文書を閲覧して、プログラムが、ITプロジェクトの集計されたポートフォリオをプログラムの目標に照らして十分に評価されていることを確かめる。プログラムでは、必要な資源を特定すべきである。必要に応じて、資金、プロジェクト管理者、プロジェクトチーム、IT資源、ビジネスの資源を含む。
- 文書を閲覧してプロセスを通じて活動を追跡し、プログラム管理チームも必要な資源を特定していることを確かめる。必要に応じて、資金、プロジェクト管理者、プロジェクトチーム、IT資源とビジネスの資源を含む。
- 文書を閲覧し、プロセスを通じて活動を追跡して、プログラムが割り当てられ、そのような説明責任が容認され、活動するのに十分な権限と裁量、必要な能力、相応の資源、説明責任の明確な線引き、権利と義務に対する理解、関連する成果達成指標の説明責任を持つ人が持っていることを確かめる。
- スケジュールとその他の文書を閲覧して、プログラム管理チームが、プログラム内の複数のプロジェクトの相互依存関係を効果的に発見し、プログラム全体のスケジュールに間に合うように、完了のためのスケジュールを作成したかどうかを判断する。
- 伝達とその他の文書を閲覧して、プログラム管理チームが、企業の内外のプログラムの利害関係者を効果的に決定し、そのような当事者と適切なレベルの協力、伝達、連携を確立し、プログラムの期間中にそのような人々との意思伝達を維持していることを判断する。
- 定期的な評価とその他の文書を閲覧して、プロジェクト管理フレームワークが、組織のプログラム管理アプローチの不可欠の要素として、それと整合的に効果的に用いられており、状況変化において適切であることを確かめる。
- 主要なマイルストーンを閲覧して、次のフェーズへと続く前に、適切な承認が達成されていることを検証する（対象範囲と要件が適切であることを保証するための、スポンサーとエンドユーザからなるレビュー委員会など）。
- 文書を閲覧して、プログラム管理チームがITプロジェクトのそれぞれに対して、戦略的なプログラム全体の中でプロジェクトの実行を管理するのに十分な権限を持つ一人または複数のスポンサーを割り当てており、その任命が明確に行われており、役割と責任が明確になっており、任命された人によってその責任が容認されていることを確かめる。
- 議事録や承認の文書といった文書を閲覧して、プロジェクト管理チームが、プロジェクトの開始、定義、承認の際に、影響を受けるユーザ部門のマネジメント層と主要なユーザを含む、主要な利害関係者によるコミットメントと参加を提供していることを確かめる。
- 議事録や承認の文書といった文書を閲覧し、プロセスを通じて活動を追跡し、プロジェクトのライフサイクルの残りの期間に対しての主要な利害関係者の継続的なコミットメントと参加が、プロジェクトの開始時に効果的に概説されており、効果的な改善プロセスがその後のプロセスで用いられていることを確かめる。
- プロジェクト/プログラムの伝達計画がプロジェクトを通じて効果的に維持されていることを確かめる。
- 変更依頼のサンプルを取り、利害関係者が適切な承認をしたことを確かめる。
- 計画、ポリシー、手続を閲覧して、影響を受けるビジネスとIT部門で任命された管理者とエンドユーザが、次のフェーズが始まる前に、システム開発ライフサイクルのプロジェクトの各フェーズ（要件分析、設計、開発、テスト、本番移行など）で作成された成果物を承認し受け入れ可能なようにプロジェクト管理フレームワークが効果的に設計されていることを確かめる。
- 文書を閲覧して、承認プロセスの基準が、プロジェクトフェーズの成果物を開始する作業に先立って、あるいは最低限、あるフェーズでの成果物の完成に先立って、主要な利害関係者と合意した受入れ基準を明確に定義していることを確かめる。
- 計画、ポリシー、手続を閲覧して、フェーズの開始と承認が、実際のコスト、時間、進捗の管理を考慮し、プロジェクトで期待されている便益に対する重要な逸脱を評価するのに効果的に設計されていることを確かめる。
- 計画、ポリシー、手続を閲覧して、適切なプログラムガバナンス機能が、重要な差異の評価を承認するのに効果的に設計されており、重要な差異がプログラムのビジネスケースに反映されていることを確かめる。
- 実際に文書を閲覧し、監査証跡を調査し、統合プロジェクト計画によって、マネジメント層がプロジェクト

の進捗をコントロールできるようになっていることを確かめる。
- 文書を閲覧して、統合プロジェクト計画と依存するすべての計画が、合意計画の保持者とともに最新の状態を保っており、実際の進捗とプログラム管理フレームワークから重要な変更を反映していることを評価する。
- プロジェクト管理の組織図やRACIチャートが完全かどうか調査する。
- プロジェクトリスク評価と関連する文書/議事録をレビューして、プロジェクトを通じて、プロジェクトガバナンス体制の中での適切なレベルで、リスク（内的なものも外的なものの）が管理され議論されていることを確かめる。
- リスク管理計画がプロジェクトの全体計画に統合されていることを判断する。
- リスクの評価と再評価、変更依頼の評価、その他の文書を閲覧して、定期的な再評価が効果的であり、プロジェクトでのリスクの変化に対応していることを確かめる。
- リスク管理計画に対して必要な更新がなされていることを確かめる。
- 文書を閲覧し、監査証跡を調査し、プロセスを通じて取引を追跡することによって、プロジェクトリスク管理が、予期せぬリスクへの緊急対応を含め、効果的に実施されていることを確かめる。
- プロジェクトリスクのログ、プロジェクトの問題点のログ、その他の文書を閲覧することによって、プロジェクトリスクのログとプロジェクトの問題点のログとが、是正措置に伴って維持されていることを確かめる。
- 文書を閲覧することによって、プロジェクトの目的と主要なプロジェクト成果物を文書化する対象範囲が含まれており、品質プロセスが定義されていることを確かめる。

コントロールの欠陥による影響を文書化するために以下のステップを踏む。
- 集計されたプロジェクトのポートフォリオが十分かどうかを評価することによって、それがビジネスの目的に十分に合致しているかどうかを判断する。
- 資源に関する衝突が存在するかどうか、プロジェクトの相互依存が理解されていないかどうか、プロジェクトが投資の収益率を確保しているかどうかを評価する。
- 組織が資源を効果的かつ効率的に管理する能力を評価する。
- 組織内での異なるプロジェクト管理アプローチが資源を効果的に活用しているかどうか評価する。
- 組織での報告体制が適切な職務分掌を実現しているかどうかを評価する。
- プロジェクト管理ルーツが、モニタリングと報告で効果的かどうかを評価する。
- 規制要件の遵守を評価することによって、時間、スケジュール、成果への悪影響を回避するのに効果的に資源が活用されているかどうかを判断する。
- プロジェクトスポンサーによる、プロジェクトの対象範囲ついての記述のレビューと承認を評価することによって、目標が明確に定義され、IT関連投資プログラムと合致していることを確かめる。
- 承認された統合プロジェクト計画を複数のプロジェクトの相互依存に関して評価することによって、プロジェクト全体を通じて、プロジェクトの実行とプロジェクトのコントロールが存在することを確かめる。
- プログラムとプロジェクトのガバナンスフレームワークとの調整と承認に対する統合プロジェクト計画への変更を評価することによって、コスト、スケジュール、成果への影響を特定する。
- 主要なプロジェクトフェーズをレビューし承認を与えるための適切な管理組織をプロジェクトで定義したかどうかを評価する。
- 組織の調達活動を評価することによって、調達プロセスが、プロジェクトのコスト、スケジュール、成果を管理するために、有能な人材や請負業者の調達、配属がタイムリーに実施されているかどうかを判断する。
- 品質管理計画を評価することによって、サードパーティを含むプロジェクト全体での品質保証活動の一貫したレベルを決定する。
- 品質管理での考慮事項がタイムリーに導入されたかどうかを評価することによって、プロジェクトのマスタープランにコストが含まれており、コストがプロジェクトのマスタープランと合致していることを確かめる。
- 変更が承認または正当化され、それが、予算、スケジュール、成果へのいかなる悪影響も含め、初期の達成目標と目的に合致しているかどうかを評価する。
- 保証業務がシステムの認定に適切なレベルを提供しているかどうかを評価することによって、内部統制とセキュリティの特性が、定義された要件に合致しているという保証を与える。
- プロジェクトの進捗をモニタリングするのに効果的な報告メカニズムが存在するかどうかを評価する。

- マネジメント層がプロジェクトリスクを効果的かつ効率的に管理する能力を決定する。
- タイプや対象範囲が同様の将来のプロジェクトをサポートするためのフィードバックを目的に、プロジェクト終了を評価することによって、コスト、スケジュール、成果への影響を判断する。

付録Ⅲ—調達と導入（AI）

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　技術インフラストラクチャの調達と保守
AI4　運用と利用の促進
AI5　T資源の調達
AI6　変更管理
AI7　ソリューションおよびその変更の導入と認定

付録Ⅲ—調達と導入（AI）

プロセス保証のステップ

AI1 コンピュータ化対応策の明確化

新しいアプリケーションや機能を必要とする場合は、実際の調達または構築の前に、それらがビジネス要件を効果的かつ効率的なアプローチで確実に満たすものであるか分析する必要がある。この分析のプロセスには、ニーズの定義、代替となる調達元の検討、技術的および経済的実現性の見直し、リスク分析および費用対効果分析、アプリケーションを「開発」するか「購入」するかの最終決定が含まれる。これらすべての手続を踏むことにより、ソリューションの実施および導入費用が最小限に抑えられ、ビジネス目標の達成を確実に支援できるようになる。

コントロール目標	価値のドライバー	リスクのドライバー
AI1.1 ビジネスの機能的および技術的要件の定義と保守 IT関連の投資プログラムで期待される成果を得るために必要な、すべての案件についてのビジネスの機能的および技術的な要件を特定し、優先順位を決定して、承認する。	・ 潜在的なソリューションの検討にあたっての、すべての重要な機能的、技術的要件の検討 ・ 開発や調達にあたって利用可能な、完全かつ正確な機能的、技術的要件 ・ 効果的かつ効率的に定義された機能的、技術的要件 ・ 選択されたソリューションのより迅速かつ少ない手戻りでの導入	・ 要件を十分に理解できていないことによる誤ったソリューションの選択 ・ 重要な要件の事後の発見および、それによる手戻りの費用と導入の遅れ

コントロール設計のテスト
・ 主要な担当者へのインタビューを通じて、ビジネスの機能的および技術的な要件が定義され、保守プロセスについての合意がなされていることを確かめる。要件と保守プロセスの文書を閲覧し、設計が調達の規模、複雑さ、目的、リスクに見合っており関連するオーナ/スポンサーに承認されていることを確かめる。 ・ 主要な担当者へのインタビューを通じて、すべての要件と受入基準が検討され、捕捉され、優先順位をつけられ、利害関係者とスポンサーに理解可能な形で記録されていることを確かめる。 ・ 主要な担当者へのインタビューを通じて、アプリケーションとインフラストラクチャの技術的な要件が、組織の情報アーキテクチャの基準と戦略的な技術指針の必要性に合致していることを確かめる。 ・ 計画、ポリシー、および手続をレビューして、情報アーキテクチャの基準と戦略的な技術指針からの例外/逸脱を特定する。

コントロール目標	価値のドライバー	リスクのドライバー
AI1.2 リスク分析報告 要件策定に向けた組織プロセスの一環として、ビジネスの要件とソリューションの設計に関連するリスクを特定、文書化、分析する。	・調達リスクの早期の特定による、潜在的な影響の低減や回避 ・潜在的なリスクに対する経営者の意識の向上	・特定されていない、潜在的に重要な調達リスク ・リスクを認識できず、適切なコントロールを適用できない経営者 ・危険にさらされたシステムセキュリティ

コントロール設計のテスト

・主要な担当者へのインタビュー、プロジェクトの文書の閲覧等を通じて、自動化ソリューションのリスク分析に対して全体的なアプローチを用いていることを確かめる。
・インタビューを通じて、ビジネス部門とIT部門の両方からの代表者を含む利害関係者が関与していることを確かめる。
・ソリューションの設計の際に適切なリスク低減メカニズムを検討し、組織が直面しているリスクによって正当化できる場合には、着手の時点からそれが組み込まれているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI1.3 実現可能性調査および代替対応策の策定 要件導入の実現性を検討する実現可能性調査を実施する。IT部門によるサポートの下、ビジネス部門の管理者は実現可能性および代替ソリューションを評価し、ビジネススポンサーに提案する必要がある。	・企業にとって最も効果的かつ効率的なソリューションの選択 ・選択したソリューションを導入し運用するために利用可能な資源 ・調達にコミットする際の重要な要件 ・正当な事由に基づいた、選定に関する意思決定	・要件に合致していないソリューション ・期待通りの成果をあげていないソリューション ・既存のインフラストラクチャと統合できていないソリューション

コントロール設計のテスト

・主要な担当者へのインタビューを通じて、実現可能性調査のプロセスが存在し、ビジネスの機能的および技術的要件を満たす（機能が、ビジネスと技術の要件の必要性に合致する）代替対応策に着手することができるようになっているかどうか尋ねる。
・経営者と主要な担当者が利用する資源を確定し、実行か中止かのコントロールのチェックポイントを意識しているかどうかを調査して、それを確認する。
・主要な担当者に問い合わせて、実現可能性調査が、特定された代替手段とシステムの機能の潜在的な費用便益分析を含んでいることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI1.4 要件および実現可能性の決定および承認 あらかじめ規定された主要な段階において、ビジネススポンサーが、ビジネスの機能的および技術的要件と実現可能性調査の報告を承認することが義務付けられたプロセスになっていることを確認する。ソリューションおよび調達方法の選択に関しては、ビジネススポンサーに最終決定権がある。	・ビジネス要件に合致している可能性の高いソリューション ・導入時に業務部門のコミットメントと関与があるソリューション ・ソリューションの性質とそれがビジネスプロセスと組織に及ぼす影響についてよりよく理解している業務部門	・ビジネスの要件に合致していないソリューション ・適切に特定されていない代替的ソリューション ・潜在的なソリューションにおいて十分に考慮されていない、ビジネスプロセスと組織の側面

コントロール設計のテスト

・ビジネススポンサーへのインタビューを通じて、ビジネスの機能と技術の要件および実現可能性調査レポートのための品質レビューを実施しており、ビジネススポンサーが当初の受け入れ基準を認識していることを確かめる。
・プロジェクトの代表サンプルについて、プロジェクトの文書を評価し、ビジネススポンサーがビジネスの機能と技術の要件および実現可能性についての報告を承認していることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・ビジネススポンサーと利害関係者とのやり取りを調査し、主要な要件（ユーザ要件の定義、代替対応策の定式化、商業ソフトウェアパッケージの特定、技術的な利用可能性・経済的な利用可能性・情報アーキテクチャ・リスク分析調査の成果など）が捕捉され検討されているかどうかを確かめる。
・要件の文書を選択したものを閲覧し、プロジェクトの開発、導入、変更の前に、提案されている新規システムや変更システムが、事情に精通しているユーザによって、明確に定義され、レビューされ、書面で承認されているかどうかを決定する。
・アプリケーションとインフラストラクチャの技術要件の文書を選択して閲覧し、その要件が組織の情報アーキテクチャの標準と戦略的な方向性（事業継続性計画、災害復旧計画、セキュリティ、法的要件など）に合致しているかどうかを決定する。
・リスク分析の文書を選択して閲覧し、ビジネスとITのリスクが、ビジネス部門とIT部門の両方によって特定され、検証され、評価され、理解されているかどうか、および、内部統制の測定指標と監査証跡がリスク分析（事業継続性計画、災害復旧計画、セキュリティ、法的要件についてのリスクなど）の一環として特定されているかどうかを決定する。
・リスク分析の文書を選択して閲覧し、リスク分析の文書が、ビジネス部門とIT部門の代表者を含む主要な利害関係者に承認されたかどうかを決定する。
・プロジェクト、監査、またはその他の評価レポートを選択して閲覧し、コンプライアンス、監査、リスク管理、セキュリティの担当者へのインタビューを通じて裏を取って、リスク対応メカニズムの設計の際に、防止的コントロールと発見的コントロールとの間の良好なバランスが検討されているかどうかを決定する。
・実現可能性調査の文書を閲覧して、技術的および経済的な実現可能性が、ビジネスと技術の要件の必要性に合致していることを確かめる。
・実現可能性の研究の文書を選択して閲覧し、その計画が、調達または開発のライフサイクルの各ステージを十分に考慮しており、実行か中止かのコントロールのチェックポイントを含んでいることを確かめる。
・技術的および経済的な実現可能性調査の文書を選択して閲覧し、特定された代替策とシステムの機能のそれぞれについて、特定可能な費用と便益が、適切にサポートされ、技術的および経済的な実現可能性調査での要求事項の一部として含まれていることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・要件がユーザの必要性に合致しない場合の、プロジェクトの時間と費用への影響を評価する。

- システム開発努力が頑健なリスク分析を含んでいないせいで特定されなかったリスク（脅威、潜在的な脆弱性、セキュリティ、内部統制など）を評価する。
- システム開発努力が、ポリシー、法律、規制を遵守していない場合の、プロジェクトの時間と費用への影響を評価する。
- 主要なオーナ/スポンサーが代替対応策を検討せず、それによってより費用の高いソリューションを選んだ場合の追加的な費用を評価する。
- 組織のシステム開発ライフサイクルの方法論における不備を特定する。
- ユーザの要件に合致しないソリューションを特定する。
- 以下のような場合のシステム開発努力を特定する。
  - 代替策を検討せず、それによってより費用の高いソリューションを選んだ
  - 時間と費用がもっと少なくて済んだはずの商用ソフトウェアパッケージを検討しなかった
  - 代替策の技術的な実現可能性を検討しなかったか、選択したソリューションの技術的な実現可能性を適切に検討しなかったことにより、ソリューションを当初の設計通りに導入できなかった
  - 経済的な実現可能性調査で誤った仮定を設け、その結果、間違った対応策を取った
  - 情報アーキテクチャ/企業データモデルを検討せず、その結果、間違った対応策を選んだ
  - 頑健なリスク分析を実施しなかったため、リスク（脅威、潜在的な脆弱性と影響を含む）を十分に識別せず、かつ特定されたリスクを減らしたり除去したりするための適切なセキュリティと内部統制も特定しなかった
- 以下のようなソリューションを特定する。
  - 費用対効果の高いコントロールとセキュリティを適切に検証しなかったせいで、コントロールに過不足があった
  - 十分な監査証跡をもっていなかった
  - ユーザフレンドリーな設計と人間工学的な問題点を検討しなかったため、避けることができたはずのデータ入力のエラーが生じた
  - 組織で確立された調達アプローチに従わず、そのため、組織に追加的な費用が課せられた

AI2 アプリケーションソフトウェアの調達と保守

アプリケーションは、ビジネス要件に沿った形で利用可能になる。このプロセスには、アプリケーションの設計、業務処理統制とセキュリティ要件の適切な組み込み、および各種標準に準拠した設計と構成が含まれる。このプロセスにより、組織は自動化された適切なアプリケーションを利用して、ビジネス運営を的確に支援できる。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.1 概要設計 組織の技術的方向性や情報アーキテクチャを考慮の上、ビジネス要件をソフトウェアの調達の概要設計仕様に変換する。この概要設計がビジネス要件に確実に対応していることを踏まえ、設計仕様についてマネジメント層からの承認を得る。開発または保守の際に重大な技術的差異または論理的差異が生じた場合は、評価を再度実施する。	・ 費用の減少 ・ ビジネス要件と概要設計結果との一貫性 ・ 納期の改善	・ 主要な個人のもつ知識への依存 ・ 開発における不明確な対象範囲 ・ ビジネスの要件を提供していないソリューション ・ IT戦略計画、情報アーキテクチャおよび技術指針と整合的でないソリューション ・ 断片的なソリューションのための高い費用

コントロール設計のテスト

- 主要なIT担当者に、ソフトウェア開発のビジネス要件を変換する概要設計仕様が定義されていることを確かめる。
- プロジェクト設計仕様のサンプルを入手してレビューし、それがすべてのビジネス要件を扱っているかどうかを決定する。
- 主要なIT担当者に、プロジェクト設計のアプローチが組織の設計基準に従っているかどうかを確かめる。
- 概要設計の文書をレビューして、組織の設計基準に従っているかどうかを決定する。
- プロジェクト計画と対象範囲の文書といったようなプロジェクトの文書をレビューして、設計プロセスにおけるユーザの役割と責任が適切に含まれているかどうかを決定する。
- ユーザ/利害関係者とのユーザの関与についてマネジメント層の考え方の裏づけを取って、新規システムの設計プロセスで、ユーザ/利害関係者の専門性と知識が考慮されていることを確かめる。
- 題名と日付も含めて、明確な相互参照の助けとなる文書をレビューする。
- 利害関係者（IT部門とビジネス部門）に、概要設計を承認し、自らのインプットが設計（プロセスオーナ、情報オーナ、セキュリティ、ユーザ代表者など）に取り込まれたことを確かめる。
- 利害関係者（IT部門とビジネス部門）に、概要設計が、組織が提供、運用、保守できるようなソリューション（ITスポンサー、ビジネススポンサーなど）を構成していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.2 詳細設計 詳細設計およびソフトウェアアプリケーションの技術的要件を作成する。このとき、要件の受け入れ基準も定義する。この要件が、概要設計に確実に対応していることを踏まえ、要件への承認を得る。開発または保守の際に重大な技術的差異または論理的差異が生じた場合は、評価を再度実施する。	・費用の減少 ・効率的なアプリケーションコーディングと保守 ・重要な特性に対する優先順位付け ・データの冗長性の回避 ・使いやすさの要件に合致したアプリケーション	・不正なトランザクションの処理 ・システムの再設計による費用の増加 ・アプリケーションシステムにおいて誤って処理されたデータ

コントロール設計のテスト

- コードのウォークスルーを実施しデータの入出力に関連する文書を調査して、格納、配置、検索のための適切な方法がデータディクショナリの標準にしたがって実装されているかどうかを決定する。
- 情報アーキテクチャとデータディクショナリの文書を調査して、プログラム設計におけるデータディクショナリ標準からの逸脱を特定する。
- データディクショナリの標準を用いているかどうかを主要な担当者に尋ね、データの入出力の実際の成果を主要な担当者からの回答と比較する。
- 主要な担当者に、ソースデータ収集の設計が、計算され格納されたデータを取り込む仕様になっていることを確かめる。
- コードのウォークスルーを実施して計画を閲覧して、トランザクションの処理のためにデータが収集され検証されていることを確かめる。
- 主要なIT担当者に、十分な冗長性、障害回復、およびバックアップ手順が定義され詳細設計仕様に含まれていることを確かめる。
- バックアップの計画と手順をレビューして、新規システムの要件に十分に対処できており、費用対効果が高いことを決定する。
- 主要なIT担当者に尋ね、関連するプロジェクト文書をレビューして、データの格納、配置、検索のためのファイルの要件が詳細設計仕様で定義されているかどうかを決定する。
- プロジェクトの文書をレビューして、可用性、コントロールと監査可能性、セキュリティ、ネットワークの要件といったようなベストプラクティスが検討されているかどうかを決定する。
- 主要な担当者に尋ね、関連するプロジェクト文書を閲覧して、トランザクションタイプを含む処理ステップ、ロジック変換や特定の計算を含む処理ルールが定義され詳細設計仕様に含まれているかどうかを決定する。
- 主要な担当者に尋ね、関連するプロジェクト文書を閲覧して、システムの統合（既存のものまたは計画されているサブシステムおよび調達されたパッケージソフトウェア）とインフラストラクチャが、プロセスのライフサイクルを通じて継続的に対処されているかどうかを決定する。
- 主要なIT担当者に、特定されたすべての出力データ要件が適切に定義されていることを確かめる。
- 詳細設計の文書をレビューして、異なるタイプの受け手、利用法、要求の詳細、開発の頻度と方法といった、関連する設計仕様が検討されていることを決定する。
- 詳細設計の要件の文書をレビューして、出力データの可用性、網羅性、インテグリティ、機密性および他のプログラムに及ぼす影響に適切に対処しているかどうかを決定する。
- 主要な担当者に、ユーザとシステムアプリケーションとの間のインターフェースが定義され詳細設計仕様に含まれていることを確かめる。
- 詳細設計仕様を閲覧して、それがユーザインターフェースの要件に十分に対処していることを確かめる。
- 重要な技術的ないし論理的な不一致の結果としての設計変更に対処する、システム設計再評価手続について調査する。
- システム設計分析レポートやシステム設計変更要求といった文書をレビューして、システム設計再評価手続に従っていることを確かめる（システムの設計変更はビジネス部門とIT部門のスポンサーによって承認される必要がある）。
- 詳細設計仕様の文書をレビューして、それが組織や業界で受け入れられた仕様の基準および情報アーキテクチャにしたがって作成されたかどうかを決定する。
- IT部門とビジネス部門の利害関係者に、開発を開始する前に設計のウォークスルーが実施されることを確かめる。
- 詳細設計仕様をレビューして、設計のウォークスルーをすべての利害関係者のために実施して、開発の前に利害関係者の承認を得ていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.3業務処理統制および可監査性 ビジネスコントロールが自動化された業務処理統制に適切に反映され、それにより、処理が正確、完全かつタイムリーとなり、承認され監査可能になるように導入する。	・一貫したアプリケーションコントロールの確立 ・保証されたデータインテグリティ ・必要に応じて検証し再構築できるトランザクションデータ履歴	・費用のかかる補完的なコントロール ・データのインテグリティの問題 ・アプリケーションコントロールと実際の脅威、リスクとの間のギャップ ・処理結果とデータリポジトリのコンプライアンスの要件との不適合

コントロール設計のテスト

・コントロールの設計のための要件の文書をレビューして、自動化されたアプリケーションコントロールが、業務処理統制の要件に基づいて定義されていることを決定する。
・コントロールの設計のための要件の文書をレビューして、承認、入力、処理、出力、および境界のコントロールが不十分であるような事例を特定する。
・パッケージ化されたアプリケーションソフトウェアに自動化コントロール機能を実装するための計画をレビューして、業務処理統制の要件に十分に対処していることを決定する。
・ビジネスプロセスオーナとIT技術設計の権限保持者に、開発あるいは購入したアプリケーションにおけるすべての自動化アプリケーションコントロールのための設計仕様が承認されていることを確かめる。
・開発または購入/パッケージ化されたアプリケーションにおけるすべての自動化アプリケーションコントロールのための設計仕様をレビューして、それが承認されていることを確かめる。
・プロジェクト担当者に、セキュリティ、データのインテグリティ、監査証跡、アクセスコントロール、およびデータベースインテグリティコントロールといった全般統制目標をサポートする、自動化コントロールがアプリケーションの中で定義されていることを確かめる。
・開発されたソフトウェアと調達されたパッケージソフトウェアでのアプリケーションコントロールのウォークスルーを実施し、トランザクションを追跡し、文書をレビューして、全般統制目標（セキュリティ、データのインテグリティ、監査証跡、アクセスコントロール、データベースインテグリティコントロールなど）に十分に対処していることを確かめる。
・プロジェクトの文書をレビューして、設計仕様が、内部監査、コントロール、リスク管理の基準と目標に照らし合わせて評価されたことを確かめる。
・プロジェクトの文書をレビューして、アプリケーションソフトウェアの領域の外にある補完的なコントロールの効果が検討されたかどうかを決定する。
・概要レビューの証拠をレビューして、自動化アプリケーションコントロールと全般統制の目標（可用性、セキュリティ、正確性、網羅性、適時性、承認、可監査性など）に合致していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.4 アプリケーションのセキュリティおよび可用性 アプリケーションのセキュリティおよび可用性は、識別されたリスクに応じ、組織のデータの分類方法、情報アーキテクチャ、情報セキュリティアーキテクチャ、およびリスク許容レベルに対応した要件を目指す。	・必要に応じて確立している、防止的および発見的セキュリティコントロール ・データの機密性、インテグリティ、可用性の保証 ・業務処理のためのシステム可用性の維持	・発見されないセキュリティ違反 ・費用のかかる補完的コントロール ・考慮されているセキュリティコントロールと実際の脅威、リスクとの間のギャップ

コントロール設計のテスト
・主要な担当者に尋ねて、インフラストラクチャにおけるセキュリティと可用性のためのソリューションがアプリケーションにどのように統合されているかについての知識と意識を評価する。 ・アプリケーションの調達、導入、およびテスト計画をレビューして、統合された環境の中にあるアプリケーションのセキュリティと可用性に対処していることを確かめる。 ・可用性の設計が技術的な権限保持者に承認されたかどうかを調査して、それを確認する。 ・適切な利害関係者による文書の承認を閲覧する。 ・ビジネススポンサーにインタビューし、ウォークスルーの文書をレビューして、可用性の設計の理解と妥当性を評価し、その設計がセキュリティと可用性の要件に合致している可能性が高いかどうかを調査する。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.5 調達したアプリケーションソフトウェアの構成および導入 調達したアプリケーションソフトウェアを事業目標に合わせて構成、導入する。	・ビジネスで定義された要件に合致するように構成された調達システム ・既存のアーキテクチャに準拠した調達システム	・ビジネス上の焦点の喪失 ・将来の更新を効果的に適用する能力の欠如 ・システムの可用性と情報のインテグリティの低下

コントロール設計のテスト

- ビジネスプロセスオーナと主要な担当者に尋ねて、彼らのインプットとガイダンスが求められ、アプリケーションのカスタマイズと構成に反映されているかどうかを決定する。ビジネスプロセスオーナのインプットを求められなかったような事例を特定する。
- 主要な担当者に、ベンダの助言するようなベストプラクティスを活用し、内部のアーキテクチャの標準に従って、アプリケーションソフトウェアがカスタマイズされ構成されているかどうかを確かめる。
- ベンダが提供したベストプラクティスを閲覧し、導入戦略と比較し、不適切な構成とカスタマイズを特定する。
- 主要な担当者に、調達されたアプリケーションのコントロール目標（機能性、既存のアプリケーションとインフラストラクチャとの相互運用性、システムパフォーマンスの効率性、統合、キャパシティ、付加テスト、データのインテグリティなど）が検証できるようなテスト手続が、実施されていることを確かめる。
- 単体テストと結合テストの文書を閲覧し、テスト手続のウォークスルーを実施し、テストの十分性を確かめる。
- 主要な担当者に、すべてのユーザマニュアルとオペレーションマニュアルが完全で必要に応じて更新されていることを確かめる。ユーザマニュアルとオペレーションマニュアルに対するカスタマイズのサンプルを追跡し、文書の更新を確かめる。

コントロール目標

AI2.6 既存システムの大幅なアップグレード

現行の設計や機能に多大な影響を及ぼす大幅な変更を既存システムに加える場合、新規システムの開発の場合と同様の開発プロセスに従う。

価値のドライバー

- 一貫したシステム可用性
- 処理データの機密性、インテグリティ、可用性の維持
- 開発のための費用と品質のコントロール
- 技術インフラストラクチャとの整合性の維持

リスクのドライバー

- システム可用性の低減
- 処理データの機密性、インテグリティ、可用性の毀損
- 主要な開発のための費用のコントロールの欠如

コントロール設計のテスト

- 主要な担当者に確認し、関連する文書を閲覧して、特定の客観基準（ビジネス要件など）、それに伴うリスク（既存のシステムとプロセスまたはセキュリティへの影響など）、費用と便益の裏づけ、その他の要件に対処するように、主要な更新の影響度評価が行われたことを決定する。
- 関連する文書を閲覧して、通常の開発および導入のプロセスからの逸脱を特定する。
- ビジネススポンサーと他に影響を受ける利害関係者に尋ね、関連する文書を閲覧して、開発と導入のプロセスのための同意と承認を得たかどうかを決定する。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.7 アプリケーションソフトウェアの開発 システムの機能が、確実に設計仕様、開発標準と文書化標準、QA要件、および承認された標準に従って開発されるようにする。サードパーティが開発したアプリケーションソフトウェアに関して、法律上および契約上のすべての側面が、確実に識別され、対応されるようにする。	・業務、顧客、ユーザの必要性に合致していることの確保 ・資源を管理し優先順位をつける能力 ・業務のための能力を創出するアプリケーションソフトウェア ・使いやすさの要件に合致したアプリケーション	・資源の浪費 ・ビジネス要件に関する焦点の喪失 ・多数の失敗 ・アプリケーションを効果的に保守する能力の欠如

コントロール設計のテスト

・主要な担当者に、すべての開発活動が確立され開発標準が確実に遵守されていること、開発したソフトウェアが、ビジネス、機能、技術の要件に合致した同意済みの仕様に基づいていることを確かめる。
・関連する文書（設計、コードレビュー、ウォークスルーなど）を閲覧して、仕様と標準の例外を特定する。
・開発されたソフトウェアの評価の文書を入手しレビューして、その妥当性を確認する。
・主要な担当者に、技術的な権限とオペレーション管理のアプリケーションの本番環境への移行の準備ができており、適合していることを確かめる。
・コードのウォークスルーを実施し、問題/例外を特定する。
・主要な担当者に尋ねて、すべての義務と要件を遵守しているかどうかを決定する。
・サードパーティの開発業者に関連する契約上の義務とライセンスの要件をレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
AI2.8 ソフトウェアの品質保証 要件定義および組織の品質に関するポリシーと手続で規定された品質を確保するために、ソフトウェアQA計画を策定、提供し、実施する。	・包括的なテストアプローチ ・ビジネスのプロセスと要件を反映して実施されたテスト ・正式に受け入れられたソフトウェア	・貧弱なソフトウェア品質 ・開発したソフトウェアのテストのやり直し ・現在のビジネスプロセスを反映していないテスト ・誤って用いられ、企業のセキュリティを損なうテストデータ ・不十分なテスト ・コンプライアンス要件違反

コントロール設計のテスト

- 主要な担当者に、品質基準の仕様、妥当性チェックと検証のプロセス、どのようにして品質をレビューするかの定義を含む、ソフトウェアQA計画が定義されていることを確かめる。
- 上記で挙げた基準のための計画をレビューし、QAレビューが開発チームから独立して実施されていることを確かめる。
- 主要な担当者に、ソフトウェアの品質をモニタリングするためのプロセスが設計され確立していることを確かめる。
- 関連する文書をレビューして、プロセスがプロジェクト要件、企業のポリシー、品質管理手続、および受け入れ基準に基づいていることを確かめる。
- 主要な担当者に、品質に関するすべての例外が特定され、是正措置を取ったことを確かめる。
- QAレビュー、レビュー結果、例外、是正に関する文書を閲覧して、QAレビューが必要に応じて繰り返し行われていることを決定する。

コントロール目標

AI2.9 アプリケーション要件の管理

設計、開発、導入の際に、個々の要件（否認されたすべての要件を含む）の状況を追跡し、要件への変更を、確立された変更管理プロセスを経て承認する。

価値のドライバー

- 正式に定義された要件とビジネスに関する明確な期待
- 確立した変更管理手続の遵守
- アプリケーションへの変更を効果的な方法で実施するための合意済みの標準化されたアプローチ

リスクのドライバー

- 承認されていない変更
- 目的のシステムに適用されない変更
- 期待と要件との間のギャップ

コントロール設計のテスト

- 個々の要件への変更が確実にモニタリングされ、レビューされ、関連する利害関係者に承認されていることを確かめる。
- 関連する文書を閲覧して、すべての変更と変更の状況が変更管理システムに記録されていることを確かめる。
- 追跡されていない変更を特定して報告する。

コントロール目標

AI2.10 アプリケーションソフトウェアの保守

ソフトウェアアプリケーションの保守およびリリースに関する戦略と計画を策定する。

価値のドライバー

- 確立した変更管理手続の遵守
- アプリケーションへの変更を効果的な方法で実施するための合意済みの標準化されたアプローチ

リスクのドライバー

- 承認されていない変更
- 目的のシステムに適用されない変更
- 期待と要件との間のギャップ
- システム可用性の減少

コントロール設計のテスト

- 主要な担当者へのインタビューを通じて、すべての変更に対して均一に適用することができるようなアプリケーションソフトウェア保守活動のための効果的かつ効率的なプロセスが設計されており、迅速かつ効果的に実施することができることを確かめる。
- プロセスの文書を閲覧して、関連する問題点が含まれていることを決定する（これには、リリースの計画とコントロール、資源計画、バグ修復と障害の修正、軽微な改良、文書の維持管理、緊急変更、他のアプリケーションとインフラストラクチャとの相互依存、アップグレード戦略、サポートの問題やアップグレードといったような契約条件、ビジネスの必要性に対する定期的なレビュー、リスク、セキュリティ要件が含まれる）。
- 主要な担当者に、すべての保守変更が、既存のアプリケーションとインフラストラクチャへの影響を含む、正式な変更管理プロセスを遵守していることを確かめる。
- 関連する文書を閲覧して、正式な再開発として対処した方がよいようなものを特定するために、変更に優先順位をつけていることを確かめる。正式な変更管理プロセスからのいかなる逸脱も特定する。
- 正式な変更管理プロセスに従わずに適用された変更がレビューされ承認されているかどうかを、主要な担当者に尋ねて確認する。
- 関連する文書を閲覧して、レビューと承認をされていない変更を特定する。
- 保守活動のパターンと分量が正常でない傾向を示しているか定期的に評価しているかどうかを、主要な担当者に尋ねて確認する。
- 関連する分析結果の文書を閲覧して、品質または成果に関するすべての潜在的問題が適切に分析され報告されていることを確かめる。
- 主要な担当者に、すべての保守活動が完全かつ成功裡に完了したことを確かめる。
- 保守活動のウォークスルーを実施して、ユーザ、システム、オペレーションに関する文書と相互依存性の更新を含む、すべての作業とフェーズに対処したことを確かめる。
- 契約条件の変更、ビジネスの傾向、その他のアップグレードでまだ対処していないものをすべて特定する。

コントロール目標の達成を検証するために以下のステップを踏む。

- プロジェクト設計の文書をレビューして、その設計が、ビジネスプラン、戦略、該当する規制、およびIT計画と整合的であることを確かめる。
- プロジェクトの承認の文書のサンプルを入手してレビューし、そのプロジェクトがQA上の承認を経ているかどうか、またIT部門とビジネス部門の利害関係者（プロジェクトスポンサー）による概要設計が適切に承認されて進められているかどうかを決定する。
- ITマネジメント層の裏づけを取り、関連する文書をレビューして、サンプルのプロジェクト設計仕様が組織の技術指針と情報アーキテクチャと整合的であるかどうかを決定する。
- 統合の計画と手続をレビューして、それが妥当であるかどうかを決定する。
- プロジェクトの文書をレビューして、既存のアプリケーションとインフラストラクチャへの新規導入の影響が評価され、適切な統合アプローチを実施したかどうかを決定する。
- 最終段階の文書をレビューして、すべての開発活動がモニタリングされ、変更要求と品質成果と設計のレビューが追跡され、最終的に行われた正式な議論で検討されたことを確かめる。また、すべてを代表する利害関係者が集まり、最終的なレビューが承認基準を取り込んでいることも確かめる。問題のログを閲覧し、文書と承認をレビューして、開発活動の妥当性を確かめ、逸脱を特定する。
- 設計の文書をレビューして、セキュリティと可用性に対する適切なソリューションとアプローチが、定義された要件に十分に合致し、既存のインフラストラクチャの能力に基づいて構築され、またはそれを拡張するよう設計されていることを確かめる。
- QAの文書と障害のログをレビューして、品質上の重要な例外がすべて特定され是正措置が取られていることを確かめる。QAレビュー、レビュー結果、例外、是正に関する文書を閲覧して、QAレビューが必要に応じて繰り返し行われていることを決定する。

- 変更要求を入手して閲覧して、それが分類され優先順位をつけられていることを決定する。主要な担当者に、すべての変更要求の影響が評価されていることを確かめる。
- 変更コントロールの文書をレビューして、正式な変更管理プロセスに従わずに適用された変更がレビューされ承認されていることを確かめ、レビューされ承認されていない変更を特定する。
- リスク分析の文書を閲覧して、ビジネス部門とIT部門の両方によってビジネスとITのリスクが特定され、検証され、評価され、理解され、すべての利害関係者が関与しているという証拠が存在するかどうかを決定する。
- 実現可能性調査をレビューして、技術的な実現可能性と経済的な実現可能性の両方が十分に検討されたことを確かめる。
- 品質レビューの文書をレビューして、当初の受け入れ基準と比較して、当初の受け入れ基準からの例外や逸脱を特定する。
- 最終段階の文書をレビューして、提案されているアプローチや、さらなる実現可能性の分析を要求するようなフィードバックの承認を得たことを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- ユーザ要件を反映していない設計仕様を特定する。
- 組織のデータディクショナリのルールと合致しないデータ管理要求を特定する。
- ファイル、プログラム、ソースデータの選択、入力、ユーザ—マシンインターフェース、処理、出力、コントロール可能性の要件が十分に定義されていない、新規のシステム開発または改変のプロジェクトを特定する。
- セキュリティと可用性が十分に考慮されていないような設計を特定する。
- データのインテグリティの設計の不備を特定する。
- テスト計画の要件の不備を特定する。
- システムの開発や保守の間に発生したが、システム設計の再評価につながらなかったため、それが修正されなかったり、システムに対して、非効率的で効果のない非経済的なパッチを当てることになったりしたような、技術的ないし論理的な重要な不一致を特定する。

AI3 技術インフラストラクチャの調達と保守

組織は、技術インフラストラクチャの調達、導入、およびアップグレードに関するプロセスを策定する必要がある。これを実現するには、合意された技術戦略に基づいてインフラストラクチャを調達、保守、および保護するためのアプローチを計画し、開発環境とテスト環境を用意する必要がある。この結果、ビジネスアプリケーションに対する継続的な技術的サポートが確保される。

コントロール目標	価値のドライバー	リスクのドライバー
AI3.1 技術インフラストラクチャの調達計画 確立された機能面および技術面でのビジネス要件を満たし、組織の技術的方向性と一致する技術インフラストラクチャの調達、導入、および保守の計画を策定する。	・一貫した技術計画 ・システムセキュリティの向上 ・バランスの取れたハードウェアとソフトウェアの活用 ・IT戦略計画、情報アーキテクチャおよび技術指針との整合 ・財務計画の改善	・調達モデルの不在 ・一貫していない技術インフラストラクチャ ・ビジネスの必要性をサポートしていない技術 ・情報セキュリティの危殆化

コントロール設計のテスト
・担当者に、技術インフラストラクチャの調達、導入、およびアップグレードの計画が策定され、それがビジネスの機能的技術的な要件を満たしていることを確かめる。 ・計画をレビューして、その計画が組織で確立された技術指針に従っており、すべての主要な側面が含まれていることを確かめる。 ・組織の技術指針と整合的なインフラストラクチャ調達計画を策定し維持するためのプロセスが定義され導入されているかどうかを調査して、それを確認する。 ・インフラストラクチャ調達計画を閲覧して、要件、リスク、移行といった主要な側面に対処していない領域を特定する。 ・財務的な評価が正確で全体をカバーしているかどうかをレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
AI3.2 インフラストラクチャ資源の保護と可用性 ハードウェアおよびインフラストラクチャソフトウェアの構成、統合、および保守の際に、内部統制、セキュリティ、および可監査性の測定指標を導入することで、資源を保護し、可用性およびインテグリティを確保する。機密性の高いインフラストラクチャコンポーネントの使用上の責任を明確に定義し、インフラストラクチャコンポーネントの開発および統合にあたる担当者に周知する必要がある。これらのコンポーネントの使用状況はすべてモニタリングおよび評価されなければならない。	・一貫した技術計画 ・システムセキュリティの向上 ・バランスの取れたハードウェアとソフトウェアの活用 ・すべてのシステムの局面で維持された、データのインテグリティと機密性	・本番の処理におけるサービスの中断 ・アクセスコントロールにおける発見されない迂回 ・機密性の高いソフトウェアに対する承認されていないアクセス ・技術によってサポートされていないビジネス上のニーズ

コントロール設計のテスト

- 主要な担当者に、インストールないし保守の作業に先立って、インフラストラクチャのすべてのデータとスフとウェアのバックアップを取っていることを確かめる。バックアップログを閲覧して、インフラストラクチャのデータとソフトウェアのバックアップをきちんと取っていることを確かめる。
- 主要な担当者に、インストールに先立った、本番環境と分離されかつ本番環境と十分に類似した環境で、すべてのアプリケーションソフトウェアがテストされていることを確かめる。テストの仕様と手続をレビューして、機能性、セキュリティ、可用性、およびインテグリティの条件と、ベンダによる他の推奨内容がテストに含まれていることを確かめる。
- ソフトウェアの構成を閲覧して、セキュリティとその他のベンダのデフォルトと関連して、デフォルトパスワードと初期のアプリケーションパラメータ設定からの変更を含む、主要な側面に対処していることを確かめる。
- インストールを目的として与えられている一時的なアクセスがモニターされ、インストールが完了してすぐにパスワードが変更されているかどうかを調査して、それを確認する。アプリケーションのセキュリティ設定を閲覧して、コンプライアンスを確認する。
- 主要な担当者に、適切なライセンスを持つソフトウェアのみがテストされインストールされ、ベンダのガイドラインにしたがってインストールが実施されていることを確かめる。ベンダのガイドラインに従っていないインストールを特定し、潜在的な影響に関してベンダが相談を受けていることを確かめる。
- 主要な担当者に、ライブラリ内でのプログラムとデータの移動のために独立したグループ（ライブラリアンなど）にアクセス権を与えていることを確かめる。必要に応じて、ライブラリ管理システムへのユーザのアクセスを調査する。
- すべてのユーザのチェックイン/チェックアウトプログラムとデータへのアクセスをライブラリからその起点となるリクエストフォームまで追跡して、しかるべき上級担当者による承認を確かめる。
- 客観的な受け入れ基準を用いて受け入れ手続きを守らせており、受け入れ基準によって、本番でのパフォーマンスが合意済みの仕様と要件に確実に整合するようにしているかどうかを、担当者に尋ねる。合意済みの仕様ないしSLAの要件をレビューして、受け入れ手続きと比較して、手続に十分に従っていないような領域を特定する。
- 主要な担当者に、重要なインフラストラクチャコンポーネントに対する保守活動へのアクセスが記録され、責任を持つ上級担当者によって定期的にレビューされていることを確かめる。
- 保守ログをレビューして、すべての項目が記録されていることを確かめる。関連する文書（ログレビューマトリックスと定期的なシステムセキュリティレポートなど）をレビューして、ログが定期的にレビューされていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI3.3 インフラストラクチャの保守 インフラストラクチャの保守の戦略および計画を策定し、変更が組織の変更管理手続に従って確実にコントロールされるようにする。保守には、ビジネス上の必要性、パッチ管理およびアップグレード戦略、リスク、脆弱性の評価、およびセキュリティ要件に関する定期的なレビューを組み込む。	・ モニタリングされた保守契約 ・ 効果的な保守プロセス ・ ソフトウェアのリプレースにあたっての運用変更管理	・ 本番の処理におけるサービスの中断 ・ 重要なソフトウェアに対する承認されていないアクセス ・ ビジネスのニーズをサポートしていない技術 ・ ライセンス契約違反

コントロール設計のテスト

- 主要な担当者に、インストールされたシステムソフトウェアプロセスの保守で、必要に応じてアプリケーションの更新と同じプロセスを活用していることを確かめる。計画的なシステムソフトウェアの保守を調査し、アプリケーションの更新のための通常のプロセスからの逸脱ないし、ベンダの手続とガイドラインに対する例外を特定する。
- 主要な担当者に、システム保守のすべての活動について、システムソフトウェアの文書が維持され、最新の状態に保たれ、ベンダの文書とともに更新されていることを確かめる。
- 関連する文書を閲覧して、不完全あるいは最新でない領域を特定する。
- 主要な担当者に尋ねて、ベンダのアップグレードやパッチが利用可能になるたびにタイムリーな通知を得るためのプロセスや方法（特定のベンダ合意、製品のユーザグループに入る、トレードジャーナルを購読するなど）を確かめる。
- システムソフトウェアのサンプルを閲覧して、アップグレードないしパッチがタイムリーに適用されていることを確かめる。
- すべての逸脱ないし例外を特定する。
- 保守を実施する分量、サポートされていないインフラストラクチャの脆弱性、および将来のリスクとセキュリティの脆弱性が定期的にレビューされているかどうかを主要な担当者に尋ねる。
- このようなレビューの評価を実施し、評価で特定されたリスクが主要な担当者によって議論されていないような領域を見つける。
- 保守追跡ログとフィードバックツールを調査して、インフラストラクチャ計画プロセスの中で、このようなレビューの結果が、検討事項としてIT委員会やそれに準じたグループに伝達されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI3.4 実現可能性テスト環境 インフラストラクチャコンポーネントの効果的かつ効率的な実現可能性テストおよび統合テストをサポートする開発環境とテスト環境を構築する。	・ソフトウェアのリプレースを検証するための効果的なサポート ・本番処理に影響する前のエラーと問題点の発見	・ビジネスの中断 ・悪意によるダメージ

コントロール設計のテスト

- 主要な担当者に、戦略的な技術計画に相応のアプローチが設計されており、それによって適切なテストおよびシミュレーションの環境が構築され、それによって計画された調達や開発の実現可能性を検証できるようになっていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

- 調達インフラストラクチャ計画をレビューして、それがレビューされ承認され、リスク、費用、便益、および技術的な適合性が検討されていることを確かめる。計画を閲覧して、IT委員会やそれに準じた組織の承認を確かめる。
- 主要な担当者に、アプリケーションソフトウェアのインストールと保守のプロセスにともなうすべてのセキュリティ要件に対処し、新たに発見されたいかなるリスクも評価され、是正措置が取られたことを確かめる。
- 研修部門と重要なインフラストラクチャコンポーネントを使用している主要な人員に、適切な研修が提供されていることを確かめる。
- 主要な担当者に、インフラストラクチャ保守の指針となるテストの計画と戦略が、変更管理手続に沿って実施されていることを確かめる。計画に関連する文書を閲覧して、インフラストラクチャ保守の要件のすべての側面（変更要求、パッチ、アップグレード、修復など）が含まれていることを確かめる。また、戦略と計画が、組織の技術指針に沿っており、タイムリーにレビューされ、責任を持つマネジメント層によって承認されていることも確かめる。

- システム環境を開発環境とテスト環境に分ける方法が妥当であることを確かめる。
- テスト環境が構築され、機能、ハードウェアとソフトウェアの構成、統合とパフォーマンスのテスト、環境間の移行、バージョンコントロール、テストのためのデータとツール、およびセキュリティを適切に考慮していることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- システム全体のパフォーマンスに影響を及ぼしたパフォーマンス上の問題を特定する。
- システム全体のパフォーマンスに影響を及ぼした予防的保守の問題を特定する。
- システムに格納されているデータとプログラムのセキュリティに悪影響を及したような、システムソフトウェアのセットアップ、インストール、および保守の欠陥を特定する。
- システムに格納されているデータとプログラムのセキュリティに悪影響を及ぼしうるシステムソフトウェアのテストの欠陥を特定する。
- システムに格納されているデータとプログラムのセキュリティに悪影響を及ぼしうるシステムソフトウェアの変更コントロールプロセスの欠陥を特定する。

AI4 運用と利用の促進

新たなシステムに関する知識を利用可能にする必要がある。このプロセスでは、ユーザおよびIT部門のための文書や資料を作成し、アプリケーションとインフラストラクチャの適切な使用と運用を確保するための研修を実施する。

コントロール目標	価値のドライバー	リスクのドライバー
AI4.1 運用上のソリューションの計画 技術、運用能力、および利用状況に関する側面をすべて特定、および文書化するための計画を策定する。これにより、自動化されたソリューションの運用、利用、および保守を担当する人員が自らの実行責任を果たせるようになる。	・一貫性のあるユーザマニュアルとオペレーションマニュアル ・ユーザ研修のサポート ・サービスの品質向上	・期限を過ぎた変更 ・期待と能力との間のギャップ ・異なる提供サービスに対する不適切な優先順位付け ・ギャップに対処するのに不十分な予算と資源

コントロール設計のテスト
・主要な担当者に、新規またはアップグレードされた自動化システムやインフラストラクチャの導入に先立って、運用手続とユーザ文書（オンラインアシスタンスを含む）が定義され文書化されていることを確かめる。 ・関連する文書を閲覧して、新規またはアップグレードされたシステムやインフラストラクチャに関連して、管理、ユーザ、および運用の手続の作成のための実行責任を確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI4.2 ビジネス部門の管理者への知識の移転 ビジネス部門の管理者に知識を移転する。これにより、ビジネス部門の管理者がシステムおよびデータのオーナシップを担い、サービスの提供と品質、内部統制、およびアプリケーション管理に関する責任を果たすことができるようにする。	・組織内での知識の移転 ・関連するすべてのチームでの品質の一貫性 ・ビジネスのための効率的なサポート ・ビジネスプロセスをサポートするユーザマニュアル	・主要な担当者への依存の増加 ・毎日の運用における問題 ・日々直面し繰り返されるインシデント ・ヘルプデスクの過負荷

コントロール設計のテスト

・主要な担当者へのインタビューを通じて、システムのオーナシップと運用を可能にするためのプロセス（アクセス承認、特権管理、職務の分離、自動化ビジネスコントロール、バックアップリカバリ、物理的セキュリティ、ソースドキュメントのアーカイブなど）に対する経営者の意識と知識を確かめる。
・研修と導入の教材をレビューして、定義されたプロセスが要求された内容を含んでいるかどうかを決定する。
・主要な担当者へのインタビューを通じて、マネジメント層が、サポートする文書、手続、および関連する研修が十分かどうかを評価するためのフィードバックメカニズムを認識しそれらを利用することができるということを確かめる。
・ビジネス部門の経営者にインタビューして、システムを効果的に利用する能力を評価する。
・ビジネス部門の経営者とともに主要な機能のウォークスルーを実施して、追加的な研修があった方が有益な領域を特定する。
・研修教材をレビューして、カバーされていなかったり明確でなかったりする領域がないかどうか評価する。

コントロール目標	価値のドライバー	リスクのドライバー
AI4.3 エンドユーザへの知識の移転 エンドユーザに知識とスキルを移転させる。これにより、エンドユーザが効果的かつ効率的にアプリケーションシステムを使用し、ビジネスプロセスをサポートできるようにする。	・利害関係者への知識の移転 ・効率的かつ効果的な研修 ・最適化された運用とシステムの利用	・一貫性を欠くシステム利用 ・不十分な文書化 ・主要な担当者への依存の増加 ・毎日の運用における問題 ・ユーザの要件に合致していない研修 ・ヘルプデスクの過負荷

コントロール設計のテスト

・ユーザがアプリケーションシステムを効果的かつ効率的に使用しビジネスプロセスをサポートできるようなプロセス（研修とスキルの開発、研修教材、ユーザマニュアル、手順書、オンラインヘルプ、サービスデスクサポート、主要なユーザの識別、評価など）についてのユーザグループの意識と知識について、主要な担当者にインタビューする。
・ 研修と導入の教材をレビューして、要求された内容が定義されたプロセスに含まれているかどうかを決定する。
・ 主要な担当者へのインタビューを通じて、ユーザが、サポートする文書、手続、および関連する研修が十分かどうかを評価するためのフィードバックメカニズムを認識しておりそれらを利用することができるということを確かめる。

コントロール目標

AI4.4 運用スタッフおよびサポートスタッフへの知識の移転

運用スタッフおよび技術サポートスタッフに知識とスキルを移転させる。これにより、効果的かつ効率的にシステムと関連インフラストラクチャを提供、サポートおよび保守できるようにする。

価値のドライバー

・ 利害関係者への知識の移転
・ 効率的かつ効果的な研修
・ 最適化された運用とシステムサポート
・ アプリケーション開発のすべての段階で正式に定義されているアプローチ

リスクのドライバー

・ 不十分な文書化
・ 主要な担当者への依存の増加
・ 毎日の運用における問題
・ 運用やサポートの要件に合致していない研修
・ ヘルプデスクの過負荷

コントロール設計のテスト

・ アプリケーションシステムと関連するインフラストラクチャを、サービスレベルにしたがって、効果的かつ効率的に提供、サポート、および保守するためのプロセス（研修とスキルの開発、研修教材、ユーザマニュアル、手順書、オンラインヘルプ、サービスデスクシナリオなど）における運用スタッフおよび技術サポートスタッフの意識と知識について、主要な担当者にインタビューする。
・ 研修と導入の教材をレビューして、要求された内容が定義されたプロセスに含まれているかどうかを決定する。
・ 主要な担当者へのインタビューを通じて、運用担当者および技術サポート担当者が、サポートする文書、手続、および関連する研修が十分かどうかを評価するためのフィードバックメカニズムを認識しておりそれらを利用することができるということを確かめる。
・ 運用担当者およびサポート担当者が、運用およびサポート文書の作成と保守に関与しているかどうかを決定する。
・ 運用サポート手続が既存の運用サポート手続に統合されていないような領域を特定する。

コントロール目標の達成をテストするために以下のステップを踏む。
・ ソリューション提供プロジェクトを選択するために、文書を閲覧して、ユーザと運用手続のマニュアルが存在することを決定する。
・ 経営者の知識を評価して、マネジメント層のメンバーが自らのビジネスのエリアのための管理手続（アクセス承認、特権管理、職務の分離、自動化ビジネスコントロール、バックアップ/リカバリ、物理的セキュリティ、ソースドキュメントのアーカイブなど）を主導して作成したかどうかを決定する。このような手続が、既存の管理手続とコントロール手続に統合されていることを確かめ、マネジメント層が不一致を認識しているかどうかを決定すべく調査する。
・ 新規またはアップグレードされたアプリケーションに対してビジネスのマネジメント層と共にウォークスルーを実施して、追加的な研修が必要な領域を特定する。使用されている研修教材をレビューして評価する。
・ フィードバックの文書を選択して閲覧し、サポートの文書、手続、および関連する研修教材を作成する

ための十分なフィードバックメカニズムが用いられたかどうかを決定する。
- 自らのビジネスエリアにおけるユーザ手続策定へのユーザの関与を評価する（研修とスキルの開発、研修教材、ユーザマニュアル、手順書、オンラインヘルプ、サービスデスクサポート、主要なユーザの識別、評価など）。このような手続が既存のユーザとコントロールの手続（システムのインプット/アウトプット、システム統合、エラーメッセージなど）に統合されていることを確かめて、ユーザが不一致を認識しているかどうかを決定すべく調査する。
- 新規またはアップグレードされたアプリケーションとインフラストラクチャのウォークスルーを、オペレーションのマネジメント層と技術サポートスタッフとともに実施して、追加的な研修があった方が有益な分野を特定する。研修教材が十分かどうか、レビューして評価する。
- 運用と技術のサポートスタッフの手続の策定における、運用と技術のサポートスタッフの自らの領域への関与を評価する（研修とスキルの開発、研修教材、ユーザマニュアル、手順書、オンラインヘルプ、サービスデスクシナリオなど）。このような手続（バックアップ、リスタート/リストア、レポート/出力の配布、緊急修理、オペレータのコマンド/パラメータ、問題のエスカレーションなど）が、既存の運用と技術のサポートスタッフメンバーの手続に統合されていることを確かめる。運用と技術のサポートスタッフメンバーが不一致を認識しているかどうかを決定すべく調査する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 研修やユーザ手続や運用手続が不十分なことによる、費用と運用の非効率性を評価する。
- ユーザマニュアル、運用マニュアル、および研修マニュアルの不備を特定する。

AI5 IT資源の調達

要員、ハードウェア、ソフトウェア、サービスを含むIT資源を調達する必要がある。そのためには、調達手続の策定と実施、ベンダーの選定、契約等の整備、および調達が必要である。これらを行うことにより、組織はタイムリーかつ費用効率よく、必要なIT資源をすべて確保可能になる。

コントロール目標	価値のドライバー	リスクのドライバー
AI5.1 調達のコントロール IT関連のインフラストラクチャ、設備、ハードウェア、ソフトウェア、およびサービスの調達が、ビジネス要件を確実に満たすよう、全組織の調達プロセスや調達戦略と整合性のとれた一連の手続および標準を整備し、それを遵守する。	・供給業者との最適化された関係 ・ビジネスとITのプロセスへの質の高い貢献 ・ビジネスとITで望まれる達成目標の実現をサポートする調達	・供給業者が要求を満たす際のギャップ ・商業的および契約上の調達の障害 ・組織の短期および長期の計画に沿っていない自動化ソリューション ・調達したソリューションでの不十分なソフトウェア品質 ・費用のコントロールの欠如

コントロール設計のテスト
・主要な担当者へのインタビューを通じて、IT調達プロセスと調達戦略が調達に関する組織のポリシーと手続と整合的であることを確かめる（法規制の用件、組織のIT調達戦略の遵守、ライセンスとリースの要件、技術アップグレードの条項、ビジネス部門の関与、総所有コスト（TOC）、主要な調達における調達計画、資産の記録など）。 ・プロジェクト管理のポリシーと手続を閲覧して、企業全体の調達のポリシーと手続を遵守しているかどうか評価する。

コントロール目標	価値のドライバー	リスクのドライバー
AI5.2 供給業者との契約の管理 すべての供給業者に対する、契約の締結、変更、終了の手続を策定する。この手続では、少なくとも、法律、財務、組織、文書、成果、セキュリティ、知的財産、および契約の終了に関する責任と義務（罰則条項を含む）について扱う必要がある。すべての契約および契約変更について、法律の専門家のレビューを受ける必要がある。	・供給業者との関係について定義された目標と達成目標 ・効率的に管理された資源調達 ・ビジネスとITのプロセスへの質の高い貢献	・費用管理の欠如 ・業務部門の期待と供給業者の能力との間のギャップ ・定義されていないサービス費用の発生 ・ビジネスの要件を反映していないサービス ・運用サポートの欠如

コントロール設計のテスト
・主要な担当者へのインタビューを通じて、供給業者との契約を締結するためのポリシーと標準があることを確かめる。供給業者とクライアントとの間の関係、供給業者のSLA、SLAと照らし合わせたモニタリングと報告、移行の合意、通知とエスカレーションの手続、セキュリティ標準、記録管理とコントロールの要件、および供給業者に要求されるQA活動に対して、ポリシーと標準で対処すべきである。契約には、法律、財務、組織、文書、成果、セキュリティ、可監査性、知的所有権、実行責任と法的責任の側面についても含めるべきである。

コントロール目標	価値のドライバー	リスクのドライバー
AI5.3 供給業者の選定 存続性のある最適な供給業者を公正かつ正式な実施基準に従って選定する。要件は、供給業者の候補からの情報を基に最適化する。	・新しいアイディアと活動への貢献 ・供給業者のSLAを越えた組織の目標への継続的な貢献	・供給業者の不適切な選定 ・組織の目標の達成には不十分なサポート ・供給業者の要件と能力との間のギャップ

コントロール設計のテスト

・主要な担当者へのインタビューを通じて、供給業者と調達の選定のために、事前に定義され具体的で確立した判断基準（要件定義、タイムテーブル、意思決定プロセスなど）を用いていることを確かめる。
・情報提供要求（RFI）と提案要求（RFP）を閲覧して、確立した判断基準が定義されているかどうかを決定する。
・ソフトウェア調達に、すべての当事者の権利と義務（知的財産の所有権ライセンス、保守の保障、裁定手続、アップグレードの条項、およびセキュリティ、エスクロー、アクセス権を含む目的との適合性など）が含まれており、それを守らせているかどうかを調査して確認する。ソフトウェア調達の選出に際し、関連する文書を閲覧して、契約条項にすべての当事者の権利と義務が含まれているかどうかを決定する。
・開発資源の調達にすべての当事者の権利と義務が含まれており、それを守らせているかどうかを調査して確認する（たとえば、知的財産の所有権とライセンス、開発の方法論を含む目的への適合性、言語、テスト、パフォーマンスの判断基準を含む品質管理手続、パフォーマンスレビュー、支払い方式、保障、裁定手続、人事管理、および組織のポリシーの遵守などを確かめる）。
・開発資源の調達における知的財産の所有権とライセンスについての合意事項に関して、法的助言を受けたかどうかを決定する。
・開発資源の調達の選出に際し、関連する文書を閲覧して、契約条項にすべての当事者の権利と義務が含まれているかどうかを決定する。
・インフラストラクチャ、設備、関連するサービスの調達に、すべての当事者の権利と義務（サービスレベル、保守手続、アクセスコントロール、セキュリティ、パフォーマンスレビュー、支払い方式、裁定手続など）が含まれており、それを守らせているかどうかを調査して確認する。
・インフラストラクチャ、施設、および関連するサービスの調達の選定に際し、関連する文書を閲覧して、契約条項にすべての当事者の権利と義務が含まれているかどうかを決定する。
・RFIとRFPが承認された手続と判断基準にしたがって評価されているかどうかを調査して、それを確認する。
・文書による証拠が効果的に維持されているかどうかを決定する。

コントロール目標	価値のドライバー	リスクのドライバー
AI5.4 IT資源の調達 ソフトウェアの調達、開発資源、インフラストラクチャ、およびサービスの調達にかかわる契約条項に、すべての当事者の権利と義務を含め、あらゆる調達契約の合意事項で組織の利益を保護し、徹底管理する。	・効果的かつ効率的なインシデント管理 ・意図した通りで中断しにくいシステム運用 ・インシデントのタイムリーな解決	・必要なときに利用できないソフトウェア更新 ・ビジネスプロセスをサポートできないソフトウェア ・意図した通りに適用できないアプリケーションへの変更 ・問題やインシデントを起こしやすく、ビジネスの中断を起こしやすいシステム

コントロール設計のテスト

- 調達に関するすべての合意事項を検証したかどうかを決定する。
- 合意内容をレビューして、それをポリシーの文書と比較して、それが企業のポリシーを遵守しているかどうかを決定する。
- 適切な人員によって調達がレビューされ承認されたかどうか、法的な助言を得たかどうかを決定する。
- 契約のレビューと承認の文書を閲覧する。
- ソフトウェア、インフラストラクチャ、施設の調達のための共通コントロールプロセスが確立され用いられているかどうかを調査する。
- プロセスのウォークスルーを実施して、そのコントロールプロセスが効果的に運用されているかどうかを決定する。
- 調達に関するすべての当事者の権利と義務が調達プロセスで評価されたかどうかを調査する。このような権利と義務は以下のようなものを含みうる。
  - 承認
  - サービスレベル
  - 保守手続
  - アクセスコントロール
  - セキュリティ
  - パフォーマンスレビュー
  - 支払い方式
  - 裁定手続
- 調達の代表サンプルについて、すべての当事者の権利と義務が評価されたかどうかを決定する。
- 調達プロセスが、以下を含む関連する権利と義務のすべてを十分に考慮しているかどうかを調査する。
  - 知的財産の所有権とライセンス
  - 保守
  - 保障と裁定手続
  - アップグレード条項
  - セキュリティを含む目的への適合性
  - エスクローとアクセス権
- 調達に関連する経営者への報告の要件に対処しているかどうかを決定する。
- すべての調達での品質評価と受け入れのプロセスが確立され用いられているかどうかを調査して、すべての調達での支払いの前にこのプロセスが効果的に実施されているかどうかを決定する。
- すべてのハードウェアとソフトウェアの調達が記録されているかどうかを調査する。
- 調達の代表サンプルを選択し、それが資産台帳に記録されていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
- 最近の調達の選定について、選定のアプローチが調達の単一のリスクに対応したものかどうかを決定する（ビジネスの機能と技術の要件に合致する、リスク分析報告で特定されたリスクに対処する、調達の意思決定を遵守するなど）
- IT調達の選定について、主要な意思決定ポイントでの承認の証拠を閲覧する。証拠には、標準のポリシーに従わなかった選定に対する上級マネジメント層の承認も含まれる。
- 契約の選定について、承認された供給業者のみが利用されているかどうかを決定する。
- 供給業者と調達の契約の選定について、RFIとRFPを事前定義された要件と比較し、確立された判断基準に合致しているかどうかを決定する。
- ソフトウェア調達に、すべての当事者の権利と義務（知的財産の所有権ライセンス、保守の保障、裁定手続、アップグレードの条項、セキュリティを含む、目的との適合性、エスクローとアクセス権など）が含まれており、それを守らせているかどうかを調査して確認する。ソフトウェア調達の選定について、関連する文書を閲覧して、契約条項にすべての当事者の権利と義務が含まれているかどうかを決定する。
- 開発のための資源の調達にすべての当事者の権利と義務が含まれており、それを守らせているかどうかを調査して確認する（たとえば、知的財産の所有権とライセンス、開発の方法論を含む目的への適合性、言語、テスト、パフォーマンスの判断基準を含む品質管理手続、パフォーマンスレビュー、支払い方式、保障、裁定手続、人事管理、および組織のポリシーの遵守などを確かめる）。
- 資源の開発の調達において知的財産の所有権とライセンスについての合意に関して、法的助言を受けたかどうかを決定する。
- インフラストラクチャ、設備、関連するサービスの調達に、すべての当事者の権利と義務（サービスレベル、保守手続、アクセスコントロール、セキュリティ、パフォーマンスレビュー、支払い方式、裁定手続など）が含まれており、それを守らせているかどうかを調査して確認する。インフラストラクチャ、施設、および関連するサービスの調達の選定に際し、関連する文書を閲覧して、契約条項にすべての当事者の権利と義務が含まれているかどうかを決定する。
- RFIとRFPが承認された手続と判断基準にしたがって評価されているかどうかを調査して確認する。文書による証拠が効果的に維持されているかどうかを決定する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- ITの調達が組織の調達ポリシーと整合的でないことの費用的および時間的影響を評価する。
- ITの調達が、ビジネス、法律、契約の要件に合致しないことの費用的および時間的影響を評価する。
- 供給業者と調達先の選定プロセスが法律と契約の要件を遵守していないことが法的にどのような意味を持つかを評価する。

AI6 変更管理

インフラストラクチャおよびアプリケーションに関連する緊急保守やパッチ適用を含む、本番環境におけるすべての変更は、コントロールされた方法で、正式に管理されている。変更(手続、プロセス、システムパラメーター、およびサービスパラメーターを含む)は、変更の実施前に記録、評価、および承認され、変更の実施後には計画された成果に照らしてレビューされる。これにより、本番環境の安定性やインテグリティに悪影響を及ぼすリスクを低減できる。

コントロール目標	価値のドライバー	リスクのドライバー
AI6.1 変更の標準と手続 アプリケーション、手続、プロセス、システムパラメーターとサービスパラメーター、および基盤プラットフォームに対するすべての変更要求(保守やパッチ適用を含む)を、標準化された方法で処理できるよう、正式な変更管理手続を確立する。	・変更管理を効率的かつ効果的な方法で実施するための合意済みで標準化されたアプローチ ・一貫した協調的な方法でレビューされ承認される変更 ・正式に定義された期待と成果の測定	・不適切な資源配分 ・追跡されていない変更 ・緊急変更に対する不十分なコントロール ・承認されていない変更が主要な業務システムに導入される可能性の増加 ・コンプライアンス要件の遵守違反 ・承認されていない変更 ・システム可用性の減少

コントロール設計のテスト

・変更要求(保守とパッチ適用を含む)を扱うためのプロセスと手続が、アプリケーション、手続、プロセス、システムとサービスパラメータ、および基盤プラットフォームに適用されているかどうかを調査して、それを確認する。
・変更管理フレームワークをレビューして、そのフレームワークが以下を含むかどうかを決定する。
  - 役割と責任の明確化
  - すべての変更の分類(インフラストラクチャとアプリケーションソフトウェアとの区別など)と優先順位づけ
  - 影響、権限、承認の評価
  - 変更の追跡
  - バージョンコントロールメカニズム
  - データのインテグリティへの影響(データファイルへのすべての変更が、ユーザが直接介入するのではなく、システムとアプリケーションのコントロールのもとで行われるなど)
  - 開始からレビューと終了までの変更の管理
  - ロールバック手続の策定
  - 緊急変更プロセスの利用
  - 事業継続性計画
  - 記録管理システムの利用
  - 監査証跡
  - 職務の分離
・契約を締結している供給業者(インフラストラクチャ、アプリケーション開発、アプリケーション供給業者、共有サービス)のためのプロセスと手続が変更管理プロセスに含まれているかどうかを調査して、それを確認する。
・プロセスと手続に、契約条件とSLAが含まれているかどうかを決定する。

コントロール目標	価値のドライバー	リスクのドライバー
AI6.2 影響評価、優先順位付け、および認可 すべての変更要求を評価して、本番運用中のシステムや、その機能に与える影響を体系的に特定できるようにする。変更は分類した上で優先順位を付け、許可を与える。	・影響を効率的かつ効果的な方法で評価するための合意済みで標準化されたアプローチ ・ビジネスリスクと成果の測定に基づき、正式に定義された、変更による影響の予想 ・一貫した変更手続	・意図せざる副次効果 ・インフラストラクチャのキャパシティとパフォーマンスへの悪影響 ・変更に対する優先順位の管理の欠如

コントロール設計のテスト

・変更管理プロセスによって、ビジネスプロセスオーナとIT部門が、インフラストラクチャ、システム、ないしアプリケーションに対する変更を要求することができるかどうかを調査して、それを確認する。
・要求された変更が分類されている（インフラストラクチャ、オペレーティングシステム、ネットワーク、アプリケーションシステム、市販のアプリケーションソフトウェアなど）かどうかを調査して、それを確認する。
・主要な担当者へのインタビューを通じて、要求された変更に対して、所定の判断基準に基づいて優先順位がつけられていることを確かめる（変更に対するビジネスと技術上の必要性および、法律、規制、契約上の要件など）。
・インフラストラクチャ、システム、およびアプリケーションへの影響の分析を扱う構造化された方法で、変更要求が評価され文書化されているかどうかを調査して、それを確認する。
・変更要求の評価プロセスにおける、セキュリティ、法律、契約、コンプライアンスとの関わりが考慮されており、ビジネスオーナが関与しているかどうかを調査して、それを確認する。
・要求された変更のそれぞれが、ビジネスプロセスオーナとIT部門の技術の当事者によって正式に承認されているかどうかを調査して、それを確認する。
・変更管理要求の代表サンプルを閲覧して、それが適切に評価され、優先順位をつけられ、レビューされたことを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI6.3 緊急変更 規定された変更プロセスに従わない緊急変更の定義、提起、テスト、文書化、評価、および承認のプロセスを確立する。	・変更管理を効率的かつ効果的な方法で実施するための合意済みで標準化されたアプローチ ・緊急変更による影響と成果に関する、正式に定義された測定 ・緊急変更に対する一貫した手続	・緊急変更の必要性に対して効果的に対応する能力の欠如 ・適切に終了していない追加的なアクセス承認 ・承認されていない変更の適用と、それによるセキュリティの危殆化と、企業情報に対する未承認のアクセス

コントロール設計のテスト

- 変更管理プロセス全体に、緊急変更手続（緊急変更の定義、提起、テスト、文書化、評価、権限授与など）が含まれているかどうかを調査して、それを確認する。
- 緊急変更の代表サンプルについて文書を閲覧し、主要な担当者にインタビューすることによって、緊急変更が変更管理プロセスで特定されたとおりに実施されているかどうかを確証する。
- 主要な担当者へのインタビューを通じて、緊急にアクセス権を付与する場合は、承認され文書化され、変更が適用された後でアクセス権が剥奪されていることを確かめる。
- 緊急変更に対する導入後のレビューが実施されているかどうかを調査して、それを確認する。

コントロール目標

AI6.4 変更の状況追跡および報告
否認された変更を文書化し、承認された変更、および現在進行中の変更の状況を周知し、さらに変更を実施するための追跡および報告システムを構築する。承認された変更が予定どおり実施されるようにする。

価値のドライバー

- 効率的かつ効果的な方法で変更管理を実施するための合意済みで標準化されたアプローチ
- 正式に定義された期待と成果の測定
- 一貫した変更手続

リスクのドライバー

- 不十分な資源配分
- 記録されておらず追跡されていない変更
- 本番環境への変更で発見されておらず未承認のもの

コントロール設計のテスト

- 要求者と利害関係者が、変更管理プロセスの様々なステージを通じて要求の状況を追跡できるような確立したプロセスがあるかどうかを調査して、それを確認する。
- 追跡と記録のシステムで、変更要求の状況（却下、承認されているが開始していない、承認済、作業中など）をモニタリングしているかどうかを調査して、それを確認する。
- マネジメント層が、変更の詳細な状態と全体の状態（変更要求がなされてからの日数の分析など）をレビューしてモニタリングしているかどうかを調査して、それを確認する。
- 開始され承認された変更が、優先順位に応じてタイムリーに終了しているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI6.5 変更の終了および文書化 変更を実施した場合は都度、関連するシステムマニュアルやユーザマニュアル、手続などを適切に更新する。	・変更を文書化するための、合意済みで標準化されたアプローチ ・正式に定義された期待 ・変更と文書化のための一貫した手続	・主要な個人への依存の増加 ・現在のシステム構成を反映していないシステム構成文書 ・ビジネスプロセスの文書の欠如 ・ハードウェアとソフトウェアの変更状況が更新されない状態

コントロール設計のテスト

・変更に関する文書（運用手続、構成情報、アプリケーションの文書、ヘルプスクリーン、研修教材など）が最新の状態を保っているかどうかを調査して、それを確認する。
・変更に関する文書（導入前および導入後のシステムとユーザの文書）が保存されているかどうかを調査して、それを確認する。
・ハードウェアやソフトウェアに導入された変更に関して、ビジネスプロセスの文書が更新されているかどうかを調査して、それを確認する。

コントロール目標の達成をテストするために以下のステップを踏む。
・変更のサンプルについて、適切な利害関係者（ビジネスプロセスオーナとITマネジメント層）によって以下が承認されていることを確かめる。
  – 変更要求
  – 変更の仕様
  – ソースプログラムへのアクセス
  – プログラマによる変更の完了
  – ソースをテスト環境へ移行させる要求
  – 受け入れテストの完了
  – コンパイルの要求と本番環境への移行
  – セキュリティへの全体的および個別的な影響の決定と受け入れ
・配布プロセスの策定
・以下を含むための変更コントロールの文書のレビュー
  – 要求された変更の日付
  – 要求者
  – 変更要求の承認
  – 実施された変更の承認—IT部門
  – 実施された変更の承認—ユーザ
  – 文書を更新した日付
  – 本番環境への移行日
  – 変更に対するQA上の承認
  – 運用部門による受け入れ
・変更を選び出したものについて、文書をレビューして、バージョンコントロールメカニズムが存在するかどうかを決定する。
・業務委託先に関連する変更を選び出したものについて、導入された変更を調査し、それがベンダの提供する指示に従っているかどうかを決定する。
・変更を選び出したものを閲覧し、要求が分類されているかどうかを決定する。
・変更を選び出したものを調査して、事前定義済みの判断基準に基づいて変更の優先順位がつけられ

ているかどうかを決定する。
- 変更を選び出したものを調査して、変更が構造化された方法論（セキュリティ、法律、契約、コンプライアンスへの影響が考慮され、ビジネスオーナが関与しているなど）で評価されているかどうかを決定する。
- 緊急変更のサンプルを調査して、それが変更管理フレームワークにしたがって処理されていることを確かめる。アクセス権を承認し、文書化し、変更が適用された後に廃止するための手続に従っているかどうかを確かめる。
- 緊急変更のサンプルを調査して、変更が適用された後で導入後のレビューが実施されているかどうかを決定する。アプリケーションシステムへのさらなる保守への影響、開発環境とテスト環境への影響、アプリケーションソフトウェア開発の品質、文書とマニュアル、データのインテグリティを検討する。
- 追跡システムおよび記録システムへのウォークスルーを実施して、却下された変更、承認されて作業中の変更の状況、完了した変更に関する文書が保存されていることを確かめ、ユーザとともに、その状況が最新であることを確認する。
- 変更状況報告を選び出したものを閲覧して、導入から廃棄まで変更を追跡するための監査証跡が用いられているかどうかを決定する。
- 変更状況報告のサンプルを閲覧して、経営者のレビューやモニタリングを支援するための、成果の測定指標が用いられているかどうかを決定する。
- 変更のサンプルを調査して、変更に関する文書が適切な保持期間にしたがって保持されているかどうかを決定する。
- ビジネスプロセスマニュアルを閲覧して、それがハードウェアとソフトウェアに対して新規または改善された機能をもたらす変更によって更新されているかどうかを決定する。
- 変更のサンプルを選び、サードパーティとの協力の質を評価する。
- 変更管理プロセスの成果を評価するプロセスを確認する。ITマネジメント層に対して、変更管理プロセスの改善を提言することになるような潜在的な改善を特定したら、それを評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 正式な変更管理の標準と手続が無いことによる時間と費用を評価する（資源配分が不適切、役割と責任が不明確、セキュリティ違反、ロールバック手続がない、文書と監査証跡がない、研修が不十分など）。
- 変更の優先順位をつけて承認するための正式な影響度評価が無いことによる時間と費用を評価する。
- 緊急変更に関する正式な標準と手続が無いことによる時間と費用を評価する（セキュリティが損なわれている、追加的なアクセス権限を適切に終了していない、企業の情報に対して承認されていないアクセスがあるなど）
- 変更に対する追跡と記録が無いことによる影響を評価する（資源配分が不十分、優先順位の管理がない、変更の記録と追跡がない、本番環境への承認されていない変更が発見されないなど）。
- システムとユーザの文書が無いことによる影響を評価する（主要な個人への依存が増している、構成の文書が現在のシステム構成を反映していない、文書にビジネスプロセスの記載がない、ハードウェアとソフトウェアの変更についての更新がないなど）。
- 変更プロセスの評価が無いことによる影響を評価する（システムがエンドユーザの必要性に合致していない、変更に対する費用と資源のコントロールがない、変更がビジネスの焦点と合っていない、投資の収益率が経営者の期待に合致していない、ビジネスプロセスで新しいシステムが利用できないなど）。

AI7 ソリューションおよびその変更の導入と認定

新規システムの開発完了後、そのシステムを実際に運用可能な状態にする必要がある。これには、適切なテストデータをしようした専用環境における公式的なテストの実施、展開と移行の指示書の策定、リリース計画策定と実際の本番環境への移行、および導入後のレビューが必要である。これにより、運用システムが合意された計画と成果に合致していることを保証する。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.1 研修 すべての情報システムの開発、導入、修正プロジェクトの一環として、策定された研修計画と導入計画、および関連資料に従って、影響を受ける部門のスタッフやIT部門の運用グループのスタッフに研修を実施する。	・ 新しいスキルの一貫性のある開発 ・ 効果的かつ効率的な作業の成果のための研修の改良 ・ 新しいシステムや改変されたシステムへの習熟	・ システムやその利用における問題の発見の遅れ ・ 要求された責務や活動の実施にあたっての知識におけるギャップ ・ 新しいプロジェクトから生じるエラー

コントロール設計のテスト

- 研修計画が、開発プロジェクト全体のマスタープランの一部となっているかどうかを調査して、それを確認する。
- 影響を受けるグループ（ビジネスエンドユーザ、IT運用部門、サポートチームとITアプリケーション開発研修チーム、供給業者など）を研修計画で特定し、それに対処しているかどうかを（主要な担当者へのインタビューやプロジェクト計画を閲覧するなどして）調査して、それを確認する。
- 費用対効果の高いアプローチが選択され研修のフレームワークに導入されるよう、代替的な研修戦略が検討されているかどうかを調査して、それを確認する。
- 研修計画の遵守を確かめるためのプロセスが存在するかどうかを調査して、それを確認する。
- 研修の文書を閲覧して、研修計画を遵守しているかどうかを決定する（研修に招待された担当者の一覧、受講者一覧、学習目標の達成と他のフィードバックのための評価フォームなど）。
- システムへの潜在的な改善のもとになりうるフィードバックを得るために研修をモニタリングするプロセスがあるかどうかを調査して、それを確認する。
- 研修の要件が検討されそれに適合する計画が作成されるよう、計画された変更がモニタリングされているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.2 テスト計画 組織全体の標準に基づいて、役割、実行責任、開始基準、および終了基準を定義するテスト計画を策定する。テスト計画について関係者からの承認を得る。	・ 主要な利害関係者のコミットメント ・ システムの処理が機能しなくなることによるビジネスの中断の最小化	・ 自動化テストスクリプトによる不十分なテスト ・ 発見されないパフォーマンスの問題 ・ テスト活動に対する費用のコントロールの欠如 ・ テストにおける定義されていない役割と責任

コントロール設計のテスト

- プロジェクト品質計画と関連する組織での標準にしたがってテスト計画が作成され文書化されており、それが適切なビジネスオーナとITの利害関係者に伝達されているかどうかを調査して、それを確認する。
- テスト計画が、プロジェクトのリスク評価を反映しており、すべての機能的および技術的なテスト要件が含まれているかどうかを調査して、それを確認する。
- テスト計画で、テストを実行しテスト結果を評価するための資源を特定しているかどうかを調査して、それを確認する。
- テスト計画の資源への影響について利害関係者が相談を受けていることを確かめる。
- 場所の準備、研修の要件、定義されたテスト環境のインストールと更新、テストケースの計画/実施/文書化/保持、エラーと問題の扱い、修正とエスカレーション、および正式の承認を含むテストの準備をテスト計画で考慮しているかどうかを調査して、それを確認する。
- テスト計画のサンプルについて、文書を閲覧して、適切なテストフェーズが実施されているかどうかを決定する。
- テスト計画で、それぞれのテストフェーズの着手の成功を測定するための明確な判断基準を確立しており、成功基準を策定する際にビジネスプロセスオーナとITの利害関係者との相談が考慮されているかどうかを調査して、それを確認する。
- 成功基準に合致しないときの修復手続を計画で確立しているかどうかを決定する（テストフェーズに重要な不備がある場合には、次のフェーズへ進むか、テストを中止するか、導入を延期するかについてのガイダンスを計画で提供するなど）。
- テスト計画が、必要に応じてビジネスプロセスオーナとIT部門を含む、利害関係者によって承認されているかどうかを調査して、それを確認する。他の利害関係者の例としては、アプリケーション開発管理者、プロジェクト管理者、およびビジネスプロセスのエンドユーザなどが挙げられる。

コントロール目標

AI7.3 導入計画

代替/変更取り消しを含む導入計画を策定する。関係者からの承認を得る。

価値のドライバー

- 変更の導入を効率的かつ効果的な方法で実施するための合意済みで標準化されたアプローチ
- 正式に定義された期待と成果の測定
- 導入に失敗した場合の効果的な回復

リスクのドライバー

- 変更の有効な導入を確実に行うのに適切でない資源配分
- セキュリティ違反

コントロール設計のテスト

- プロジェクトの代表サンプルについて、導入計画がレビューされ承認されていることを確かめる。
- 広範な導入戦略、導入のステップの順序、資源の要件、相互依存性、経営者が本番環境への導入に合意するための判断基準、本番環境でのサポートのための導入の検証の要件と移行戦略を含む、導入計画が策定されているかどうかを調査して、それを確認する。
- プロジェクトの代表サンプルを選び、導入計画がビジネス部門の変更管理計画と整合的であることを確かめる。
- 導入の各段階でサードパーティが関与することにコミットしているかどうかを調査して、それを確認する。
- 導入計画で、代替および回復のプロセスが特定され文書化されているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.4 テスト環境 セキュリティ、内部統制、運用上の実践方法、データ品質、プライバシーの要求、および作業負荷に対応して計画された運用環境を想定した安全なテスト環境を定義、確立する。	・本番環境での最小化された業務の中断	・自動化テストスクリプトを用いた不十分なテスト ・発見されないパフォーマンス上の問題 ・システムセキュリティの侵害

コントロール設計のテスト

・本番環境をミラーするテスト環境が立ち上げられているかどうかを調査して、それを確認する（作業負荷/ストレス、オペレーティングシステム、必要なアプリケーションソフトウェア、データベース管理システム、ネットワークとコンピュータのインフラストラクチャといった要素が含まれる）。
・テスト環境が本番環境と相互に関連できないようになっているかどうかを調査して、それを確認する。
・テストデータベースが存在するかどうか質問して確認する。
・テストデータベースを作成する際のデータ洗浄プロセスの存在と品質を評価する。
・テスト環境の保護手段とテスト環境へのアクセス権限を評価する。
・テスト結果の保持と廃棄を管理するためのプロセスが存在し、それを遵守しているかどうかを調査して、それを確認する。
・保持プロセスが規制やコンプライアンスの要件に合致するかあるいはそれを上回っているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.5 システムおよびデータの変換 監査証跡、変更取り消し計画、代替計画を含む組織の開発手法の一環として、データ変換とインフラストラクチャ移行の計画を策定する。	・発見され本番環境から取り除かれる不適切な構成要素 ・意図した通りに動作してビジネスプロセスをサポートする新システム	・必要なときに利用できない旧システム ・信頼できないシステムと変換結果 ・後続の処理への支障 ・データのインテグリティの問題点

コントロール設計のテスト

・（主要な担当者へのインタビューやポリシーと手続の閲覧によって）データ変換とインフラストラクチャの移行の計画が存在することを確かめて、以下を検討する。ハードウェア、ネットワーク、オペレーティングシステム、ソフトウェア、トランザクションデータ、マスタファイル、バックアップとアーカイブ、内部および外部の他のシステムとのインターフェース、手続、システム文書など。
・主要な担当者へのインタビューを通じて、変換のカットオーバの時期と網羅性について尋ねる。
・変換に先立ってバックアップを取っており、監査証跡を維持しており、代替と回復の計画が存在するかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.6 変更のテスト 本番環境への移行前に、定められたテスト計画に従って、独立して変更をテストする。テスト計画においては、セキュリティと性能を考慮する。	・アーカイブされたシステムのパフォーマンス ・費用の効果的なコントロール ・顧客の信頼の増加	・資源の浪費 ・全体のセキュリティの低下 ・システムのパフォーマンスと可用性に影響する変更

コントロール設計のテスト

・変更のテストが独立して策定され（職務の分離）、テスト環境でのみ実施されているかどうかを調査して、それを確認する。
・セキュリティとパフォーマンスの要件を検証するためのテストスクリプトが存在するかどうかを調査して、それを確認する。
・変更が本番環境へと進むのに先立って、代替および回復の計画が作成されテストされていることを、インタビューを通じて確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.7 最終受け入れテスト ビジネスプロセスオーナとIT利害関係者がテスト計画に従ってテストプロセスの成果を評価する。テスト計画とその他必要な回帰テストで特定された一連のテストを通じて、テストプロセス中に明らかになった重大なエラーを是正する。評価を実施した後、本番環境への移行の承認を行う。	・本番環境における最小化された業務の中断 ・重要なデータフローの保護 ・期待されたサービス品質からの逸脱の特定 ・使いやすさの要件に合致したアプリケーション	・パフォーマンス上の発見されない問題 ・提供されている性能のビジネス部門による拒絶

コントロール設計のテスト

・最終受け入れテスト活動で、主要な利害関係者が考慮されていることを確かめる。
・最終受け入れの段階で、成功基準がテスト計画で特定されているかどうかを調査して、それを確認する。
・レビューと評価のための適切な文書が存在するかどうかを調査して、それを確認する。
・最終受け入れテスト結果の文書化および提出が完全かつタイムリーかどうかを、主要な利害関係者に尋ねる。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.8 本番環境への移行 テストを実施した後、導入計画に従って、変更したシステムの運用段階への移行をコントロールする。ユーザ、システムオーナ、現場管理者など主要な利害関係者から承認を得る。可能な場合は、旧システムをある一定期間並行して実行し、運用状況と結果を比較する。	・効率的かつ効果的な方法で変更を本番へ反映させるための合意済みで標準化されたアプローチ ・正式に定義された期待と成果に関する測定 ・一貫した変更手続	・職務の分離の違反 ・不正やその他の悪意ある行動に晒されたシステム ・前のバージョンのアプリケーションシステムへのロールバックの不在

コントロール設計のテスト

・プログラムの移行のための手続をレビューして、ユーザ部門のマネジメント層とシステム開発部門の書面による承認を必要とするような、正式なプロセスが存在することを確かめる。
・承認プロセスが、新しいシステム、アプリケーション、ないしインフラストラクチャの有効な本番移行日、および旧来のシステム、アプリケーション、およびインフラストラクチャの有効な停止日を特定していることを確かめる。
・ビジネスプロセスオーナ、サードパーティ、ITの利害関係者（開発グループ、セキュリティグループ、データベース管理、ユーザサポート、および運用グループなど必要に応じて）からの正式な書面による承認が承認プロセスに含まれているかどうかを調査して、それを確認する。
・システムの文書と関連するコンティンジェンシープランのコピーを更新するための手続を確認する。
・すべてのソースプログラムライブラリを更新するための手続きと、前のバージョンのラベルをつけ保持するための手続に関して、主要な担当者に尋ねる。
・受け入れテスト部門から導入に用いたメディアを得るために要求される手続について、主要な担当者に尋ねる。
・ソフトウェアの自動配布がコントロールされているかどうか、および配布先の環境が正しい導入基準およびバージョン下にあるかどうかを検証するチェックが配布プロセス中に存在するかどうかを、主要な担当者に尋ねる。
・コントロールの有効性を評価して、承認され正しく特定された配布先にのみ配布が行われることを確かめる。
・どのソフトウェアと構成項目が配布されたか、誰に配布されたか、どこで導入されたか、およびそれぞれがいつ更新されたかの正式なログが保存されているかどうかを主要な担当者に尋ねる。
・すべてのプログラムのコピーを迅速に更新するための手続および、影響を受けるすべての場所に先立って導入の指示を与えるための手続について、主要な担当者に尋ねる。

コントロール目標	価値のドライバー	リスクのドライバー
AI7.9 導入後レビュー 導入計画の規定に従い、変更管理に関する組織の標準に基づいて導入後レビューを実施するための手続を定める。	・導入後のレビューのための、合意済みで標準化されたアプローチ ・一貫性のある分かりやすいレビュー手続 ・組織の資源の効率的な利用 ・エンドユーザの満足度の向上	・システムがエンドユーザのニーズに合致していないことを特定できない状態 ・マネジメント層の期待に合致しない投資の収益率

コントロール設計のテスト

・主要な担当者へのインタビューを通じて、導入後の手続が確立していることを確かめる。
・主要な担当者へのインタビューを通じて、ビジネスプロセスオーナとITの技術管理部門が、要件と利益の成功と達成を測定するための指標の選定に関与していることを確かめる。
・主要な担当者へのインタビューを通じて、導入後のレビューの形式が、組織の変更管理プロセスにしたがっており、ビジネスプロセスオーナとサードパーティが必要に応じて関与していることを確かめる。
・主要な担当者へのインタビューを通じて、外部のビジネス部門とIT部門から生じる導入後のレビューの要件が考慮されていることを確かめる。
・主要な担当者へのインタビューを通じて、導入後のレビューで特定された問題点に対処するための行動計画が存在し、ビジネスプロセスオーナとITの技術管理部門が、行動計画の策定に関与していることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・研修計画を閲覧して、それが学習目標、資源、主要なマイルストーン、依存性、クリティカルパスの作業を明確に特定しているかどうかを決定する。研修計画で、ビジネスでの必要性に応じて代替的な研修戦略を検討していることを確かめる。
・研修計画の文書を閲覧して、以下を確認する。
  – 研修を受講しなければならない担当者を特定している
  – 研修がタイムリーな方法で提供されている
  – 費用対効果の高いアプローチが選択され利用されている（講師向けの事前研修、エンドユーザの認定、インターネットベースの研修など）
  – システムでの潜在的な改善の領域を特定する際に、フィードバック（評価フォーム、コメントシートなど）を受け取り利用している
  – 計画された変更が研修の要件で考慮されている
  – プロジェクト品質計画と関連する組織の標準と整合的である
  – テスト計画がしかるべきビジネスオーナとIT部門の利害関係者に伝達されている
・テストの文書を閲覧して、プロジェクトのリスク評価に基づいてテストが実施されているかどうかを決定する。すべての機能的および技術的なテスト要件がカバーされており（パフォーマンス、ストレス、使いやすさ、パイロット、およびセキュリティのテストなど）テスト計画が内部および外部の認定のためのいかなる要件にも対処していることを確かめる。
・テストの文書を閲覧して、テストを実行しその結果を評価するための資源が特定されたかどうかを決定する（テスト環境の構築とテストグループのための担当者など。本番環境または開発環境でのテスト担当者の一時的にあり得る置き換えを含む）。
・テストスクリプトのサンプルをレビューして、それがそれぞれのテスト基準に十分に対処していることを確かめる。
・システム開発、導入、または改変のプロジェクトのサンプルについて、テストの文書を閲覧して、適切なテ

ストフェーズが実施されているかどうかを決定する（単体テスト、システムテスト、統合テスト、ユーザ受け入れテスト、パフォーマンステスト、ストレステスト、データ変換テスト、セキュリティテスト、運用準備テストなど）。
- テスト計画のサンプルについて、文書を閲覧して以下を決定する。
  - それぞれのテストフェーズの成功を測定するための判断基準を検討しているか
  - テスト計画が承認されているか
  - テストデータベースが洗浄されたデータのみを用いており、漏洩から保護されているか
- 変換計画が十分かどうかを調査して、データオーナと共に変換の結果の網羅性とインテグリティを確認する。
- 代替/回復計画のための文書を閲覧して評価する。
- タイムリーなバグ修正および復旧を容易にするような監査証跡がエラーログに含まれていることを確かめる。
- 最終受け入れテスト活動をレビューして、すべての構成要素が効果的に対象範囲でカバーされており、そこで受け入れ基準に効果的に対処しているかどうかを評価する。
- 受け入れテストの結果をレビューして、その解釈と提示の有効性を評価する。
- テストの結果を調査して、本番環境移行前に正式な承認が存在することを確かめる。
- ソースプログラムライブラリを閲覧して、それが現在のバージョンへと更新されており、合理的な期間にわたって、前のバージョンにラベルがつけられ保持されていることを確かめる。
- コントロールの有効性を評価して、承認され正しく特定された配布先にのみ配布が行われることを確かめる。
- ログを閲覧して、網羅性とインテグリティが確保された手続が実施されていることを確かめる。
- ファイル上の導入の指示を物理的に調査する。
- システムの開発、導入、改変のプロジェクトのサンプルを選び、変更の文書を閲覧して、ソフトウェアが本番へとリリースされる前に変更が確実に承認され、テストされ、適切に文書化されるようマネジメント層の承認が実施されているかどうかを決定する。
- アーカイブ環境のウォークスルーを実施して、アーカイブされたバージョンと文書を物理的に閲覧する。
- 承認され、テストされ、文書化された変更のみが本番環境に受け入れられるということを保証するための変更の移行プロセスの有効性を評価する。
- 導入されているソフトウェアがテストされたものから変更されていないことを保証するためのプロセスの有効性を評価する。
- ビルド要求のサンプルを選び、文書を閲覧して、メディアの作成が、正式なビルド要求のみに基づいているかどうかを決定する。
- 変更や取り消しの手続の有効性を確かめる。
- 配布されているソフトウェアと構成の項目、誰に配布したか、どこに導入されたか、およびそれぞれがいつ更新されたかが、配布監査証跡に含まれていることを確かめる。
- 承認され正しく特定された配布先にのみソフトウェアの自動配布が行われることを確かめる。
- ビジネス要件に合致している度合い、期待された便益が実現している度合い、システムが利用しやすいと考えられる度合い、内部と外部の利害関係者の期待に合致している度合い、予期せぬ影響が組織に生じる度合い、主要なリスクが軽減される度合い、および、変更管理、インストール、認定のプロセスが効果的かつ効率的に実施される度合いを、導入後の手続で特定し、評価し、報告していることを確かめる。
- 外部のビジネス部門とIT部門から生じる導入後のレビューの要件が考慮されているかどうかを調査して、それを確認する。
- システムの開発または導入のプロジェクトのサンプルについて、外部のビジネスとITの要件（内部監査、全社的なリスク管理、規制の遵守など）が導入後のレビューに含まれていることを確かめる。
- システムの開発と導入のプロジェクトのサンプルを選び、導入後の計画に、特定された問題点に対処するための行動計画が含まれていることを確かめる。ビジネスプロセスオーナとITの技術管理部門が行動計画の策定に関与していることを確かめる。
- 変更の成功や失敗を確かめるためのプロセスの有効性を評価する。
- 構成の棚卸を評価して、変更がレビューされ受け入れられているかどうかを決定する。

・以下を特定する。
  – 承認なしになされた変更
  – 考慮されていない変更
  – 現在のライブラリ（ソースとオブジェクト）で最新の変更を反映していないもの
  – 変更コントロール手続の差異
・失敗したりエラーとなった変更の影響を評価する。
・時期が遅かったり遅延したりした変更の影響を評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・研修が無いことによる費用と運用の非効率性を評価する（問題を迅速に発見できない、職務を遂行するための知識にギャップがあるなど）。
・テスト計画が無いことによる影響を評価する（自動化テストスクリプトによるテストが不十分、パフォーマンスの問題を発見できない、費用のコントロールがない、役割と責任が定義されていないなど）。
・主要な利害関係者によって導入計画がレビューされ承認されており、プロジェクト全体を通じて適切なコミットメントが存在するようになっているかどうかを評価する。
・本番環境をミラーしてビジネスの業務への変更に関して信頼できる将来の状態を提供するためのテスト環境が存在するかどうかを評価する。
・データ変換計画の網羅性を評価して、監査証跡、ロールバック手続、フォールバック手続が含まれていることを確かめる。
・本番環境への移行に先立って、定義されたテスト計画にしたがって独立にテストされている変更を評価する。
・セキュリティとパフォーマンスの要件を検証するテストを含めるためのテスト計画を評価する。
・本番移行前にタイムリーに修復することが求められるエラーを特定するためのテストプロセスの結果を評価する。
・導入後の計画が無いことによる影響を評価する。

（空白ページ）

付録Ⅳ—サービス提供とサポート（DS）

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　性能と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　費用の捕捉と配賦
DS7　利用者の教育と研修
DS8　サービスデスクとインシデントの管理
DS9　構成管理
DS10 問題管理
DS11 データ管理
DS12 物理的環境の管理
DS13 オペレーション管理

付録Ⅳ—サービス提供とサポート（DS）

プロセス保証のステップ

DS1 サービスレベルの定義と管理

IT管理部門とビジネス部門の顧客間で、求められるサービスについて効果的なコミュニケーションを行うためには、ITサービスおよびサービスレベルの定義と合意内容を文書化する必要がある。本プロセスには、サービスレベルの達成状況についてモニタリングし、利害関係者にタイムリーな報告をすることも含まれる。このプロセスにより、ITサービスと関連するビジネス要件との間の整合を図ることができる。

コントロール目標	価値のドライバー	リスクのドライバー
DS1.1 サービスレベル管理フレームワーク 顧客とサービスプロバイダ間で正式に合意されたサービスレベル管理プロセスを定めたフレームワークを定義する。このフレームワークを通じて、サービスレベルとビジネス要件およびビジネス上の優先事項との間の整合性を継続的に維持すると同時に、顧客とサービスプロバイダ双方における認識の共有を促進する。このフレームワークには、サービスに対する要件、サービス定義、SLA、OLAを策定し、資金の調達元を明確にするためのプロセスを含める。これらのサービス属性は、サービスカタログ(service catalog)にまとめる。またこのフレームワークでは、サービスレベルの管理のための組織構造を定義する。その定義には、組織内外のサービスプロバイダと顧客の役割、タスク、および実行責任を含める。	・ 明確化されたITサービスの責任と、事業目標と整合的なITの達成目標 ・ ビジネスカスタマーとITサービスプロバイダとの間の意思伝達と理解の改善 ・ サービスレベル、サービス定義、サービスの提供とサポートにおいて促進される一貫性	・ 期待と能力との間にギャップとそれによる係争 ・ 自らの責任を理解していない顧客とプロバイダ ・ 異なる提供サービスに対する不適切な優先順位付け ・ 非効率的で費用のかかる運用サービス

コントロール設計のテスト

- SLAのポリシーと手続を閲覧して、SLAの達成目標と成果の測定指標が事業目標およびIT戦略と整合的であるかどうかを見る。
- ポリシーがSLAの達成目標及び成果の測定指標と事業目標及びIT戦略と整合するために存在しているかどうかを調査して、確認する。
- サービスカタログを閲覧して、サービス要件、サービス定義、SLA、OLA、資金源を取り入れてあることを確かめる。
- SLAのエスカレーションと問題解決に説明責任を持つ担当者に問題に対応する際に合理的なサービスレベルを手続や方法論で確立したかどうかを尋ね、確認する。
- 関連する変更のサンプルを調査して、変更管理プロセスにしたがって変更が実施されていることを確かめる。
- 成果を測定するための標準に関して、サービス改善プログラムの設計を閲覧する。

コントロール目標	価値のドライバー	リスクのドライバー
DS1.2 サービスの定義 主にサービスカタログやポートフォリオ方式の導入を通じて収集され、蓄積されたサービス特性とビジネス要件に基づいて、ITサービスの基本的な定義を行う。	・事業目標と整合的なITサービスの目標 ・正しい要件と優先順位に基づくIT運用サービス ・影響の及ぶサービスと関連付けられており、効果的に対応の優先順位をつけられたインシデント	・不適切なサービス提供 ・提供されているサービスに対する誤った優先順位 ・影響を正しく理解されていないインシデントと、それによる対応の遅れ及びビジネスへの重大な影響 ・提供されているITサービスに対する異なる解釈と誤解

コントロール設計のテスト
・サービスカタログやサービスのポートフォリオを作成し、レビューし、調整するためのプロセスが存在するかどうかを調査して、それを確認する。 ・サービスカタログやポートフォリオが利用可能で最新の状態を保つようにするための管理プロセスの存在を確認する。 ・サービスカタログやポートフォリオのプロセスを閲覧して、それが定期的にレビューされていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS1.3 サービスレベル・アグリーメント 顧客側の要件とITの提供能力に基づいて、すべての重要なITサービスについてSLAを策定し、合意を得る。ここでは、顧客の確約事項、サービスサポート要件、利害関係者により承認されたサービスの量的/質的測定指標、資金の調達、および商業上の調整(該当する場合)、そしてSLA自体の監督業務を含む役割と実行責任が定められる。検討すべき事項は、可用性、信頼性、成果、容量計画、サポートレベル、継続計画、セキュリティ、および需要面での制約である。	・事業目標と整合的な、サービスの責任とITの達成目標 ・サービス提供の適切な理解と整合性による、サービス品質の向上 ・現実の必要性と優先順位に基づいてITサービスを効率的に展開していることによる、サービス効率の向上と費用の減少	・顧客のサービス要求への不適合 ・サービス提供のための資源の非効率的で効果的でない利用 ・重大なサービスインシデントを特定し対応することができない状態

コントロール設計のテスト

- 利害関係者がSLAおよびそのフォーマットと内容に含まれているものに合意し、記録し、伝達しているかどうかを調査して、それを確認する。
- SLAの内容のフォーマットを閲覧して、そこに除外事項、商業協定、およびOLAが含まれていることを確かめる。
- SLA管理プロセスを閲覧して、それがSLAを（定性的かつ定量的に）測定し、SLAの達成目標をモニタリングしていることを確かめる。
- 承認と適切な署名があるかどうか、SLAを調査する。
- SLAレビュープロセスを観察しレビューして、それが十分かどうかを評価する。
- SLAの改善と調整のためのプロセスが、顧客の要求とビジネス要件に対するパフォーマンス・フィードバックと変更に基づいていることを確かめる。
- サービスがSLAで文書化されないようになっているかどうかを主要な担当者に尋ねる。

コントロール目標

DS1.4 オペレーショナルレベル・アグリーメント
SLAを最適な形で満足するサービスの技術的提供方法を、OLAにおいて明記する。OLAは、技術プロセスをサービスプロバイダに理解し易い形で規定し、必要に応じて、複数のSLAに対応する可能性がある。

価値のドライバー

- SLAと整合的であり、したがって、ビジネスの必要性とも整合的であるような運用サービス
- 標準化およびサービス要件との整合性による、運用のための資源の最適化
- 資源の最適化された利用と少ないサービスインシデントによる、費用の減少

リスクのドライバー

- 提供サービスのビジネス要件への不適合
- インシデントをもたらすようなサービスについての技術的理解におけるギャップ
- 運用のための資源の非効率的で費用のかかる利用

コントロール設計のテスト

- OLAを策定し、管理し、レビューし、調整するためのプロセスが定義されているかどうかを調査して、それを確認する。
- SLAを閲覧して、SLAでの技術要件をOLAでサポートしていることを確かめる。
- OLAの代表的なサンプルを入手して、サービスの提供についての運用可能で最適な定義をOLAが含んでいるかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
DS1.5 サービスレベル達成状況のモニタリングと報告 規定されたサービスレベルの成果基準を継続的にモニタリングする。サービスレベルの達成状況に関する報告は、利害関係者が容易に理解できる形式で提出する必要がある。モニタリング結果の統計データを分析、処理し、サービス全般のほか、個々のサービスにおけるマイナス/プラス要因を特定する。	・信頼できる情報に基づいてサービスレベルパフォーマンスをモニタリングできるユーザ ・企業内で周知されているITサービスの価値 ・関連する当事者間での一貫した伝達	・組織にとって重要な、定義された測定手段の欠如 ・サービスにおける識別されていない問題 ・サービスの品質によらず情報が無いことにより不満を抱いているユーザ

コントロール設計のテスト
・サービスレベル・パフォーマンスをモニターすることに責任を持つ主要な担当者へのインタビューを通じて、報告基準を判断する。 ・SLAパフォーマンス報告のサンプルを入手して、分布を検証する。 ・サービスレベル・パフォーマンスの予測と傾向についてのレビューを閲覧する。

コントロール目標	価値のドライバー	リスクのドライバー
DS1.6 サービスレベル・アグリーメントと請負契約の見直し 組織内外のサービスプロバイダと協力してSLAとその請負契約（UC）を定期的に見直し、契約内容が有効かつ周辺動向に則した内容であり、要件の変化が反映されることを確実にする。	・変化するビジネスの必要性と整合的であるように提供されたITサービス ・既存のサービス合意で特定され修正された弱点	・契約が失効していることによる、商業的および法的な要件への不適合 ・変更された要件に合致していないサービス ・サービスの連携が取れていないことによる、財務上の損失とインシデント

コントロール設計のテスト
・SLAを閲覧し、請負契約を比較し、その有効性および変化に追随しているかどうかを確認する。 ・SLAの文書化要件のウォークスルーを入手する。 ・SLAと請負契約をレビューして、事業目標との整合性が定期的に評価されていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
- ビジネス部門とIT部門を代表する上級マネジメント層に、SLAフレームワークの設計と承認への関与について尋ねる。
- SLAの目標達成をサポートし測定するためのパフォーマンスの判断基準が正式化されているかどうか、および目標の達成をモニタリングし報告するためのプロセスがあるかどうかを主要な担当者に尋ねる。
- SLAの内部と外部のパフォーマンスを調査して、期待されたSLA要件と実際の結果が整合的かどうか比較する。
- ITサービスの達成目標が事業目標と整合的であり、期待とパフォーマンスの測定を正式に定義していることを確かめる。
- サービス記録を閲覧して、パフォーマンスが良好でない理由を究明して、パフォーマンス改善プログラムが実施されていることを確かめる。

- パフォーマンスの履歴を分析して、先に行われたサービス改善のコミットメントと照らし合わせて結果が追跡されていることを確認する。
- 利害関係者がSLAおよびそのフォーマットと内容に含まれているものに合意し、記録し、伝達しているかどうかを主要な担当者に尋ねる。
- SLAの内容のフォーマットを閲覧して、そこに除外事項、商業協定、およびOLSが含まれていることを確かめる。
- 過去および現在のSLAのサンプルについて、その内容に以下のものが含まれていることを確認する。
  - サービスの定義
  - サービスの費用
  - 定量化可能な最低限のサービスレベル
  - IT 部門からのサポートのレベル
  - 成長のための可用性、信頼性、可能性
  - 合意内容のあらゆる部分に対する変更手続
  - 継続計画
  - セキュリティ要件
  - サービスプロバイダとユーザとの間の書面による正式に承認された合意
  - 有効期間と新規の期間のレビュー/更新/打ち切り
  - サービスに対するパフォーマンス報告と支払いの内容と頻度
  - 過去、業界、ベストプラクティスと比較して現実的な料金
  - 料金の算定
  - サービス改善のコミットメント
  - ユーザとプロバイダの正式な承認
- しかるべきユーザがSLAのプロセスと手続に注意しており理解していることを確かめる。
- SLAを閲覧して、OLAと請負契約が、SLAの技術要件をサポートしており、最適な方法で提供されていることを確かめる。
- SLAのサンプルを選び、不適切なサービス提供、とりわけパフォーマンスの悪化を解決するための手続が含まれており、それに合致していることを確かめる。
- サービスカタログを閲覧して、すべてのサービスが適切に定義されていることを確かめる。
- 追加的な費用のかかるITサービスが定義され文書化されているかどうかを調査して、それを確認する。
- ビジネスプロセスオーナが、自らのビジネスプロセスをサポートするITサービスについての知識を持っているかどうかを確認する。
- ビジネスプロセスとそれをサポートするインフラストラクチャやITサービスを特定する文書で利用可能なものがあったらすべて閲覧して、紐付けが正確かつ完全かどうかを確認する。これはたとえば、組織図、ビジネスの命令系統などへの紐付けを比較することで達成することができる。
- ビジネスプロセスオーナとITサービスオーナがITサービスのビジネスプロセスへの紐付けに合意したかどうかを、ビジネスプロセスオーナとITサービスオーナに尋ねる。
- 提供されているITサービスへの満足度についてビジネスプロセスオーナとユーザに尋ね、潜在的に弱い分野を特定する。そのような質問は、個別にすることもできれば、匿名のアンケート調査で行うこともできる。
- ITサービスエリアとビジネスプロセスとの紐付けに関連する文書を閲覧して、紐付けの運用上の側面（たとえば、SLAが適切かどうかを検証すべきである）があるかどうかを確認する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- 同様の組織や適切な国際基準/業界で認知されているベストプラクティスと照らし合わせて、SLAのベンチマークを取る。
- サービスレベルの期待と提供されているサービスとの間のギャップが存在するかどうかを、質問および文書化された係争と料金の割引のレビューを通じて確認する。
- サービスが頻繁に追加料金を発生させたり基本料金を超過したりするかどうかを確認する。
- サービスレベルの不全がエスカレートされ、タイムリーに解決されているかどうかを確認する。
- サービスカタログが最新の状態を保っており、ビジネスの到達目標と整合しているかどうかを確認する。

- 提示されているサービス改善が、費用便益分析との比較で十分かどうかを評価する。
- 期待されたサービスにおけるギャップに適切に優先順位をつけてあり、サービスの特性とビジネス要件に基づいてサービスを管理するというコントロール要件に対処していることを判断する。
- 情報サービスのプロバイダとユーザとの間の関係を記述し、調整し、伝達する規定の十分性を評価する。
- プロバイダが将来の改善へのコミットメントに合致する能力が十分かどうかを評価する。
- SLAと契約が現状に即しており、事業目標と整合しているという保証をサービスレベル・フレームワークで提供しているかどうかを、主要な管理担当者に尋ねる。
- マネジメント層が満足度の成果を確かなものとするために、個別のサービスパフォーマンスの達成についての報告が適切に用いられているかどうかを確認する。
- マネジメント層が是正措置を取るために、直面したすべての問題についての報告が適切に用いられているかどうかを確認する。
- 提供されているサービスを評価して、オペレーションの合意事項がSLAと整合しているかどうかを確認する。
- 報告されたSLA情報のカテゴリから選び出したものについて、サービス提供に一貫性を欠く部分が存在するかどうかを確認する。
- 現在のサービスレベルプロセスと実際の合意事項によって、ユーザの満足度を評価する。
- サービスレベルの測定基準を評価して、すべての関連当事者間の情報伝達のフローの有効性を判断する。
- SLAをレビューして、義務が定義されており、それに合致していることを確かめるような定性的かつ定量的な規定を確認する。
- サービスレベル報告に対するマネジメント層の継続的なレビューと是正措置を評価する。
- 財務上の損失が、サービスの品質が不十分なことを反映しているかどうかを確認する。
- 変更要求、ネットワーク計画、サーバの文書、インシデント記録、タイムシート、その他の伝達手段をレビューして、照合することによって、サービスカタログの網羅性を確かめる。
- 日々の職務と責任についてITサービスのリーダーにその職務がITインフラストラクチャに対する十分なカバレッジを提供しているかどうかを尋ねて、確認する。
- データセンタの視察、資産台帳、ネットワークダイアグラム、その他のインフラストラクチャの棚卸の成果によって、議論の結果の裏づけを取り、ITリーダーに関連していないインフラストラクチャを特定する。
- 資産台帳、ネットワークダイアグラム、その他のインフラストラクチャの棚卸を閲覧して、ITサービスのエリアに割り当てられていない資産の比率を確認する。
- 提供されているサービスの観点からそのような資産の重大性を文書化する。
- ITサービスとビジネスプロセスを特定する文書を閲覧して、割り当てられていないITサービスのエリアの度合いを確認する。
- 影響を受けるビジネスプロセスの観点から、そのようなサービスのエリアの重大性を文書化する。

DS2 サードパーティのサービスの管理

サードパーティが提供するサービスがビジネス要件を確実に満たすようにするには、効果的なサードパーティの管理プロセスが必要である。このプロセスでは、サードパーティとの合意のもと、役割、実行責任、および要求事項を明確に定義し、このような合意事項の有効性とコンプライアンスをレビューおよびモニタリングする。サードパーティが提供するサービスを効果的に管理することで、不適格なサービスプロバイダに起因するビジネスリスクを最小限に抑えることができる。

コントロール目標	価値のドライバー	リスクのドライバー
DS2.1 すべてのサービスプロバイダとのリレーションシップの特定 すべてのサービスプロバイダのサービスを特定し、サービスプロバイダのタイプ、重要性、および依存度に従って分類する。技術的および組織的な関係を正式に文書化して管理する。この文書には、サービスプロバイダの役割と実行責任、目標、期待される成果物、および代表者の信用証明が含まれる。	・サービスプロバイダの意思決定をサポートするための、サービスプロバイダの全体像の集中的な把握 ・将来の調達のために特定された好ましいサービスプロバイダ ・重大なサービスプロバイダに集中させている、サービスプロバイダ管理のための資源	・重要かつ重大であるにもかかわらず、特定されていないサービスプロバイダ ・サービスプロバイダを管理するための資源の非効率的かつ効果的でない利用 ・不明確な役割と責任と、それによる意思伝達の齟齬、不十分なサービス、費用の増加

コントロール設計のテスト

- サービスプロバイダとのリレーションシップの台帳が維持されているかどうかを調査して、それを確認する。
- サービスプロバイダとのリレーションシップの基準を入手して、サービスプロバイダのタイプ、重要性、および重大性による分類の合理性と網羅性を検証する。
- サービスプロバイダの分類のスキームが、契約サービスの性質に基づいてすべてのサービスプロバイダのリレーションシップを分類するのに十分なほど詳細であるかどうかを確認する。
- サービスプロバイダの選定/却下についての過去の履歴を保存しており利用しているかどうかを検証する。
- サービスプロバイダのリレーションシップの台帳を閲覧して、既存のサービスプロバイダに対するモニタリングの基礎を提供するのに十分なほど詳細であり、最新の状態を保っており、適切に分類されていることを確かめる。
- サービスプロバイダとの契約、SLA、および他の文書の代表的なサンプルを閲覧して、それがサービスプロバイダの台帳に対応していることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS2.2 サービスプロバイダとのリレーションシップ管理 サービスプロバイダごとに正式なリレーションシップ管理プロセスを確立する。リレーションシップオーナは連携して、顧客とサービスプロバイダにかかわる問題に取り組み、SLAなどにより信頼と透明性に基づく良質なリレーションシップの維持に努める必要がある。	・企業全体の達成目標(ビジネスとITの両方)をサポートするリレーションシップの促進 ・効果的かつ効率的な意思伝達と問題解決 ・顧客とサービスプロバイダとの間の明確な責任の所在	・リレーションシップに反応しなかったりコミットしていなかったりするサービスプロバイダ ・未解決の問題 ・不十分なサービス品質

コントロール設計のテスト
・正式化された役割と責任の証拠に関してサービスプロバイダの文書を閲覧して、サービスプロバイダ管理の役割が文書化され組織内で伝達されているかどうかを確認する。 ・正式な契約の必要性、契約内容の定義、および、契約が作成され、維持され、モニタリングされ、必要に応じて再交渉されることを確かにするという責任をオーナーやリレーションシップ管理者に割り当てることに対処するためのポリシーが存在するかどうかを確認する。 ・サービスプロバイダ管理の役割の割り当てが合理的であり、リレーションシップを効果的に管理するのに要するレベルと技能に基づいているかどうかを評価する。

コントロール目標	価値のドライバー	リスクのドライバー
DS2.3 サービスプロバイダにかかわるリスクの管理 サービスプロバイダが安全かつ効率的な方法を使用し、継続的なサービスを提供する上で想定されるリスクを特定し、低減する。契約が、法令要件に従い一般的なビジネス標準に準拠していることを確認する。リスクマネジメントではさらに、秘密保持契約(NDA)、エスクロー契約(訳注:サードパーティ預託契約サービス提供者の破産等に備えて、ソースプログラム等をサードパーティに預託し、事由の発生時に、委託者に提供する契約)、サービスプロバイダの存続能力、セキュリティ要件へのコンプライアンス、代替サービスプロバイダ、SLA未達と超過達成などについて検討すべきである。	・法律と契約の要件の遵守 ・インシデントと潜在的な損失の減少 ・低リスクで適切に管理されているサービスプロバイダの特定	・規制と法律の義務の遵守違反 ・セキュリティおよびその他のインシデント ・サービスの中断による、財務上の損失とレピュテーション(評判)ダメージ

コントロール設計のテスト

- サービスプロバイダとの契約を果たすことができないことによるリスクが定義されているかどうかを調査する。
- サービスプロバイダとの契約を定義するときに契約上の救済措置のことを検討したかどうかを調査する。
- レビューの証拠のために契約書を閲覧する。
- サービスプロバイダのリスクを特定しモニタリングするためのリスク管理プロセスが存在するかどうかを主要な担当者に尋ねる。
- ベンダの調達と選定のプロセスの中で、また、ベンダと組織内の管理者との間で、独立性を要求するポリシーが存在するかどうかを確認する。

コントロール目標

DS2.4 サービスプロバイダの成果のモニタリング

サービス提供状況のモニタリングプロセスを確立する。これにより、サービスプロバイダが現行のビジネス要件を満たすと同時に、継続的に契約合意とSLAを厳守し、その成果が、市場の状況および他のサービスプロバイダと比較した場合の優位性があることを確認する。

価値のドライバー

- サービスレベルにおける不履行事項のタイムリーな発見
- 業務委託契約の利益の実現
- コントロールされたコスト
- 費用のかかる係争と訴訟の可能性の回避

リスクのドライバー

- 発見されないサービス低下
- 費用とサービスの品質を追及する能力の欠如
- サービスプロバイダの選定を最適化する能力の欠如

コントロール設計のテスト

- サービスプロバイダの請求書のサンプルを選び出して、それがサービス契約で特定されているように、契約しているサービスに課金しているかどうかを確認し、内部、外部、および業界における様々な同等のパフォーマンスと比較して料金が合理的かどうかを評価する。
- サービスプロバイダのサービス報告のサンプルを閲覧して、サービスプロバイダが、合意済みの成果基準について定期的に報告しているか、またパフォーマンスの報告が客観的で測定可能で、定義されたSLAとサービスプロバイダの契約と整合的であるかどうかを確認する。

コントロール目標の達成をテストするために以下のステップを踏む。

- サービスプロバイダのサンプルについて、サービスプロバイダの記録が、サービスプロバイダとの間のすべてのリレーションシップを特定し分類するために用いる、定義された分類スキームと整合的であるかどうかを評価する。
- サービスプロバイダのリレーションシップの判断基準の一覧を入手してその網羅性を検証し、サービスプロバイダの記録を、すべてのサービスプロバイダのリレーションシップを特定し分類するために用いる分類スキームと照らし合わせてレビューする。サービスプロバイダのタイプ、提供されているサービスの重要性、重大性が文書化されているかどうか評価する。
- サービスプロバイダの台帳を入手して、サービス契約のサンプルの閲覧を通じて、データの正確性を確かめる。
- サービスプロバイダの台帳を入手して、データの正確性を確かめる。サービスプロバイダとのリレーションシップの判断基準の変更を要するような、組織の変更やITのランドスケープの最近の変更に対して考慮すべきである。
- サービスプロバイダの文書が、コミュニケーション方法、サービスの優先順位づけ、エスカレーション手続、最低限のサービスレベル、および運用上の目標を特定するのに十分なほど詳細であるかどうかを確認する。
- サービスプロバイダとユーザ組織との間の責任を文書で明確に線引きしているかどうかを確認する。
- サービスプロバイダの文書が集中的に管理され維持されているかどうか、文書を定期的にレビューして更新するためのプロセスが存在するかどうかを確認する。
- サードパーティ契約のそれぞれに対して詳細なレビューを実施して、情報サービスのプロバイダとユーザとの間のリレーションシップを調整し、伝達するための規定を含む、義務を裏付けるような定性的かつ定量的な規定が存在するかどうかを確かめる。
- マネジメント層がサービスプロバイダの報告を定期的にレビューするためのポリシーが存在するかどうかを確認し、マネジメント層のレビューの証拠のためにサービスプロバイダの報告のサンプルを選ぶ。
- サービスプロバイダのインシデント報告を入手して存在を確かめ、重大性に関する合意済みのレベルにしたがってインシデントが分類されエスカレートされているかどうか、および解決するまでそれが組織内で追跡され伝達されているかどうかを確認する。報告されたインシデントには、サービスプロバイダの管理部門とサービスのユーザへの伝達が含まれているべきである。
- 達成目標と期待されたサービスレベルが現在のビジネス要件をサポートし続けており、提案されている変更がサービスプロバイダに明確に伝達されていることを確かなものとすべく、到達目標と期待されたサービスレベルが定期的にレビューされていることを検証する。
- サービスプロバイダの台帳を閲覧してリレーションシップ管理者の任命に関して調べ、サービスプロバイダの伝達プロセスの証拠を入手して閲覧する。
- 契約を入手してレビューして、サードパーティレビューに関連する条項が存在するかどうか調べ、マネジメント層がそのようなレビューからの報告を入手してレビューしたかどうかを確認する。
- サービスプロバイダのサンプルについて、入手できる文書を閲覧して、サービスプロバイダのリスクが検討され、特定されたリスクに対処したり低減したりしたかどうかを確認する。
- サービスプロバイダのリレーションシップのサンプルについて、サービスプロバイダとの契約の中で以下に触れているかどうかを確認する。
  - セキュリティ要件
  - 機密保持の保証
  - アクセス権と監査権
  - 正式な管理と法的な承認
  - サービスを提供する法的主体
  - 提供されるサービス
  - 定性的かつ定量的な SLA
  - サービスの費用とサービスに対する支払いの頻度
  - 問題解決プロセス

  - パフォーマンス未達成のペナルティ
  - 契約解消プロセス
  - 改変プロセス
  - サービスの報告—内容、頻度、分布
  - 契約期間中の契約当事者の間の役割分担
  - サービスがベンダによって提供されるという継続性の保証
  - サービスのユーザとプロバイダとの間の伝達プロセスと頻度
  - 契約期間
  - ベンダに提供されるアクセス権のレベル
  - 規制の要件
- サービスプロバイダのサンプルについて、組織にとっての重大性のためにサービスが評価されているかどうかを確認し、組織への継続的なサービスを確かにすべく、サービスプロバイダとの契約で、サービスプロバイダによるコンティンジェンシープランを含むサービスの継続性に触れているかどうかを確認する。
- サービスプロバイダのリレーションシップのサンプルについて、弁護士とマネジメント層がサービスプロバイダとの契約を承認したかどうかを確認する。
- サービスプロバイダの請求書のサンプルを選び出して、それがサービス契約で特定されているように、契約しているサービスに課金しているかどうかを確認し、内部、外部、および業界における様々な同等のパフォーマンスと比較して料金が合理的かどうかを評価する。
- サービスプロバイダのサービス報告を閲覧して、サービスプロバイダが、合意済みの成果基準について定期的に報告しているか、またパフォーマンスの報告が客観的で測定可能で、定義されたSLAとサービスプロバイダの契約と整合的であるかどうかを確認する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- ユーザとITマネジメント層に質問し、同様の規模の組織と同一業界内の組織に対して組織のベンチマークをとることを通じて、サービスプロバイダ台帳に含まれていないサービスプロバイダとのリレーションシップを特定する。
  以下のようなサービスプロバイダのリレーションシップを検討する。
  - PBX のサービスプロバイダ
  - 紙とフォームのサプライヤ
  - 保守サポートサービスプロバイダ
  - オフサイトのデータ貯蔵とホットサイトのサービスプロバイダ
  - データ処理を提供するサービス組織（ASP、コロケーションなど）
  - 外部のソフトウェア開発業者と品質保証
- サービスプロバイダ管理部門に質問して、サービスプロバイダのリレーションシップと契約サービスの性質について熟知しているかどうかを確認する。
- サービスプロバイダの、対象範囲外の請求書のサンプルを閲覧して、超過分のレビューと承認にサービスプロバイダ管理部門が関与しているかどうかを確認する。
- サービスプロバイダのサンプルについて、サービスプロバイダの報告したパフォーマンスの測定指標を入手して、合意済みのパフォーマンス目標からの逸脱に関してレビューする。サービスプロバイダ管理部門が逸脱および逸脱に対して取った行動の合理性に注意していたかどうかを確認する（行動計画の策定、パフォーマンス未達成に対するサービス料金のペナルティなど）。
- サービスプロバイダのリレーションシップのサンプルについて、サービスのレベルが記述されている契約上の義務と同等かどうかを確認する。サービスプロバイダのリレーションシップの変化に関して、リスク評価が更新されたかどうか、サービスプロバイダとの契約が適切に改変されたかどうかを確認する。
- サービスプロバイダが報告したパフォーマンスの測定指標のサンプルを閲覧して、パフォーマンス目標を一貫して達成しなかったようなケースを特定する。
- マネジメント層がパフォーマンスの不全を特定して評価したかどうか、および、評価が実施されたり、リレーションシップを見直したり、リレーションシップを変える必要を評価したかどうかを確認する。
- 組織に最大の影響を及ぼすサービスプロバイダのリレーションシップに関して、契約サービスの回復や副次的な供給源の確保のためのコンティンジェンシープランが存在するかどうかを確認する。

- サービスプロバイダに対する第三者の評価（SAS 70、ISA 402、監査報告など）または監査報告を利用できるかどうか、およびマネジメント層がその報告を受け取りレビューしたかどうかを確認する。報告されているコントロールの不備に関して、マネジメント層がサービスプロバイダと共にその不備を議論したかどうか、行動計画を実施したかどうかを確認する。過去およびそれに引き続く報告のレビューを通じて、サービスプロバイダがコントロールの不備を迅速に修復したかどうかを確認する。
- 主要なサービスプロバイダが年次リスク評価と監査計画のプロセスに含まれているかどうかを確認する。
- サービスプロバイダが報告したパフォーマンスの測定指標のサンプルを閲覧して、パフォーマンス目標を一貫して達成しなかったようなケースを特定する。
- マネジメント層が、パフォーマンスの不全を特定し評価したかどうか、是正措置と継続的なモニタリングのためのプロセスが実施されているかどうかを評価する。
- サービスプロバイダのサンプルについて、サービスプロバイダの報告したパフォーマンスの測定指標を入手して、合意済みのパフォーマンス目標からの逸脱に関してレビューする。
- サービスプロバイダ管理部門が、逸脱および逸脱に対して取った行動の合理性に注意しているかどうかを確認する（行動計画の策定、パフォーマンス未達成に対するサービス料金のペナルティなど）。

DS3 性能とキャパシティの管理

IT資源の性能とキャパシティを管理するには、IT資源の性能とキャパシティを定期的にレビューするプロセスが必要である。このプロセスには、作業負荷、ストレージ、および緊急時の要件に基づいて今後のニーズを予測することが含まれる。このプロセスにより、ビジネス要件を支援する情報資源の継続的可用性が保証される。

コントロール目標	価値のドライバー	リスクのドライバー
DS3.1 性能とキャパシティの計画策定 IT資源の性能とキャパシティのレビュー計画の策定プロセスを確立する。これにより、SLAで規定されている合意された作業負荷を処理するための費用的に妥当な性能とキャパシティを保証する。性能とキャパシティの計画では、適切なモデル化技法を用いて、現状、および予測されるIT資源の性能、キャパシティ、およびスループットのモデルを作成することが必要である。	・ オーバーヘッドコストを回避することによる効率的な資源管理 ・ 内部のベンチマーキングを通じて達成される、最適化されたシステムパフォーマンス ・ 将来のパフォーマンスとキャパシティの要件に対する予測 ・ 改善事項を特定するために組織の範囲を通じて、また外部において、キャパシティのベンチマークを取る能力	・ キャパシティ不足による予期せぬインシデント ・ 資源のキャパシティとパフォーマンスに関する積極的な計画が無いことによるシステム可用性の不全 ・ パフォーマンスとキャパシティの計画が陳腐化していることによる、ビジネス要件への不適合

コントロール設計のテスト
・ パフォーマンスとキャパシティの計画を策定し、レビューし、調整するためのプロセスやフレームワークが定義されているかどうかを調査して、それを確認する。 ・ パフォーマンスとキャパシティの計画の策定に関与した主要な担当者へのインタビューを通じて、キャパシティ計画の策定中に適切な要素が検討されたかどうかを尋ねる（顧客の要求、ビジネス要件、費用、アプリケーションパフォーマンス要件、拡張性の要件など）。 ・ パフォーマンスとキャパシティの計画が作成され維持されているかどうかを調査して、それを確認する。 ・ 根拠となる文書を閲覧して、利害関係者の関与を確かめ、また、その計画が記録され最新の状態を保っていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS3.2 現状の性能とキャパシティ 現状のIT資源の性能とキャパシティを評価する。これにより、合意されたサービスレベルに照らし合わせて十分な性能とキャパシティが提供されているかどうかを確認する。	・ IT資源の効率的かつ効果的な管理 ・ パフォーマンスとキャパシティの計画の改善 ・ パフォーマンスとキャパシティに関する積極的な計画によって最適化されたシステムパフォーマンス	・ ビジネスの中断 ・ SLAへの不適合 ・ ビジネス要件への不適合 ・ キャパシティの測定方法が不明なことによる、サービス提供へのコミットメントの過不足

コントロール設計のテスト

- 以下の要因に基づいてしかるべきIT資源に対してシステムモニタリングソフトウェアが導入されているかどうかを調査して、それを確認する。
  - IT 資源のビジネスでの重大性
  - SLA で特定された要件
  - パフォーマンスやキャパシティの問題に直面する IT 資源の可能性や歴史的な傾向
  - パフォーマンスやキャパシティの問題からの業務/財務/法規制への影響
- ビジネス要件とSLAに基づいてIT資源に対して基準値が確立し導入されているかどうかを確認する。基準値の例としては、以下のものが含まれる。
  - 回線の 80 パーセントが通話中であるときに、コールセンタがフリーダイヤルの回線を追加する
  - ハードドライブが一定のキャパシティレベルに到達するときに、サーバのディスクスペースを追加する
- 不十分なパフォーマンスによるインシデントがどのように特定され追跡されているかを判断する。
- トラブルチケットを入手して、特定されたトランザクションをシステムを通じて追跡して、適切な追跡調査が生じたかどうかを確認する。
- 組織でのSLAの提供に責任を持つ主要な担当者に尋ねて、IT資源のキャパシティとパフォーマンスの測定指標をどのようにモニタリングし、追跡し、報告しているかを確認する。
- 主要な利害関係者に提供される運用報告をレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
DS3.3 将来の性能とキャパシティ IT資源の性能とキャパシティの予測を定期的に実施する。これにより、キャパシティ不足または性能の低下に起因するサービス中断のリスクを最小限に抑え、IT資源の再配置が必要になるような余剰能力が存在しないかを検証する。作業負荷の傾向を識別し、かつ予測値を決定し、性能とキャパシティの計画に取り込む。	・IT資源の最適化された利用 ・ITインフラストラクチャに対する予測されたビジネス需要 ・パフォーマンスとキャパシティの計画の改善	・利用されているサービスレベルがビジネスに提供されていない状態 ・IT資源の不全によるシステムの可用性の欠如 ・システムが対応できない高い処理負荷

コントロール設計のテスト

- 以下を実施するのにふさわしいツール、技法、プロセスの利用を（主要な担当者にインタビューし、プロセスの文書と報告書を閲覧することによって）確認する。
  - 実際のパフォーマンスとキャパシティを測定する
  - キャパシティの利用状況、帯域（ネットワークと回線の活用上の報告）、およびパフォーマンスの報告のレビューを実施する
  - 資源に対する予測需要と実際の需要とを比較する
  - マネジメント層が、予測レポートをレビューし、差異について議論することに関与する
- 実際のIT資源のパフォーマンスを期待されたキャパシティとパフォーマンスに照らし合わせて測定する文書を閲覧する。
- モデルの予測を改訂する際に、ベースライン/モデルと実際のものとの間の差異をどのように用いているかを判断し、分析が定期的にタイムリーな方法で実施されていることを確かめる。
- キャパシティ計画プロセスを熟知しているかどうか、および、アプリケーション、サーバ、またはその他のIT資源への変更を要するような新しいビジネス要件に対してどのように注意を喚起されるかを、主要な担当者に尋ねる。
- 予測モデルがIT資源の計画と調達を調整するためのプロセスに影響するとき、主要な担当者にそのプロセスを確認する。
- パフォーマンスとキャパシティの予測値のレビューによって必要になる定期的な調整に関して、SLAとOLAの代表的なサンプルとキャパシティ計画をレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
DS3.4 IT資源の可用性 標準作業負荷、緊急事態、ストレージに関する要件、およびIT資源のライフサイクルなどの面を考慮して、必要となるキャパシティと性能を提供する。作業の優先順位付け、フォールトトレランスメカニズム、資源の割り当て実行などへの対応を講じる。マネジメント層は、緊急時対応計画において確実に個々のIT資源の可用性、キャパシティ、および性能について適切に対応可能であることを確認する必要がある。	・IT資源の効果的な活用 ・ビジネス要件に合致したサービスレベル ・IT資源に対する効果的な可用性管理	・IT資源の不全によるシステムの可用性の欠如 ・ITサービスの可用性と有用性を予測する能力の欠如 ・ITサービスの予期せぬ停止

コントロール設計のテスト

- ベンダ要件を入手し、レビューし、実施するためのプロセスについて主要な担当者に尋ね、現在のキャパシティとパフォーマンスの能力が、ベンダ要件に取り込まれていることを確かめる。
- ベンダの文書を閲覧して、それがベンダ要件及び最小かつ最適なIT資源のキャパシティとパフォーマンスについての推奨内容を特定していることを確かめる。
- パフォーマンスとキャパシティの既知のギャップについてマネジメント層に尋ねる。
- この情報を現在のパフォーマンスモニタリングおよび予測されているキャパシティ要件と比較する。
- ITアプリケーションでサポートすべき活動について優先順位をつけた一覧表があるかどうか確かめる。
- キャパシティ計画が是正措置によって更新されていることを確かめる。
- 計画プロセス（PO2–PO3）が、更新されたキャパシティ計画をインプットとして取り込んだかどうかを確かめる。
- 是正措置が変更管理プロセスによって正式に処理されていることを確かめる。
- パフォーマンスとキャパシティの問題点を是正するためのプロセスについて、主要な担当者に尋ねる。
- トラブルチケットを入手して、特定されたトランザクション（システムの追加、処理負荷の代替サーバへのシフトなど）を、システムを通じて追跡して、適切な是正措置が実施されたかどうかを確認する。
- IT資源のパフォーマンスの問題点に関連するエスカレーション手続を調査する。
- 緊急の問題が最近になって生じたかどうかを主要な担当者に尋ね、手続の遵守を検証し、その手続が有効かどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS3.5 モニタリングと報告 IT資源の性能とキャパシティを継続的にモニタリングする。収集データは次の2つの目的で使用される。 ・ ITの現行の性能を維持および調整し、障害からの回復、緊急時対応、現状および予定されている作業負荷、ストレージに関する計画と資源調達などの課題に対応する。 ・ SLAでの規定に従い、ビジネス部門に対し提供サービスの可用性の報告を行う。 すべての例外報告に対して、是正措置に関する推奨案を追記する。	・ 効果的なサービス提供に影響する問題点の特定 ・ 期待のギャップを特定している、ベースライン化されたサービスレベル ・ サービス提供を改善するためのIT資源の活用の増加	・ パフォーマンスのモニタリングの欠如 ・ 期待された品質に合致しないサービス ・ タイムリーに特定されず、サービスの品質に影響するような逸脱

コントロール設計のテスト

・ マネジメント層を支援するためにデータを収集するためのプロセス（IT資源の要件、キャパシティ、可用性、活用、資源配分についての提言、優先順位付けなど）が確立されているかどうかを、関与している主要な担当者に尋ねる。
・ モニタリングと報告の活動が正式化され一体化されているかどうかを、マネジメント層へのインタビューを通じて尋ねる。
・ キャパシティとパフォーマンスの活動に対するモニタリング結果と報告結果のフィードバックを追跡する。
・ キャパシティ報告がIT戦略計画と予算策定プロセスに取り込まれているかどうかを調査して、それを確認する。

コントロール目標の達成をテストするために以下のステップを踏む。
・ IT資源のパフォーマンスとキャパシティの計画についての文書を閲覧して、計画プロセスが以下を行っているかどうかを特定する。
  –主要な測定指標の要素は SLA から導き出される必要がある
  – ビジネス要件、技術要件、費用の検討事項を考慮に入れる
  – 現在および予測されているパフォーマンスとキャパシティのモデルを含める
  – 利害関係者からの承認の文書化を伴う
  – IT に対する継続的なモニタリングと報告を伴う
・ IT資源の稼働時間と活用状況の報告を閲覧して、現在のIT能力が十分かどうかを確認する。
・ 競合企業がパフォーマンスとキャパシティの予測にどう対処しているのかを特定するためにベンチマーキングスタディが実施されているかどうかを調査して、それを確認する。
・ 以下のエリアにおけるIT資源の可用性についての情報を提供する文書を閲覧する。
  – データ貯蔵の要件と現在のキャパシティ
  – 障害に対する許容度と冗長性
  – 可用性、キャパシティ、およびパフォーマンスの問題点に対処するための IT 資源の再配分
・ IT資源のパフォーマンス、キャパシティ、配分を管理するためのモニタリングプロセスが存在し報告されているかどうかについて、主要な担当者に尋ねる。
・ パフォーマンス報告書を閲覧して、適切な情報がマネジメント層に定期的に提供されていることを確かめる。
・ パフォーマンスと可用性の計画が予算策定プロセスおよび情報アーキテクチャの改善のために用いられていることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- インシデント報告を閲覧して、キャパシティとパフォーマンスの問題点によってサービス停止が常に生じているかどうかを主要な担当者に尋ねる。
- IT資源の保守に責任を持つ主要な担当者に、キャパシティとパフォーマンスに影響するようなビジネス要件とSLAへの変更が知らされているかどうかを尋ねて、確認する。

DS4 継続的なサービスの保証

継続的なITサービスを提供するには、IT継続計画の作成、保守、およびテスト、遠隔地のバックアップ保管施設の確保および定期的な継続計画に関するトレーニングの実施が必要である。効果的なサービス継続プロセスにより、主要なITサービスの中断の可能性と、このような中断が主要なビジネスの機能とプロセスに及ぼす影響を最小限に抑えることができる。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.1 IT継続フレームワーク 一貫したプロセスで全社的な事業継続管理を支援する、IT継続フレームワークを作成する。このフレームワークの目的は、求められるインフラストラクチャの復旧能力の決定を支援し、災害復旧計画とIT緊急時対応計画の作成を促進することである。このフレームワークでは、内外のサービスプロバイダ、その管理者と取引顧客の役割、担当作業、および実行責任を含む、継続管理に必要な組織構造、そして災害復旧計画とIT緊急時対応計画を文書化、テスト、および実施する際のルールと体制を規定する計画プロセスに対応する必要がある。また計画には、重要な資源の特定、主な依存関係の記述、その資源の可用性のモニタリングと報告、代替処理手続、およびバックアップと復旧に関する原則などの項目も規定する必要がある。	・ IT全体を通じて継続的なサービス ・ 一貫して文書化されたIT継続計画 ・ ビジネスの必要性のための、統率の取れたサービス ・ 組織の目標をサポートする短期および長期の目標の達成	・ 不十分な継続活動 ・ 適切に管理されていないIT継続サービス ・ 主要な個人への依存の増加

コントロール設計のテスト
・ 企業全体の事業継続管理プロセスが設計され、役員レベルのマネジメント層によって承認されているかどうかを調査して、それを確認する。 ・ 現在のビジネスへの影響の分析結果を閲覧して、継続計画によって、中断期間中のビジネスの業務を回復するのに必要な資源に対して明確に優先順位をつけることができるようになっているかどうかを確認する。 ・ 事業継続フレームワークを閲覧して、そこに、ビジネスが中断する場合にビジネスプロセスを再開するのに必要なすべての要素が含まれていることを確かめる（説明責任、意思伝達、エスカレーション計画、回復戦略、ITとビジネスのサービスレベル、および緊急手続を検討する。）。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.2 IT継続計画 大規模な中断が主要なビジネスの機能とプロセスに及ぼす影響の軽減を目的とする、フレームワークに基づいたIT継続計画を策定する。この計画では、ビジネスに対する潜在的な影響に伴うリスクについての理解に基づいて、すべての重要なITサービスの障害からの回復、代替処理手続、および復旧能力に関する要件について規定する。また、計画では利用ガイドライン、役割と実行責任、手続、周知プロセス、およびテスト方法も規定しなければならない。	・IT全体を通じて継続的なサービスと、それによる重大なIT資源の要件への対処 ・定義され文書化された、ガイドラインと役割と責任 ・組織の目標をサポートする短期および長期の目標の達成	・ITのシステムとサービスをタイムリーな方法で回復できない状態 ・代替的な意思決定プロセスの機能不全 ・回復に必要な資源の欠如 ・内部と外部の利害関係者への伝達の失敗

コントロール設計のテスト
・すべての主要なビジネスの機能とプロセスに関して、事業継続計画が存在することを確かめる。 ・事業継続計画の適切なサンプルをレビューして、それぞれの計画が以下のようであることを確かめる。 　– 復元力、代替的な処理、回復能力を、サービスコミットメントと可用性のターゲットに沿って確立するように設計されている 　– 役割と責任を定義する 　– 意思伝達プロセスを含める 　– 受け入れ可能な最小限の回復構成を定義する ・事業継続計画の全体的なテスト戦略と、テストが合意済みの頻度で実行されていることの証拠を入手する。 ・テストの結果をレビューして、その結果として取るべき行動を取っていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.3 重要なIT資源 IT継続計画において、最重要と定められた要素に重点を置くことで、障害からの回復力を組み込み、災害復旧時の作業の優先順位を設定する。重要度が低い要素の回復を優先させることのないよう、優先的ビジネス要件に応じた対応と復旧を確実にする。また、費用を受容可能なレベルに抑え、法的要件および契約上の要件への遵守も確保する。1～4時間、4～24時間、24時間超、重要業務の運用期間など、さまざまなレベルにおける回復力、対応、および復旧要件を考慮する。	・継続性のための費用管理 ・重要なIT資源に対する効果的な管理 ・優先順位を伴う回復管理	・重要なIT資源に関する可用性の欠如 ・継続性管理のための費用の増加 ・ビジネス上の必要性に基づいていない、サービス回復の優先順位付け

コントロール設計のテスト

- ビジネスの重大性によるビジネス機能の一覧を入手して、最も重大なビジネス機能に継続計画が存在しており、プロセスと資源をサポートしていることを確かめる。
- 計画をレビューして、それがビジネス目標および法律と規制の要件に合致するように設計（およびテスト）されていることを確かめる。
- 計画相互間の整合性がどのようにして確かなものになっているかを判断する

コントロール目標	価値のドライバー	リスクのドライバー
DS4.4 IT継続計画の保守 IT継続計画の内容が常に最新に保たれ、継続的に実際のビジネス要件が反映されることを確実にするために、IT管理部門に対し、変更管理手続の策定および実施を促す。手続と実行責任における変更内容を的確かつタイムリーに周知する。	・組織の達成目標をサポートする適切なIT継続計画 ・IT継続計画のための変更コントロール手続 ・しかるべき個人へのIT継続計画の周知	・不適切な回復計画 ・ビジネス上の必要性と技術の変化を反映していない計画 ・変更コントロール手続の欠如

コントロール設計のテスト

- IT継続計画のすべてのコピーが改訂ごとに更新されており、オンサイトとオフサイトで保管されているかどうかを調査して、それを確認する。
- IT資源に対するすべての重大な変更が、IT継続計画の更新のために継続管理者に伝達されているかどうかを調査して、それを確認する。
- 継続計画に対する変更が要因に対して適切な間隔で、かつ変更コントロール手続に従って行われているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.5 IT継続計画のテスト ITシステムが効果的に回復可能であること、欠点が解消されること、およびIT継続計画の妥当性が維持されることを確実にするために、IT継続計画の定期的なテストを実施する。このためには、綿密な準備、手続の文書化、テスト結果の報告、および結果に基づく対応計画の策定と実施が必要である。テストの範囲として、単一アプリケーションの復旧テストから、複数のテストシナリオを組み合わせたテスト、エンドツーエンドでのテスト、そしてベンダーを含む総合的なテストなどを想定する。	・ITシステムの効果的な回復 ・ITシステムの回復プロセスを経験しているスタッフ ・システムの復元における欠点を克服するアップグレードされた計画	・回復計画の欠点 ・現在のアーキテクチャを反映していない陳腐化した回復計画 ・不適切な回復ステップとプロセス ・現実に災害が発生した場合に効果的に回復する能力の欠如

コントロール設計のテスト

- ITインフラストラクチャおよび業務とそれに関連するアプリケーションの変更後に、定期的にIT継続テストが予定され、完了するかどうかを調査して、それを確認する。
- 新しい構成要素と更新がスケジュールに含まれていることを確かめる。
- サービス中断の論理的で現実的な順序を確認するために詳細なテストスケジュールが作成され、そこにテストの詳細とテスト順序が含まれているかどうかを調査して、それを確認する。
- テストのタスクフォースが創設されているか、そのメンバーは計画の中で定義されている主要なメンバーではないか、報告が適切であるかどうかを調査して、それを確認する。
- 主要な担当者へのインタビューを通じて、報告会が開催されているかどうか、その反省会の中で、失敗が分析され解決策が策定されているかどうかを尋ねる。
- 主要な担当者へのインタビューを通じて、テストを実現できないときの代替手段が評価されているかどうかを尋ねる。
- テストの成功や失敗が測定され報告され、その結果となる変更がIT継続計画に加えられているかどうかを調査する。
- 結果をレビューして、その結果がどのようにレビューされているかを評価することによって、運用の有効性を判断する。

コントロール目標

DS4.6 IT継続計画に関する研修
すべての関係者が、インシデントまたは災害発生時の各自の役割および実行責任と実施手続に関する定期訓練セッションを確実に受講する。緊急時対応テストの結果に基づいて、訓練の内容を検証および補強する。

価値のドライバー

- ITシステムの回復プロセスを経験しているスタッフ
- 回復プロセスの研修を受けているスタッフ
- 責任を持つすべての担当者に対する計画的な研修
- 緊急対応テストの結果を反映すべく更新される研修計画

リスクのドライバー

- 陳腐化した研修スケジュール
- 研修が不十分だったり陳腐化したりしているせいで、期待通りに回復できない状態

コントロール設計のテスト

- 主要な担当者へのインタビューを通じて、定期的な研修が実施されているかどうかを尋ねる。
- 研修の必要性とスケジュールが定期的に評価され更新されているかどうかを調査して、それを確認する。
- スケジュールと研修教材をレビューして、運用の有効性を判断する。
- 主要な担当者へのインタビューを通じて、IT継続の意識喚起プログラムがすべてのレベルで実施されているかどうかを尋ねる。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.7 IT継続計画の配付 計画が安全かつ適切な方法で確実に配付され、必要な時に必要な場所で許可を受けた当事者が利用できるように、定義し管理された配付方法が存在することを確認する。どのような災害発生状況においても、IT継続計画が入手でき参照可能な状態になっているよう配慮する必要がある。	・ ITシステムの回復プロセスを経験しているスタッフ ・ 回復プロセスの研修を受けているスタッフ ・ 影響を受けるすべての当事者が利用できてアクセスできる計画	・ 漏洩の危険にさらされた、計画における機密情報 ・ 要求されるすべての当事者にとってアクセス可能でない計画 ・ 配付戦略がコントロールされていないせいで、タイムリーな方法で実施されない計画のアップグレード

コントロール設計のテスト
・ IT継続計画の配付リストが作成され、定義され、維持されているかどうかを調査して、それを確認する。リストの作成時に「知っておくべき」主義が維持されているかどうかをレビューする。 ・ マネジメント層から配付手続を入手する。 ・ 手続を評価してコンプライアンスを確認する。 ・ 計画の電子コピーと紙のコピーが適切な方法で保全され、承認された人員のみが文書にアクセスできるかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.8 ITサービスの復旧および再開 ITサービスの復旧および再開中に実施すべき措置を計画する。この計画には、バックアップサイトの起動、代替処理の開始、顧客と利害関係者への周知、再開手続などが規定される。ITの復旧にかかる時間とビジネスの復旧と再開のニーズを支援するために必要な技術投資について、ビジネス部門が確実に理解しているようにする。	・ 最小の回復時間 ・ 最小の回復費用 ・ ビジネスにとって重大な作業を優先した回復	・ 回復計画の欠点 ・ 不適切な回復ステップと回復プロセス ・ ビジネスにとって重大なシステムとサービスをタイムリーな方法で回復できない状態

コントロール設計のテスト
・ インシデント対応手続のコピーを入手して、そこに損害評価のためのステップおよび継続計画が始動するための正式な意思決定ポイントと基準値が含まれていることを確かめる。 ・ IT回復計画をレビューして、それがビジネス要件に合致することを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.9 遠隔地におけるバックアップ保管施設 すべての重要なバックアップメディア、文書、およびIT復旧計画と業務継続計画に必要なその他のIT資源を、遠隔地の施設に保管する。保管するバックアップの内容については、ビジネスプロセスオーナとIT担当者が協働して決定する必要がある。遠隔地の保管施設の管理者は、データ分類方法のポリシーと企業のメディア保管活動に対応しなければならない。IT管理部門は、遠隔地保管施設について、保管内容、施設の物理的安全性、およびセキュリティを確実に定期的に（少なくとも1年に1回）評価する必要がある。アーカイブデータの復元のためのハードウェアとソフトウェアの互換性を確保し、アーカイブデータを定期的にテストおよび更新する。	・ ハードウェアが物理的に損傷した際のバックアップデータの可用性 ・ 組織全体を通じて一貫して管理されている遠隔地のデータ ・ 遠隔地での保管場所における適切な保護	・ 遠隔地での保管場所において関連文書がないことによる、バックアップデータとメディアの可用性の欠如 ・ 災害によるデータの喪失 ・ 事故によるバックアップデータの損傷 ・ バックアップテープを必要なときに見つけ出す能力の欠如

コントロール設計のテスト
・ データが遠隔地へ持っていかれるとき、データの輸送中、およびデータが貯蔵場所にあるときにデータが保全されているかどうかを調査して、それを確認する。 ・ バックアップ施設が通常使用の場所と同じリスクにさらされていないかどうかを調査して、それを確認する。 ・ バックアップとメディアの品質を確保するために定期的なテストを実施しているかどうかを調査して、それを確認する。 ・ テスト手続をレビューして、運用の有効性を判断する。 ・ バックアップないし復元されたシステムの内容を運用システムと比較することなどによって、バックアップメディアがIT継続計画に必要なすべての情報を含んでいることを確かめる。 ・ 回復のための指示とラベルが十分に存在するかどうかを調査して、それを確認する。 ・ バックアップとメディアの棚卸が存在するかどうかを調査して、それを確認し、その棚卸の正確さを検証する。

コントロール目標	価値のドライバー	リスクのドライバー
DS4.10 再開後のレビュー 災害発生後にIT機能を正常に再開するために、IT管理部門によりIT復旧計画の妥当性を評価する手続が策定されているかを確認し、必要に応じて計画を更新する。	・更新されている回復計画 ・回復計画に合致している達成目標 ・ビジネス上の必要性に従った、適切な再開計画	・不適切な回復計画 ・ビジネス上の必要性に合致していない回復計画 ・達成目標に合致していない回復計画

コントロール設計のテスト
・計画の欠点に着目して、改善の機会について論じる回復後の会合が実施されているかどうかを調査して、それを確認する。 ・計画、ポリシー、および手続をレビューして、運用の有効性を判断する。

コントロール目標の達成をテストするために以下のステップを踏む。
・企業全体の業務処理回復プロセスをサポートするための継続フレームワークを確立することに対して、マネジメントレベルを判断する。
・ビジネスの中断の際に、ビジネス戦略をサポートするIT継続の説明責任と実行責任を遂行するために定義された構成要素を判断する。
・業務処理目標に合致するための回復戦略と要求されるサービスレベルに関して、IT継続計画を評価する。
・影響を受けるすべての当事者の安全と公的機関との協力を確かにするために策定されている伝達計画の有効性を判断する。
・短期および長期の業務処理要件の回復を達成するガイドライン、役割および責任を評価する。
・IT継続計画の研修が定期的に提供されているかどうかを評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・IT継続サービスが、短期および長期の組織の達成目標に合致するための業務処理サービスの実現を十分にサポートしているかどうかを評価する。
・フレームワークを評価して、計画が回復戦略の優先順位付けよりもむしろ主要な個人に依存しているかどうかを判断する。
・代替的な意思決定プロセスがなくて、ITシステムがタイムリーな方法で回復しない場合の業務処理への影響を評価する。
・回復のための資源が利用できず、内部と外部の利害関係者にまったく伝達することができないときに求められるビジネスへの影響を判断する。
・研修を受けておらず、IT継続計画の手続に従わない担当者のせいで、ITの中断が長引いたことがあったかどうかを、マネジメント層に尋ねる。

DS5 システムセキュリティの保証

情報のインテグリティを維持し、IT資産を保護するためには、セキュリティ管理のプロセスが必要である。このプロセスには、ITセキュリティに関する役割と責務、ポリシー、標準、および手続を定め、それらを運用、改善することが含まれる。また、セキュリティ管理には、セキュリティのモニタリングと定期的なテストの実施、および識別されたセキュリティの弱点やインシデントに対する是正措置の導入も含まれる。セキュリティ管理を効果的に実行することで、すべてのIT資産を保護し、セキュリティの脆弱性やインシデントがビジネスに与える影響を最小限に抑えることができる。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.1 ITセキュリティの管理 セキュリティに係るアクティビティが、ビジネス上の要件に沿って実施されるよう、組織の適切な上位層において、最適な体制を組んでITセキュリティを管理する。	・保全された重要なIT資産 ・ビジネスの達成目標をサポートするITセキュリティ戦略 ・ビジネスプラン全体と整合的なITセキュリティ戦略 ・該当する法律および規制と整合的で、適切に導入され維持されているセキュリティ活動	・ITセキュリティガバナンスの欠如 ・ITの達成目標と事業目標との不整合 ・保全されていないデータと情報資産

コントロール設計のテスト

- 内部監査、人事、オペレーション、ITセキュリティ、法務を含む主要な機能分野からの代表者によるセキュリティ運営委員会が存在するかどうかを確認する。
- ポリシー、標準、手順書で要求されるレベルを含む、提案されているセキュリティ業務の優先順位をつけるためのプロセスが存在するかどうかを確認する。
- 情報セキュリティ憲章が存在するかどうかを調査して、それを確認する。
- セキュリティ憲章をレビューして分析して、情報セキュリティに関連する組織のリスク選好度に言及していることと、以下が明確に含まれていることを確かめる。
  - セキュリティ管理部門の対象範囲と達成目標
  - セキュリティ管理部門の実行責任
  - コンプライアンスとリスクのドライバー
- 情報セキュリティポリシーが、取締役会、マネジメント層、ラインマネジメント、スタッフメンバー、および企業の情報インフラストラクチャのすべてのユーザの実行責任をカバーしており、それがセキュリティに関する詳細な標準と手続に言及しているかどうかを調査して、それを確認する。
- セキュリティに関する詳細なポリシー、標準、手順書が存在するかどうかを調査して、それを確認する。ポリシー、標準、手順書の例としては以下のものが含まれる。
  - セキュリティコンプライアンスポリシー
  - リスク受容（セキュリティを遵守していないことを認識すること）の管理
  - 外部への通信に関するセキュリティポリシー
  - ファイアウォールポリシー
  - 電子メールセキュリティポリシー
  - IS ポリシーを遵守するという合意
  - ラップトップ/デスクトップコンピュータのセキュリティポリシー
  - インターネット利用ポリシー
- 情報セキュリティのための十分な組織構造と報告経路が存在するかどうかを調査してそれを確認し、セキュリティ管理部門に十分な権限があるかどうかを評価する。
- 取締役会、ビジネス部門、ITマネジメント層に情報セキュリティの状況を知らせるセキュリティ管理報告メカニズムが存在するかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.2 ITセキュリティ計画 ITインフラストラクチャとセキュリティ文化を考慮に入れ、ビジネス、リスク、コンプライアンスに関する要件を、総合的なITセキュリティ計画としてまとめる。この計画は、サービス、要員、ソフトウェア、およびハードウェアに対する適切な投資とともに、セキュリティポリシーや手続に盛り込むようにする。セキュリティポリシーと手続を利害関係者とユーザに周知する。	・ビジネス要件を満たし、かつビジネスを危険に晒すすべてのリスクをカバーしているITセキュリティ計画 ・セキュリティ計画を確かなものとするための一貫した方法で管理されている、ITセキュリティへの投資 ・利害関係者とユーザに周知されているセキュリティポリシーおよび手続 ・ITセキュリティ計画を意識しているユーザ	・ビジネス要件と整合的でないITセキュリティ計画 ・費用対効果の低いITセキュリティ計画 ・戦略でカバーされていない脅威に晒されているビジネス ・計画されたITセキュリティ手段と実施されているITセキュリティ手段との間のギャップ ・ITセキュリティ計画を意識していないユーザ ・利害関係者とユーザによって妥協されたセキュリティ評価基準

コントロール設計のテスト

・情報セキュリティ要件を収集し、組織での必要性の変化に対応する全体的なセキュリティ計画へと統合することの有効性を判断する。
・IT戦略計画（PO1）、データ分類（PO2）、技術標準（PO3）、セキュリティとコントロールのポリシー（PO6）、リスク管理（PO9）、外部のコンプライアンス要件（ME3）をITセキュリティ計画で考慮していることを確かめる。
・ITセキュリティ計画を定期的に更新するためのプロセスが存在するかどうか、そのプロセスで、適切なレベルのマネジメントレビューと変更の承認を要求しているかどうかを確認する。
・主要なプラットフォームに対する企業の情報セキュリティベースラインが、ITセキュリティ計画全体と釣り合っているかどうか、そのベースラインが、構成ベースライン（DS9）中央リポジトリに記録されているかどうか、および計画の変更に基づいて、それらのベースラインを定期的に更新するプロセスが存在するかどうかを確認する。
・ITセキュリティ計画に以下が含まれているかどうかを確認する。
  - 確立した情報セキュリティポリシーフレームワークに沿ったセキュリティのポリシーと基準の一式
  - ポリシーと基準を実施して守らせるための手続
  - 役割と責任
  - 人員配置の要件
  - セキュリティに対する意識喚起と研修
  - セキュリティを遵守させるための活動
  - 必要なセキュリティ資源に対する投資
・情報セキュリティ要件とITセキュリティ計画からの導入提言を、SLAとOLAの作成（DS1-DS2）、自動化ソリューションの要件（AI1）、アプリケーションソフトウェア（AI2）、ITインフラストラクチャの構成要素（AI3）を含む他のプロセスへと統合するためのプロセスが存在するかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.3 ID管理 ITシステムにおけるすべてのユーザ(内部、外部、臨時かどうかを問わず)と、ユーザのすべてのアクティビティ(ビジネスアプリケーション、IT環境、システムの操作、開発や保守)を、個々に識別できるようにする。認証メカニズムを介してユーザの識別を可能にする。システムやデータに対するユーザのアクセス権が、文書化された定義済みの業務上の必要性に即しており、該当する職務要件がユーザIDに対応していることを確認する。ユーザのアクセス権が、ユーザ管理職の申請に基づいてシステムオーナにより承認され、セキュリティ責任者により実装されていることを確認する。ユーザIDとアクセス権を単一のリポジトリで集中管理する。ユーザの識別、認証の実施、およびアクセス権の管理徹底のために、費用効率に優れた技術や手続での対策を講じ、継続的な改善を行う。	・変更の効果的な導入 ・不適切なアクセス活動に対する適切な調査 ・承認されたビジネストランザクションを確実にする安全な通信	・ハードウェアとソフトウェアに対する承認されていない変更 ・ビジネス要件を満たしておらず、ビジネスにとって重大なシステムのセキュリティが危険に晒されているようなアクセス管理 ・すべてのシステムに対して特定されていないセキュリティ要件 ・職務の分離の違反 ・危険に晒されてるシステム情報

コントロール設計のテスト

・アクセスが認められる前にユーザとシステムプロセスが一意に特定可能で、認証を強制するようにシステムが設定されることがセキュリティ活動で要求されているかどうかを確認する。
・事前に定義され事前に承認された役割がアクセス権の授与のために活用されている場合には、最少特権に基づいて役割が責任を明確に線引きしているかどうかを確認し、役割の確立と改変がプロセスオーナの管理によって承認されていることを確かめる。
・アクセスプロビジョニングと認証コントロールメカニズムが、自社および遠隔管理されているユーザ、プロセス、システムについての、ユーザ、システムプロセスとIT資源のすべてにわたる論理的アクセスコントロールのために活用されているかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.4 ユーザアカウントの管理 ユーザアカウントとそれに付随するユーザ権限の申請、設定、発行、停止、変更、および抹消は、一連のユーザアカウント管理手続に従って対応する。ユーザアカウントの管理には、データオーナまたはシステムオーナがアクセス権限を付与する場合の承認手続も含まれる。これら一連の手続は、アドミニストレーター(特権ユーザ)、内部ユーザ、外部ユーザを含むすべてのユーザに、平常時/緊急時を問わず適用されるべきである。企業が所有するシステムと情報へのアクセスに関連した権利と義務は、あらゆるタイプのユーザごとに契約の形式で定める。すべてのアカウントとそれらに関連する権限の内容は、マネジメント層が定期的にレビューする。	・一貫して管理されているユーザアカウント ・すべての種類のユーザのためのルールと規制 ・セキュリティインシデントのタイムリーな発見 ・承認されていないユーザからのITシステムと機密データの保全	・セキュリティ違反 ・セキュリティポリシーを遵守していないユーザ ・タイムリーに解決されないインシデント ・利用されていないアカウントをタイムリーに停止しておらず、企業のセキュリティに影響が及ぶ状態

コントロール設計のテスト

- システムとアプリケーションのアクセスと権限を定期的に評価し再認証するための手続が存在するかどうかを確認する。
- 組織のセキュリティポリシーおよびコンプライアンスと規制の要件にしたがって、システムとアプリケーションの権利と特権をコントロールし管理するためのアクセスコントロール手続が存在するかどうかを確認する。
- システム、アプリケーション、データが、重要度とリスクのレベルによって分類されているかどうか、プロセスオーナが特定され任命されているかどうかを確認する。
- ユーザプロビジョニングのポリシー、基準、手順書を、ベンダ、サービスプロバイダ、ビジネスパートナーを含むすべてのシステムユーザとプロセスへと拡張しているかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.5 セキュリティのテスト、監視、モニタリング ITセキュリティの実装状態を積極的な方法でテストしモニタリングする。承認された企業の情報セキュリティ基準が維持されるように、ITセキュリティを適切な時期に見直す必要がある。ログの取得とモニタリングの機能を活用することで、対応の必要な異例もしくは異常なアクティビティを早期に防止/検知できる。	・ ITシステムのセキュリティのテストとモニタリングの経験を持つスタッフ ・ 定期的にレビューされるセキュリティレベル ・ ビジネス要件からの逸脱の明確化 ・ 積極的に発見されるセキュリティ違反	・ 組織のセキュリティが危険に晒されるようなユーザアカウントの不正利用 ・ 発見されないセキュリティ違反 ・ 信頼できないセキュリティログ

コントロール設計のテスト

・ すべてのネットワーク機器、サービス、アプリケーションの棚卸が存在し、それぞれの構成要素にセキュリティリスクレートが割り当てられているかどうかを調査して、それを確認する。
・ 組織で活用しているITのすべてについて、セキュリティベースラインが存在するかどうかを確認する。
・ 組織にとって重大で、よりリスクの高いネットワーク資産が、セキュリティイベントのために日常的にモニタリングされているかどうかを確認する。
・ 新規または既存のシステムにセキュリティの脆弱性が導入されるリスクを最少化するために、開発、設計、テストの要件でセキュリティが確実に考慮されるように、ITセキュリティ管理部門が組織のプロジェクト管理に関する業務の中で統合されているかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.6 セキュリティインシデントの定義 起こり得るセキュリティインシデントの特性を明確に定義および周知することにより、インシデント管理または問題管理プロセスを通じて、適切に分類して対応できるようにする。	・セキュリティインシデントの積極的な発見 ・定義され文書化されたレベルでのセキュリティ違反の報告 ・特定された方法でのセキュリティインシデントのための意思伝達	・発見されないセキュリティ違反 ・攻撃に対抗するための情報の欠如 ・セキュリティ違反の分類の欠如

コントロール設計のテスト

・セキュリティの緊急事態に対応し効果的に管理するためのコンピュータ緊急対応チーム（CERT）が存在するかどうかを確認する。効果的なCERTプロセスの一環として、以下のエリアが存在すべきである。
  - インシデント対応—インシデントおよび報告された脆弱性に効果的に対処できるようにするための一般的かつ個別的な手続とその他の要件
  - ベンダリレーション—インシデントの防止とフォローアップ、ソフトウェアの不具合修正、および他のエリアにおけるベンダの役割と責任
  - コミュニケーション—マネジメント層の主要メンバー間の緊急および日常の意思伝達チャンネルの必要条件、実施、オペレーション
  - 法律と犯罪調査の問題点—インシデントの最中の法的な考慮事項と要件や犯罪調査組織の関与に起因する制約による問題点
  - 得意先とのリレーション—研修と意識喚起、構成管理、認証を含む、レスポンスセンターのサポートサービスと得意先との対話方法
  - リサーチアジェンダと対話—既存の調査研究活動およびレスポンスセンターの活動に関連して必要とされている調査研究の要件と根拠の特定
  - 脅威のモデル—リスク低減活動とそのような活動の促進に焦点を当てるための潜在的な脅威とリスクを特徴づける基本モデルの作成
  - 外部の問題点—企業での直接的なコントロール（法律、ポリシー、手続の要件など）の対象外だが企業活動の運用と有効性に影響しうるような要因
・セキュリティインシデント管理プロセスが、ヘルプデスク、外部のサービスプロバイダ、ネットワーク管理部門を含む、組織での主要な部門に効果的に接続しているかどうかを判断する。
・セキュリティインシデント管理プロセスに、以下の主要な要素が含まれているかどうかを評価する。
  - イベントの発見
  - イベントと脅威/インシデントの評価との相関
  - 脅威の解決、つまり作業命令の作成とエスカレーション
  - 組織の CERT プロセスの開始基準
  - 解決の文書化の検証と文書化で要求されているレベル
  - 修復後の分析
  - 作業命令/インシデント終了

コントロール目標	価値のドライバー	リスクのドライバー
DS5.7 セキュリティ技術の保護 セキュリティ関連の技術に、改ざんに対する耐性を確保し、セキュリティ関連文書が不必要に開示されないように対応する。	・保全された企業のセキュリティ技術 ・信頼できる情報の安全確保 ・保全された企業資産	・情報漏洩 ・他の組織との信頼関係の毀損 ・法規制の要件違反

コントロール設計のテスト

- セキュリティ違反の結果に対処するためのポリシーと手続が確立されているかどうかを調査して、それを確認する（特に、構成管理、アプリケーションアクセス、データセキュリティ、物理的なセキュリティの要件のコントロールに対処するためのもの）。
- アクセス権を授与してアクセスを承認したコントロール記録、および成功しなかったアクセス試行、ログアウト、機密ファイルないしデータへの承認されたアクセス、施設に対する物理的なアクセスを記録したコントロール記録を閲覧する。
- セキュリティ対策の設計で、パスワードルール（最大長、文字、有効期限、再利用など）を活用しているかどうかを調査して、それを確認する。
- ファイルとデータに対する物理的および論理的なアクセスのためのセキュリティ対策に対してマネジメント層が毎年レビューすることが、コントロールで要求されているかどうかを調査して、それを確認する。
- アクセス権限が与えられており、アクセスが適切に承認されていることを確かめる。
- ネットワーク侵入脆弱性攻撃を防止するシステムツールから生成されたセキュリティ報告を閲覧する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.8 暗号鍵の管理 暗号鍵の生成・変更・取消・失効・交付・認証・保存・入力・使用・アーカイブ化を体系的に行うためのポリシーおよび手続を確実に整備し、暗号鍵の改変や許可されていない暗号鍵の開示を防止する。	・定義され文書化された暗号鍵の管理 ・安全な方法で扱われている暗号鍵 ・安全な通信	・承認されていない人物によって不正利用される暗号鍵 ・確認されていないユーザ登録と、それによって危険にさらされるシステムセキュリティ ・暗号鍵に対する承認されていないアクセス

コントロール設計のテスト

・暗号鍵のライフサイクル管理のための定義されたプロセスが存在するかどうかを確認する。そのプロセスには以下を含むべきである。
  - 強度の高い鍵を生成するために要求される最小限の鍵の大きさ
  - 暗号鍵の生成で要求されるアルゴリズムの利用
  - 暗号鍵の生成のために要求される基準の特定
  - 暗号鍵を利用し制限する目的
  - 暗号鍵の利用可能期間や有効期間
  - 暗号鍵の好ましい配布方法
  - 暗号鍵のバックアップ、アーカイブ、破棄
・私有鍵の機密性とインテグリティを確保するための、私有鍵に対するコントロールが存在するかどうかを評価する。以下を考慮すべきである。
  - 私有署名鍵を安全な暗号化デバイスで保管する(FIPS 140-1、ISO 15782-1、ANSI X9.66 など)
  - 私有鍵が安全な暗号化モジュールから取り出されない
  - 物理的に安全な環境で、二重コントロールを用いる、承認された人員によってのみ、私有鍵のバックアップを取られ、保管され、回復される
・組織が情報を共有したり制限したりする必要性とそのような必要性に関連して組織に及ぶ影響について、組織が情報分類と関連する保護コントロールを実施しているかどうかを調査して、それを確認する。
・情報のラベルと取り扱いが、組織の情報分類スキームにしたがって実施されるようにするための手続が定義されているかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.9 不正ソフトウェアの阻止、発見、および是正 予防・発見・対処のための対策(特に最新のセキュリティパッチとウイルス管理)を組織全体にわたって実施し、ITシステムと情報技術を悪意のあるソフトウェア(ウイルス、ワーム、スパイウェア、スパム)から保護する。	・マルウェアから積極的に保護することによって確保されたシステムセキュリティ ・システムのインテグリティの確保 ・セキュリティの脅威のタイムリーな発見	・情報漏洩 ・法規制の要件に対する違反 ・ウィルスによる攻撃を受けやすいシステムとデータ ・効果的でない対応措置

コントロール設計のテスト

- 悪意あるソフトウェアを防止するためのポリシーが策定され、文書化され、組織を通じて伝達されているかどうかを調査して、それを確認する。
- ウィルスから保護するための自動化されたコントロールが実施されており、違反が適切に伝達されていることを確かめる。
- 悪意あるソフトウェアを防止するためのポリシーと、コンプライアンスを確実にするための自らの責任を意識しているかどうかを、主要な担当者に尋ねる。
- ユーザのワークステーションのサンプルから、ウィルス防止ツールがインストールされており、ウィルス定義ファイルおよび定義ファイルが更新された日付が含まれているかどうかを観察する。
- ウィルス保護ソフトウェアが、集中的な構成管理と変更管理のプロセスを用いて、集中的に配付されているかどうかを調査して、それを確認する。
- 配付プロセスをレビューして、運用の有効性を判断する。
- 新たな潜在的な脅威についての情報が定期的にレビューされ評価され、必要に応じて、ウィルス定義ファイルへと手動で更新されているかどうかを調査して、それを確認する。
- レビューと評価のプロセスをレビューして、運用の有効性を判断する。
- 要求されていない情報を遮断するために外部から来る電子メールに適切にフィルターがかけられているかどうかを調査して、それを確認する。
- フィルタリングプロセスをレビューして運用の有効性を判断するか、あるいは、フィルタリングの目的で確立している自動化プロセスをレビューする。

コントロール目標

DS5.10 ネットワークのセキュリティ
セキュリティ技術とそれに関連する管理手続(ファイアウォール、セキュリティアプライアンス、ネットワークのセグメント化、侵入検知など)を使用し、ネットワークへのアクセスの許可とネットワークに出入りする情報フローを確実にコントロールする。

価値のドライバー

- 企業のセキュリティ技術の保全
- 信頼できる情報の安全確保
- 企業資産の保全
- 一貫した方法で管理されるネットワークセキュリティ

リスクのドライバー

- ファイアウォールルールが、組織のセキュリティポリシーを反映していない状態
- ファイアウォールルールに対する承認されていない改変が発見されない状態
- 全体が危険に晒されたセキュリティアーキテクチャ
- タイムリーに発見されないセキュリティ違反

コントロール設計のテスト

- ネットワークセキュリティポリシー（提供されているサービス、許容されているトラフィック、許可されている接続のタイプなど）が策定され維持されているかどうかを調査して、それを確認する。
- すべての重大なネットワーク構成要素を管理するための手続とガイドラインが主要な管理担当者によって策定され、定期的に更新され、文書への変更が文書履歴で追跡されているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS5.11 機密データの交換 機密性を有するトランザクションデータは、内容の真正性確保、送信証明、受信証明、および送信元による否認防止が可能なコントロールを備えた信頼できる経路あるいはメディアのみを介してやり取りを行う必要がある。	・信頼された通信方法 ・信頼できる情報交換 ・保護された、システムとデータのインテグリティ	・機密情報の漏洩 ・不十分な物理的セキュリティ手段 ・遠隔地のサイトへの承認されていない外部接続 ・企業の資産情報および機密情報が漏洩し、承認されていない人員がその情報にアクセス可能になる状態

コントロール設計のテスト

・組織外へのデータ送信の際に、送信に先立って暗号化されたフォーマットが要求されるかどうかを調査して、それを確認する。
・企業のデータが危険のレベルと分類スキーム（機密、重要など）にしたがって分類されているかどうかを調査して、それを確認する。
・極秘データ処理が、送信に先立ってトランザクションの妥当性をチェックするアプリケーションコントロールを通じてコントロールされているかどうかを調査して、それを確認する。
・不正なトランザクションや未完了のトランザクションに関して、アプリケーションログや停止処理をレビューする。

コントロール目標の達成をテストするために以下のステップを踏む。
・質問と観察を通じて、セキュリティ管理部門が、リスク管理、コンプライアンス、監査を含む企業での主要な部署と効果的に交流しているかどうかを確認する。
・インシデント記録のサンプルを選び、セキュリティインシデントを特定し、対応するためのプロセスをレビューする。質問と根拠となる文書のレビューを通じて、インシデントを解決するために適切な管理活動を取っているかどうかを判断する。
・従業員のサンプルを選び、雇用条件の一環として、コンピュータの利用と機密保持（機密漏洩防止）の合意に署名したかどうかを確認する。
・ITセキュリティの戦略、計画、ポリシー、手順書をレビューして、組織の現在のITランドスケープとの関係性を判断し、それが最後にレビューされ更新されたのがいつかを判断する。
・ITセキュリティの戦略、計画、ポリシー、手順書をレビューして、データ分類を反映していることを確かめる。
・ITセキュリティの戦略、計画、ポリシー、手順書についての知識について利害関係者とユーザにインタビューして、利害関係者とユーザが、自らがリスクと組織での活動と関係あると気づいているかどうかを確認する。
・組織に対する最近または計画されている変更（ビジネスユニットの獲得/廃止、新規システム、規制の環境の変化など）について経営陣に尋ねて、ITセキュリティ計画と適切に整合しているかどうかを確認する。
・システム（開発、テスト、本番のシステム）とアプリケーションアカウント、ジョブキューとサービス、およびセキュリティソフトウェアのモード設定のレビューを通じて、すべてのユーザとプロセスの行動を一意に特定しコントロールするためのセキュリティプロセスが導入されているかどうかを確認する。
・アクセスコントロールリスト（ACL）のサンプルを通じて、セキュリティプロビジョンプロセスが以下を適切に考慮しているかどうかを判断する。

  - 関与している情報とアプリケーションの重要性（データ分類）
  - 情報の保全と配布のためのポリシー（法律、規制、契約の要件）
  - 機能が「必要のあるものだけを持つ」となっているか
  - 組織での共通の職務のための標準的なユーザアクセスプロファイル
  - 関与しているアクセス権の分離の必要性
  - アクセスのためのデータオーナとマネジメント層の承認
  - 集中的なリポジトリにおける ID とアクセス権の文書化
  - 初期パスワードの作成、伝達、変更
- 質問とACLのサンプルのレビューを通じて、セキュリティ認証に関する確立した活動と役割に不相応のアクセスプロビジョニング要求を解決するためのプロセスが存在するかどうかを確認する。
- 潜在的な職務の分離を特定するためのリスク評価プロセスが活用されているかどうか、および、追加的なレベルの管理権限を得るためにエスカレーションプロセスが活用されているかどうかを確認する。
- 情報の重要性と重大性にしたがってアクセス権を行使するための認証と承認のメカニズムが存在するかどうかを確認する（パスワード、トークン、電子署名など）
- 信頼関係によって同等のセキュリティレベルを守らせ、ユーザとプロセスのIDを維持しているかどうかを確認する。
- ユーザとシステムのアカウントのサンプルと、ACLのサンプルを選び、以下の存在を確認する。
  - 明確に定義された、要求された役割ないし特権
  - 割り当てについてのビジネス上の正当化
  - データオーナとマネジメント層の承認
  - 非標準の要求に対するビジネス/リスクでの正当化とマネジメント層の承認
  - 職務/役割に相応に要求されているアクセスと、そこで要求されている職務の分離
  - プロビジョニングプロセスを遵守し完了したことを証明する文書
- 人事部門から従業員の移動と退職のサンプルを入手して、システムアカウントプロファイルないしACLのレビューを通じて、アクセス権が適切に変更されたりタイムリーに取り消されたりしているかどうかを確認する。
- 重要なネットワーク機器やシステムサービスのサンプルを選び、アクセスコントロールメカニズムが日常的に評価されテストされているかどうかを確認して、運用の有効性を確かめる。
- 重要なネットワーク機器とシステムサービスのサンプルを選び、セキュリティインシデントの存在に関して日常的にモニタリングされているかどうかを確認する。
- セキュリティベースラインのサンプルを取り、それが組織のリスクプロファイルと受け入れられているリスクのレベルと整合しているかどうか、また共通のリスクと脆弱性を考慮しているかどうか（模範となる活動に従うなど）を確認する。
- ITデバイスのサンプルを選び、確立したセキュリティベースラインへの遵守状況を判断する。ベースラインからの逸脱に関して、リスク評価が実施されたかどうか、マネジメント層がベースラインからの逸脱を承認したかどうかを確認する。
- セキュリティレビュープロセスが、システムセキュリティの設計や運用に影響するITの変更に対してセキュリティ管理者の関与と承認を要求し、組織の調達と導入のプロセス（AI）、サービス提供とサポートのプロセス（DS）へと統合されているかどうかを確認する。レビュープロセスでは以下を考慮すべきである。
  - 全体的な技術アーキテクチャ
  - データベースへのアクセスとセキュリティの設計
  - プロトコル、ポート、ソケットの利用
  - 要求されるサービス
  - ユーザのリモートアクセスとモデムの要件
  - サーバとサーバの間の認証と暗号化
  - 拡張性、可用性、および冗長性
  - セッション管理とクッキーの利用
  - 管理能力
  - ユーザ ID とパスワードの管理
  - 監査証跡とログ/報告

- セキュリティ監査証跡が、ユーザID、イベントのタイプ、日付と時刻、成功や失敗の表示、イベントの起点、影響を受けるオブジェクトのIDや名前を記録しているかどうかを確認する。重要なデータへのアクセス、管理アカウントと特権アカウントによる活動、監査ログの初期化、システムレベルのオブジェクトの改変が、ログを取るべきイベントとして含まれているべきである。
- 潜在的なセキュリティインシデントの記録、分析、解決をサポートする文書を閲覧、レビューして、以下のステップを実施する。
  - インシデントを分類し、実施可能な脅威を特定するための方法を理解する
  - 具体的にログを取ってあるセキュリティインシデントを特定し、インシデントの性質について調査する。
- すべてのデバイスが最新のリリースとセキュリティパッチレベルになっていることを確かめることを目的に、組織のネットワーク機器の棚卸を公表されている脆弱性に合わせるために用いるプロセスの証拠となる文書を閲覧する。
- 暗号機器、ソフトウェア、運用手順への変更を含む暗号鍵管理ライフサイクルを通じて、正式な管理責任と管理手続が存在するかどうかを確認する。
- 新しい暗号鍵のサンプルについて、業界基準とコンプライアンスや規制の要件（ISO 15782-1、FIPS 140-1、ANSI X9.66など）にしたがって暗号鍵のペアが作られているかどうか、および、知識の分断した二重コントロールの暗号鍵（暗号鍵全体を再構築するために二人または三人の人が必要で、各自が鍵のうち自分の担当部分しか知らないようなもの）の存在の証拠となるような文書があるかどうかを確認する。
- 期限切れの暗号鍵のサンプルについて、暗号鍵のペアのライフサイクルの終わりに、鍵が完全に破棄された証拠となる文書が存在するかどうかを確認する。
- 暗号化ハードウェアが日常的にテストされているという証拠になる保守記録をレビューする。
- 暗号化のハードウェア、ソフトウェア、鍵へのアクセス権を持つ個人の一覧を入手し、暗号鍵の作成と導入に責任を持つ、適切に承認された個人にアクセスが限定されているかどうかを確認する。
- 暗号鍵の管理人が、自らの暗号鍵管理の責任を正式に認識し、理解し、受け入れているかどうかを確認する。
- 暗号鍵と構成要素が承認された管理者しか知らないような方法で暗号鍵が作られ、保管され、利用されているかどうかを判断する。
- サードパーティベンダから受け取った暗号鍵について、異なる日付に異なるキャリアによって別々に送られているか、および、暗号鍵のそれぞれの部分が、別々の鍵管理者がそのダイヤル番号を知っているような、別々の金庫に保管されているかどうかを確認する。
- システムセキュリティ対策を評価して、悪意あるセキュリティ攻撃から保護するための積極的なコントロールが確立しているかどうか評価する。
- データ/システム保護ソフトウェアが、ネットワーク環境を通じて集中的に配布されているかどうかを評価する。
- 要求されていない情報に対して、外部からのトラフィックをフィルターにかけるためのコントロール機能を評価する。
- 重大なネットワーク機器のサンプルを選び、その機器が特別なメカニズムやツール（デバイス管理のための認証、安全な通信、強固な認証メカニズムなど）によって適切に保護されていること、および装置を攻撃から守るための能動的監視とパターン認識が用いられていることを確かめる。
- ネットワーク機器のサンプルを選び、その機器が使用可能な最小限の機能で構成されており（機器が機能するために必要でセキュリティアプリケーションのために強化されているような機能）、すべての不必要なサービス、機能、インターフェースが取り除かれており、すべての関連するセキュリティパッチと主要な更新が、本番稼動する前にタイムリーにシステムに適用されているかどうかを確認する。
- 新しいネットワーク機器や既存のネットワーク機器への変更のサンプルを選び、組織の調達と導入（AI）のプロセスのコントロールとサービス提供とサポート（DS）のプロセスのコントロールに従っていることを判断する。
- ファイアウォールデバイスのサンプルを選び、以下についてACLをレビューする。
  - 信頼されているネットワークセグメントと信頼されていないネットワークセグメントとをアクセスルールによっ

て効果的に分離している
- ルールのビジネス上の目的とマネジメント層の承認の証拠となる文書
- 構成が、マネジメント層が承認したベースラインに従っている
- デバイスのバージョンとパッチリリールレベルが最新である

・ SSH、VPNまたはSSL/TLSといったようなすべての非コンソールの管理アクセスで暗号化が活用されているかどうかを確認する。
・ データが信頼できる発信源を通じて送信されるといったように、自動化されたコントロールによってデータとシステムを保護しているかどうかを評価する。
・ アクセス権の適切性と職務の分類の要件を確保するために、ユーザ管理部門が、ユーザプロファイルとアクセス権を定期的にレビューしているかどうか確認する。
・ データへの直接のアクセスが防止されているか、必要な場合には相応にコントロールされ文書化されていることを確かめる。
・ パスワードの品質要件がシステムによって定義され、実行されていることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・ セキュリティへの配慮（SDLCの中でセキュリティ管理部門が関与しているなど）の存在についての機能と運用に関する文書を閲覧することによって、組織内でのセキュリティに対する意識のレベルを判断する。
・ 同様の組織と照らし合わせて情報セキュリティ組織のベンチマークを取り（規模、報告経路など）、国際標準/業界で認識されているベストプラクティスに対して、正式化されたポリシー、基準、手順書のベンチマークを取る。
・ セキュリティ管理部門がITランドスケープの規模と複雑性に相応のものであるかどうかを確認する上で、以下を検討する。
  - IT ランドスケープの規模、複雑性、多様性
  - セキュリティ管理のツールと技術の利用
  - セキュリティ管理のビジネスラインとの整合性（組織のセグメントに競合するセキュリティ機能があるかなど）
  - セキュリティ管理担当者の技能と研修
・ 経営陣のメンバーがセキュリティ管理組織の重要性と自らのサポートを周知しているかどうかを確認する。正式化されたセキュリティポリシーに対する経営陣やセキュリティ運営委員会の承認を検討すべきである。
・ 組織のITランドスケープのすべての関連する側面についての論理セキュリティを取り扱う、マネジメント層に承認されたセキュリティ憲章とポリシー、基準、手順書の存在を確認する。
・ ITセキュリティ計画で、規制やコンプライアンスの要件を含む組織のセキュリティプロファイルを十分に検討したかどうかを確認する。
・ セキュリティ管理組織が計画の遵守を実行しモニタリングする能力を評価する。組織の規模、セキュリティ評価と管理のための技術とツールの利用、セキュリティ担当者に要求される経験レベル、およびセキュリティ担当者の受けている継続的な研修を検討すべきである。
・ 組織内の様々な財務、オペレーション、コンプライアンスのエリアからポリシー、基準、手順書を選び、ITセキュリティ計画の主要な規定が文書に適切に反映されているかどうかを確認する。
・ セキュリティレビュープロセスが、システムセキュリティの設計や運用に影響するITの変更に対してセキュリティ管理者の関与と承認を要求する、AIとDSのプロセスへと統合されているかどうかを確認する。
・ 組織のAIのプロセスとコントロールが、分離された開発、テストと保証、および本番環境によってサポートされているかどうかを確認する。
・ 匿名アカウントとグループアカウント（nobody, web user, everybodyなど）、リモートプロセス、および開始したタスクの存在と合理性を特定する。トランザクションの権限、特権の潜在的な上申リスク、プロセスの開始場所（信頼できるか信頼できないなど）の性質と対象範囲を考慮すべきである。あるいは、システムやアプリケーションが開始したジョブとプロセスに関してセキュリティ設計レビューが実施されたかどうかを考慮すべきである。
・ セキュリティのソフトウェアとアプリケーション、およびそれをサポートするシステムソフトウェアが、ユーザの認証を実施したり、ユーザとプロセスのIDを伝播させたりするように設定されているかどうかを確認する。匿

名のユーザやプロセスを認証するためのデフォルトアカウントが存在するかどうかを確認する。
- 信頼されていないアクセスの要求元（ビジネスパートナーやベンダなど）を決定し、一意に特定できるアカウント保持者と適切な情報保護をもたらすためにどのようにアクセス権が割り当てられているかを判断する。
- 監査ソフトウェアのツールやスクリプトの利用を通じて、休止アカウントや使用されていないアカウントの存在を特定し、業務上の正当事由が存在するかどうかを確認する。
- ベンダや請負業者の稼動アカウントを特定して、アクセスが契約の条件や期間に相応かどうかを判断する。
- ベンダが提供するアカウントが適切に保護されているかどうかを確認する（デフォルトパスワードが変更されている、アカウントが抹消されているなど）。
- 組織のリスクプロファイル、規模、複雑性、および多様性を考慮しながら、活用されている検証と脆弱性評価のプロセスの性質と頻度の合理性を評価する。
- 共通する脆弱性の存在、セキュリティメカニズムの有効性、およびユーザアクセス管理プロセスの有効性をテストするために、セキュリティのスクリプトとツールが活用されているかどうかを確認する（休止ユーザアカウントや、一度も利用されていないユーザアカウント、終了したユーザアカウント、パスワードのないアカウント、またはパスワード変更を強制されたアカウントなど）。
- 組織にとって重大なネットワーク機器（ハードウェアとアプリケーションシステム）と、リスクのあるネットワーク周辺機器のサンプルを特定して選び出す。インシデントを記録するためのセキュリティセンサの存在やホストログの利用を決定し、セキュリティインシデントや日々のレビュープロセスに含まれていることを確かめる。
- セキュリティに関連するインシデントの作業命令チケットのサンプルを入手して、問題点がタイムリーかつ適切に解決し終了したかどうかを確認する。
- セキュリティツールの配備で、組織が活用している主要な技術のすべてを扱っているかどうか、およびセキュリティツールと技術を適切に運用するのに要する技術を要員が保持しているかどうかを確認する。
- セキュリティ担当者が年次研修に参加するように要求されているかどうか、および、脅威と脆弱性のエンジンおよびサポートするデータベース/署名に対する日常的な更新をセキュリティツールが受けているかどうかを確認する。
- 会社にとって重大または重要なデータのサンプルを選び、組織の暗号化基準にしたがってデータが保護されているかどうかを確認する。
- 保存されているデータを保護するために用いる暗号化システムが、データを効果的に読み出し不能にしていることを確かめて、科学捜査的な技法を通じて消去されたデータにアクセスするための方法を活用しているかどうかを確認する。
- 悪意ある攻撃と脆弱性からの危険を防止するためにセキュリティコントロールを実施しているかどうかを確認する。
- ポータブルコード（Java、JavaScriptなど）、ダウンロードされたバイナリおよび実行ファイルが、ネットワークへの持込が許可される前にスキャンされるか、ネットワークに入れないようになっているかどうかを確認する。
- 組織のネットワークの文書が、無線機器を含む現在のネットワーク環境を正確に反映していることを判断し、ネットワーク設計を調査して、組織内の信頼されたネットワークと、信頼されていない公共ネットワーク（インターネット）、ベンダ（業務委託先）、またはビジネスパートナー（エクストラネット）のセグメントの間のネットワーク上の境界に、セキュリティバリアが戦略的に配置されているかどうかを確認する。
- セキュリティ関連のパラメータへの変更が、組織の変更管理プロセスにしたがっており、相応に承認されテストされていることを確かめる。
- 重要な情報が、承認されていない人員に開示されたり漏洩したりしていないことを確かめる。

DS6 費用の捕捉と配賦

IT費用をビジネス部門に適正かつ公平に配賦するための体系を実現するには、IT費用を正確に測定し、適正な配賦についてビジネス部門の同意を得る必要がある。このプロセスには、IT費用を捕捉し、サービスを受けるユーザへ配賦および報告するためのシステム上の構築と運用が含まれる。適正な配賦システムを導入することで、ITサービスの利用に関して、ビジネス部門が十分な情報を得た上での決定が可能になる。

コントロール目標	価値のドライバー	リスクのドライバー
DS6.1 サービスの定義 透明性のある費用モデルを実現するため、すべてのIT費用を特定し、これらの費用をITサービスに対応付ける。ITサービスをビジネスプロセスに関連付け、ビジネス部門が関連サービスの費用請求レベルを特定できるようにする。	・IT費用に対するマネジメント層の理解と受け入れの改善と、それによるITサービスへの効果的な予算配分への活用 ・コントロール可能なIT費用について信頼でき明白な情報が与えられ、より効率的なコントロールと資源の優先順位付けを活用できるようなユーザ管理 ・それぞれのビジネス部門の総費用を見ることができ、したがって、より多くの情報を用いて意思決定を行うことができるようなビジネス部門のマネジメント層	・間違って計算された費用 ・正しくない費用情報に基づいた投資の意思決定 ・ITの費用と価値の貢献について間違った見方をしているビジネスユーザ

コントロール設計のテスト

・部門に費用を配分するためのポリシーが存在するかどうかを調査して、それを確認する。
・ITサービスを定義する文書を閲覧して、費用が配賦されるような別個のITサービスが定義され文書化されていることを確かめる
・ITサービスとITインフラストラクチャとの対応関係を閲覧して、たとえば、ハードウェアとソフトウェアの棚卸とITサービスの一覧のコピーを入手して、すべてのインフラストラクチャとサービスが紐づいていることを確かめるなどして、その対応関係が適切であるかどうか判断する。
・紐付けを作成するために用いた情報源を確かめて、その情報源が紐付けの活動にふさわしいかどうかを判断する。
・ITサービスのビジネスプロセスへの対応関係を閲覧して、その紐付けが完全かつ適切になされていることを確かめる。これはたとえば、組織図、ビジネスの命令系統などへの紐付けを比較することで達成することができる。
・紐付けの結果がビジネスプロセスオーナによって確認されているかどうかを調査して、それを確認する。調査するときには、ビジネスプロセスオーナが提供されているITサービスとの対応関係に合意していることを確認することに焦点を置くべきである。
・紐付けの伝達と合意をサポートする文書を閲覧して、合意が達成されたかどうかを判断する。そのような文書として、議事録、予算の文書、およびSLAが挙げられる。

コントロール目標	価値のドライバー	リスクのドライバー
DS6.2 IT財務管理 企業の費用モデルに従って実費用を捕捉し配賦する。企業の財務測定体系に従って、予測と実費用間の不一致を分析し、報告する。	・事業目標とITの費用との間のより効果的で促進された整合性 ・競合するITプロジェクトとITプロセスへのIT資源の配分の促進 ・様々なビジネスプロセスを提供するのに発生するITの総費用を完全に理解できるビジネスユニット ・財務に対する説明責任の増加を通じた、生産性のレベルの高まり、及びIT組織内のスタッフのビジネスに対する見方とプロフェッショナリズムの拡大	・現在の会計モデルが、公平なサービス費用課金をサポートできない状態 ・企業の財務会計ポリシーを遵守していないように記録された費用 ・ITの費用と提供されている価値について間違った見方をしているビジネス部門

コントロール設計のテスト

・定義されている費用要素（IT費用配賦モデルや費用計算システムなど）のコピーを入手して、それを組織全体で定義されている費用要素と比較して、差異が存在するかどうか調べる。
・ITに独特の要素を特定して、定義されている費用要素の適正性を評価する
・ITの費用の配賦を記録するための請求書での費用配分の仕訳入力を閲覧して、そのような配賦の適正性を評価する。たとえば、部門間で比較したり、部門での支出のパーセンテージとして比較したりすることによって、費用配賦の誤りや配賦されていない費用を特定できるだろう。
・企業全体の費用会計システムの仕組みのコピーを入手して、IT支出台帳、部門間の請求書、仕訳入力などを調査することを通じて、IT費用の扱われ方を評価する。
・費用構造の変化に対して予算と予測の改訂を要するような文書のコピーを入手して閲覧して、ビジネスプロセスオーナとITサービスのリーダーとともにその文書をレビューして、そのプロセスが理解され配置されているかどうかを確認する。
・ITの予算、予測、および実際の費用の報告を作成するためのプロセスの文書を閲覧する。
・そのようなプロセスが、組織全体のプロセスと整合的であることを確かめ、初期の予算、予測と今までの実際の費用についての報告の配賦先一覧とスケジュールが適切かどうかを確認する。配賦先の適正性には、影響を受けるすべてのビジネスプロセスオーナ、上級マネジメント層などが含まれる。報告の配布のためのスケジュールの適正性には、ITがビジネスの報告のタイムラインと整合的であることを確かめることが含まれる。
・予算、予測、実際の費用の分析の受領者の役割の定義を評価して、すべての適切な当事者が受領者として割り当てられているかどうかを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS6.3 費用モデルの策定と費用請求 サービスあたりのチャージバック率を計算する際に利用できるサービス定義を基準としたIT費用モデルを策定し、使用する。IT費用モデルの策定により、サービスに対する費用請求をユーザが確実に特定、測定、および予測できるようになり、資源の適切な利用が促進される。	・影響を受けるすべての当事者にとって透明なIT費用の配賦 ・組織におけるIT総費用について組織に提供される信頼できる情報 ・現在の費用と関連づけることができるような投資の意思決定	・全体の会計手続と整合的でない費用モデル ・特定され、課金されたサービスにあるギャップ ・測定が不十分で、ビジネスでの実際の利用を反映していないようなサービス利用方法

コントロール設計のテスト
・IT部門が提供する、課金可能なすべての項目とサービスが、適切に分類され項目化され、それぞれのサービスに対応する課金が列挙されているかどうかを調査して、それを確認する。 ・企業の会計フレームワークに沿って構成要素が組織されていることを確かめる。 ・主要なユーザへのインタビューと、入金相殺明細書に対するユーザ部門の不満のレビューを通じて、入金相殺モデルが明白かつ公平であることを確かめる。 ・ITマネジメント層へのインタビューを通じて、費用と入金相殺のモデルによって効率的な資源計画ができることを確かめる。 ・サンプルとなる資源/サービスを選び、総費用を入金相殺からの収入と比較し、そのギャップを分析する。

コントロール目標	価値のドライバー	リスクのドライバー
DS6.4 費用モデルの保守 費用/課金モデルの適合性を定期的にレビューおよびベンチマーク評価し、進化するビジネスとITのアクティビティに対する妥当性および適合性を維持する。	・ビジネス部門での実際のITサービスの利用と継続して整合的であるようなIT費用の配賦 ・ビジネス部門とIT部門にとって最も適切なアプローチに基づくIT費用の配賦	・実際の利用と整合的でない費用モデル ・ビジネス部門とIT部門でのニーズに適さない形で用いられている費用配賦方法

コントロール設計のテスト
・費用/課金モデルが、現在のビジネス要件およびITサービスの料金と費用の変更を含めて定期的に（毎年または半年おきなど）レビューされているかどうかを調査して、それを確認する。 ・再評価された課金モデルの文書を閲覧して、経営者の承認を探し、運用の有効性を判断する。 ・IT費用課金モデルの実施を要求するポリシーや基準を閲覧して、企業全体のモデルと照らし合わせて定期的にレビューする要件があることを確かめるか、企業全体のモデルへの変更をITモデルに反映させるためのプロセスが存在することを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・部門への費用の配賦が、組織にとって受け入れ可能ないし適切であるかどうかを調査して、それを確認する。
・費用が個別のITサービスに配賦されているかどうかを調査して、それを確認する。
・費用を回収し配賦する責任が適切に割り当てられているかどうかを調査して、それを確認する。

- 費用配賦アプローチを定義する文書を閲覧して、すべての費用が合理的に配賦されているかどうかを確認する。これはたとえば、費用配賦を予算や実際にかかっている費用と比較することで達成できる。
- ITの予算と部門の予算を入手して、ITサービスの費用が部門の予算に存在するかどうかを確認する。
- 部門の予算、部門でサポートされているアプリケーションなどを調べることを通じて、IT予算がビジネスでの必要性と整合的に見えるかどうかを検討する。
- かかっている費用のサンプルを選び、費用を追跡して、費用がITサービスに適切に配賦されていることを確認する。
- 重要な費用（上位10パーセント、重要な部門の費用など）を抽出し、そのような費用を追跡して、それがITサービスに適切に配賦されていることを確認する。
- すべてのIT費用を抽出して、タイプごとに階層化して、ITサービス定義と比較する。
- インフラストラクチャの棚卸のすべてが、提供されているITサービスによって説明され所有されていることを、ITサービスのリーダーに確かめる。これは、ITサービスの地理的な対象範囲と、提供されているアプリケーションとビジネスサービスの性質を調査し、そのような対象範囲をITサービスのリーダと議論することによって、または議論されているITサービスの対象範囲を現在のネットワークダイアグラムで裏付けることによって達成することができる。
- ITサービスのサンプルを選び、提供されているITサービスとサポートのために必要とされている既知のインフラストラクチャの性質を検討することによって、ITインフラストラクチャの配賦の網羅性を調査する。
- ITインフラストラクチャのサンプルを選び、それがITサービスのエリアと紐づいていることを確かめる。
- 資産台帳、ネットワークダイアグラム、または他のインフラストラクチャの棚卸を閲覧して、サービスオーナへの配賦が行われているかどうかを確認する。
- データセンタの視察から資産のサンプルを選び、資産が資産台帳、ネットワークダイアグラム、または他のインフラストラクチャの棚卸に適切に記帳されていることを確かめる。
- 定義された費用要素（人員、収容先、移転、ハードウェア、ソフトウェアなど）が記録されているかどうかを調査して、それを確認する。
- ITの費用の配賦を記録するための請求書/費用配分/仕訳入力を閲覧して、そのような配賦の適正性を評価する。たとえば、部門間で比較したり、部門での支出の割合を比較したりすることによって、費用配賦の誤りや配賦されていない費用を特定できるだろう。
- 部門に配賦されている費用と、IT支出と比較して照合して、完全かつ正確な配賦が生じているかどうかを確認する。
- 総勘定元帳でのIT支出の勘定科目を閲覧して、リスクの高い勘定科目（定期的に用いられていない勘定科目やそこを通じて大量の取引が行われるような勘定科目など）を特定して、通常と異なる入力をレビューする。
- IT部門からのインボイスのサンプルを選び、会計上の扱いが、企業全体の費用配賦モデルに従っていることを確かめる。
- 総勘定元帳の勘定科目から入手したIT費用の情報を分析して、自動転記される仕訳入力や標準仕訳入力の対象となる勘定科目が正しく計上されているかどうかを確認する。たとえば、IT資産の減価償却費を再計算して、ITに対する累積償却が、サービスの利用や割合配分に基づいて部門に適切に配賦されていることを確かめる。
- 費用の配賦に対する承認されていない変更を防止し、費用の配賦への変更を発見/モニタリングするためのプロセスがあることを、ビジネスプロセスオーナとともに確かめる。
- 費用構造の変更のサンプルを閲覧して、影響を受ける部門の予算と予測が改訂され、その数値が正しいことを確かめる。
- 変更ログを閲覧して重要な変更や新規システムの配備を特定して、そのような変更が費用構造に影響を及ぼし、その結果として予算と予測を変更することになったかどうかを確認する。
- 予算化された費用、予測された費用、実際の費用の間の差異の分析を閲覧して、それがタイムリーに完了し、かつ十分に詳細かどうかを確認する。分析が組織の基準と整合的に実施されたかどうかを評価する。
- 配布先一覧を閲覧して、関連する上級マネジメント層とビジネスプロセスオーナのすべてが分析結果を

受領したかどうか検証する。
- 自らの部門に配賦されるITサービス費用の変更の知らせをどのように受けたかを、ビジネスプロセスオーナに確認する。
- 不明確な費用や価格づけの手続による質問に対するフォローアップが直ちに行われ、概略分析のために記録されているかどうかを調査して、それを確認する。システムの至る所に質問を行い、運用の有効性を決定して、即時のフォローアップを確認する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 企業全体の支出割合としてIT支出を比較して、たとえば過去数年間にわたる傾向分析や業界基準に対するベンチマーキングを用いることによって、IT支出が合理的に見えるかどうかを確認する。
- IT支出勘定のそれぞれからの支出の統計的サンプルを選び、統計的な外挿によって、配賦の誤りの影響と勘定ないし部門が影響を受ける方法を判断する。
- 部門に配賦されている費用と、IT支出と比較して照合して、完全かつ正確な配賦が生じているかどうかを確認する。
- 人事記録を閲覧して、費用構造が最後に変更されてからの人数の変化を判断し、その変化が費用モデルに及ぼす影響を定量化する。去年から今年にかけての給与台帳を比較して、給与支出の一貫性および、そのような変化が費用モデルに反映されているかどうかを評価する。
- 変更ログを閲覧して重要な変更や新規システムの配置を特定して、そのような変更が費用構造に影響を及ぼしたかどうかを確認し、費用モデルへの影響を定量化する。
- 去年から今年にかけて資産台帳を比較して、重要な新規の資産を特定して、そのような資産がたとえば減価償却や償却の点から費用構造に影響したかどうかを確認する。廃棄された重要な資産が適切に除却されていないかどうかを評価する。
- IT部門からの予算、予測、実際の費用についての情報が無いことで、費用を管理する能力に支障を来したかどうかを、ビジネスプロセスオーナに尋ねる。そのようなプロセスオーナとの議論を通じて影響度を判断する。
- IT部門が提供する、課金可能なすべての項目とサービスが、項目化され、それぞれのサービスに対応する課金が列挙されているかどうかを調査して、それを確認する。
- IT支出勘定のそれぞれからの支出の統計的サンプルを選び、統計的な外挿によって、配賦の誤りの影響と勘定ないし部門が影響を受ける方法を判断する。

DS7 利用者の教育と研修

IT部門内を含むITシステムの全ユーザに対して効果的な教育を実施するには、ユーザグループごとの研修のニーズを特定する必要がある。このプロセスには、ニーズの特定のほかに、効果的な研修のための戦略の策定と実施、および結果の測定が含まれる。効果的な研修プログラムにより、ユーザによるエラーの減少、生産性の向上、および主要コントロール（ユーザセキュリティ対策など）へのコンプライアンスの強化を実現でき、技術を一層効果的に利用できるようになる。

コントロール目標	価値のドライバー	リスクのドライバー
DS7.1 教育と研修のニーズの特定 研修対象の各従業員グループに対し、以下を考慮して研修カリキュラムを策定し、定期的に更新する。 ・ 現在/将来のビジネス上の必要性と戦略 ・ 資産としての情報の価値 ・ 企業の価値基準（倫理基準、コントロールおよびセキュリティの企業風土など） ・ 新規ITインフラストラクチャやソフトウェア（パッケージおよびアプリケーション）の導入 **・現在と将来のスキル、能力プロファイル、公的資格、資格取得に関する必要性、および必要に応じた見直し** ・ 実施方法（セミナー型、eラーニング型など）、対象グループの規模、参加のしやすさ、および実施時期	・ ビジネス要件を満たすために、要員に対する、特定された研修の必要性 ・ 組織の技術を要員が現在と将来の両方で効果的に用いるためのベースライン ・ 現在および将来に組織が直面するリスクと機会に関係ある研修と教育プログラムの確立 ・ ビジネスでの必要性を満たすために最適化されている、インストールされたアプリケーションの能力	・ 自らの職務機能を満たすのに不十分な研修しか受けていないスタッフメンバー ・ 効果的でない研修メカニズム ・ 研修の必要性にそぐわない形で提供されている研修 ・ 十分に活用されていない、インストールされたアプリケーションの能力

コントロール設計のテスト

・IT担当者の研修と専門技能開発のための計画が存在するかどうかを調査して、それを確認する。
・ カリキュラムを入手して、その網羅性について閲覧する（カバー範囲の深さと広さ、授業の頻度、授業のスケジュール、授業の複雑さ、研修の提供元—ベンダローカルか業界団体かなど）
・ 研修カレンダーを入手して閲覧する。
・ 研修予算を入手して閲覧する。
・ テストの解答用紙、得点、出欠確認のコピーを入手する（オンライン研修コースでの試験と出席の証拠など）
・ マネジメント層が従業員技能記録表を作成し維持するためのプロセスを判断する。
・ 従業員技能記録表カタログを入手してレビューして、記録されている技能が、設置されたシステムと対応づけられているかどうかを確認する。
・ 技能データベースが最新であり利用可能な知識が最新の状態を維持していることを確認する。
・ 研修戦略を閲覧して、研修の必要性がユーザ個人のパフォーマンス計画に取り込まれていることを確かめる。
・ サービスデスクの報告から、研修を含む根本原因を分析するための要件の詳細を記した文書を閲覧する。

コントロール目標	価値のドライバー	リスクのドライバー
DS7.2 教育と研修の実施 特定された教育と研修のニーズに基づいて、研修対象グループとそのメンバー、効果的な実施方法、講師、トレーナー、およびメンターを定める。トレーナーを任命し、適時に研修セッションを計画する。登録者（受講の前提条件を含む）、出席状況、および成績評価を記録する。	・正式化され周知されているような、研修に対するマネジメント層のコミットメント ・効果的な研修講師と研修プログラム ・研修プログラムとセッションへの十分な参加と関与	・不適切で効果的でない研修プログラムとメカニズムの選択 ・陳腐化した研修教材の使用 ・貧弱な参加と関与の記録

コントロール設計のテスト

・研修スケジュールをレビューして、それが研修の必要性に合致していることを確かめる。
・研修を提供するのに十分な資源が利用できることを確かめる。
・研修プログラムのサンプルを分析して、以下を確かめる。
– 内容と目標
  – 予定出席者数と実際の出席者数
  – 出席者の満足度
  – 受け取ったフィードバックの利用

コントロール目標	価値のドライバー	リスクのドライバー
DS7.3 受講研修内容の評価 教育と研修の終了後、その実施内容について、妥当性、内容の質、有効性、保有知識、費用と価値の面から評価する。この評価の結果を、将来のカリキュラムの策定と研修セッションに役立てる。	・ユーザのフィードバックに基づく効果的な研修プログラム ・関連性のある研修プログラム ・研修プログラムの品質向上 ・ユーザが知識を保持し再利用するために、適切に設計され構築されている研修内容 ・費用（財務、教材など）と付加価値に対する効果的な追跡/モニタリング	・不適切で効果的でない研修プログラムの選択 ・陳腐化した研修教材の使用 ・エンドユーザ研修プログラムの質の低下 ・知識の保持と再利用を支援していないような、研修内容の設計と構造 ・便益と付加価値を上回るような研修費用

コントロール設計のテスト

・評価フォームをレビューして、それが内容の品質と妥当性および期待に合致するレベルを効果的に測定していることを確かめる。
・将来の研修カリキュラムの策定に有用なフォーマットへとフィードバックが要約されているかどうかを確認する。
・フォローアップ活動の一覧を入手して、それが実行されたという証拠を得る。
・ターゲットとなる出席率に到達したことを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・追加教育と自習のプログラムへの参加を促すべき人員へのマネジメント層からの伝達をレビューする。
・研修費用の返還要求を入手してレビューする。
・ベンダが提供する研修教材（マニュアル、CD、研修パケット、シラバスなど）の一覧を入手する。

・ITライブラリにおける教育書の在庫状況を入手してレビューする
・ 個々の担当者と対話して、部門や組織の要件と整合的な研修計画を立てているかどうかを確認する。
・ インシデント管理記録を閲覧して、技能にギャップがあることを示すシステムのサポートと利用の傾向を特定する。
・ 環境をサポートするのにどのような特定の能力が求められるかについてマネジメント層に尋ね、組織のためにそのような技能を構築し維持するための計画や、サードパーティアレンジメントを通じてそのような技能を獲得するための計画が存在するかどうかを確認する。
・ 個人の成果計画のサンプルを閲覧して、技術研修の必要性が取り込まれているかどうかを確認する。
・ 業績評価の結果と特定された潜在的な技能ギャップに関してマネジメント層に尋ねる。
・ 問題管理記録を閲覧して、技能にギャップがあることを示すシステムのサポートと利用の傾向を特定する。
・ 効果的な研修プログラムを定義するためのプロセスに対してウォークスルーを実施して、以下を確認する。
  – 時期を含むすべての関連する必要性が考慮されているか
  – 研修セッションが特定された研修の必要性に効果的に合致しているか
  – 提供メカニズムについての情報が最新の状態を保っているか
  – 講師とプログラムの最近の評価がレビューされているか
・ 研修の出席と完了の記録および教育プログラムを、その正確性に関して閲覧する。
・ 参加者とトレーナーのフィードバックを、完了した研修セッションのサンプルから閲覧する。
・ ユーザにインタビューして、研修セッションに対する理解度を評価して、それからテスト結果をレビューして、テストが、セッションの内容の品質と妥当性および期待に合致するレベルを効果的に測定していることを確かめる。
・ 利害関係者が教育と研修についてインタビューを受け、フィードバックを提供されているかどうかを調査して、それを確認する。
・ 業績評価の結果と研修が提供されたエリアで特定された潜在的な技能ギャップに関してマネジメント層に尋ねる。
・ 研修が提供された後でユーザの有効性と知識が改善したかどうかを、マネジメント層とユーザに尋ねる。
・ サービスデスクコールの減少やユーザの生産性といった、研修が意図した通りの影響を与えているかどうかを示す指標が評価されているかどうかを確認する。
・ コース評価を閲覧して、提供された研修に対する受講者の満足度を判断する。特に、講師、コースの内容、コースの場所についての満足度を検討する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・ 人員のファイル/レジュメを入手して、技能が職務/地位にふさわしいかどうかを分析する。
・ 人員のファイル/レジュメを入手して、配備されているシステムと照らし合わせて技能を分析する。
・ マネジメント層に質問して、報告書（月末と年度末の会計と報告の修正一覧など）をレビューして、処理された情報の修正が要求されているかどうかを確認する。ユーザの知識が不十分なせいで誤った情報が生じたかどうかを分析して判断する。
・ 研修や技能が定義されていないエリアでのサービス中断時間に伴う合計費用を決定して、それを他のエリアやピアグループでのサービスコストと比較する。
・ インシデント管理記録を閲覧して、技能にギャップがあることを示すシステムのサポートと利用の傾向を特定する。
・ 業績評価の結果と、研修が提供されたエリアなどで特定された潜在的な技能ギャップに関してマネジメント層に尋ねる。
・ サービスデスクコールの減少やユーザの生産性といった、研修が意図した通りの影響を与えているかどうかを示すベンチマーク指標を評価する。

DS8 サービスデスクとインシデントの管理

ITユーザの問い合わせや発生した問題に対してタイムリーかつ効果的に対応するには、適切に構成、運用されているサービスデスクとインシデント管理プロセスが必要である。このプロセスには、インシデント登録、インシデントエスカレーション、傾向と根本原因の分析、および問題解決の機能を持つサービスデスクの設置が含まれる。ビジネス上の便益には、ユーザからの問い合わせに対する迅速な対応による、生産性の向上が含まれる。さらに、効果的な報告を通して、ビジネス部門はユーザ研修の不足といった根本原因の追究に取り組むことができる。

コントロール目標	価値のドライバー	リスクのドライバー
DS8.1 サービスデスク すべての問い合わせ、報告されたインシデント、およびサービスと情報に関する要求を登録、伝達、処理、分析し、ユーザとIT部門とをつなぐ機能を果たすサービスデスクを設置する。該当SLAに関連する、合意されたサービスレベルに基づくモニタリングおよびエスカレーション手続が存在し、報告されたすべての課題を、インシデント、サービス要求、情報要求のいずれかに分類し、優先順位付けすることが可能になっている必要がある。サービスデスクとITサービスの質に対するエンドユーザの満足度を測定する。	・顧客満足度の向上 ・定義されており測定可能な、サービスデスクのパフォーマンス ・タイムリーに報告され、フォローアップされ、解決されるインシデント	・サービス中断時間の増加 ・顧客満足度の低下 ・報告されたインシデントに対するフォローアップ手続を知らないユーザ ・再発する問題への不対処

コントロール設計のテスト

・ITサービスデスクが存在するかどうかを調査して、それを確認する。
・サービスデスクのモデル、人員、ツール、他のプロセスとの統合を決定するための分析を実施しているかどうかを調査して、それを確認する。
・運用時間とコールに対する期待レスポンスタイムがビジネス要件に合致していることを確かめる。
・サービスデスクスタッフが直ちに解決できないような問い合わせを扱うための指示が存在するかどうかを調査して、それを確認する。問い合わせには優先度のレベルをつけて、望ましい解決時間とエスカレーション手続を判断するようにすべきである。
・サービスデスクのためのツールが、サービス定義とSLAの要件にしたがって導入されているかどうかについて、関係者に尋ねる。
・サービス基準が存在し、その基準を顧客に伝達しているかについて調査する。

コントロール目標	価値のドライバー	リスクのドライバー
DS8.2 顧客からの問い合わせの登録 問い合わせ、インシデント、サービス要求、情報要求を記録および追跡するための機能とシステムを確立する。このシステムは、インシデント管理、問題管理、変更管理、キャパシティ管理、および可用性管理といったプロセスと密接に連携する必要がある。インシデントはビジネスおよびサービスの優先度に基づいて分類し、必要に応じて該当する問題管理チームに転送する。顧客に対しては、それぞれの問い合わせへの対応状況を常に通知する。	・タイムリーに効率的に解決するインシデント ・エンドユーザへの付加価値 ・インシデント解決のための説明責任	・すべてのインシデントが追跡されているわけではない状態 ・ビジネスでの必要性を反映していないような、インシデントの優先順位付け ・タイムリーに解決しないインシデント

コントロール設計のテスト
・顧客からの問い合わせ、状況、解決へ向けての行動を登録するためのプロセスとツールが用いられていることを確かめる。 ・この対処法をどれくらい完全かつ正確に維持しているかを評価する ・顧客からの問い合わせに対処し、上申するためのワークフローがプロセスに含まれていることを確かめる。 ・開始して終了した顧客の問い合わせのサンプルをレビューして、プロセスとサービスのコミットメントの遵守をチェックする。

コントロール目標	価値のドライバー	リスクのドライバー
DS8.3 インシデントエスカレーション 速やかに解決できないインシデントを、SLAで定められている制約の範囲内で適切にエスカレーションし、必要に応じてワークアラウンド（回避策）の提示を可能にする、サービスデスクの手続を確立する。インシデントの解決をどのITグループが担当しているかにかかわらず、ユーザから報告されたインシデントの担当とライフサイクルのモニタリングは、確実にサービスデスクが担う。	・顧客満足の向上 ・問題解決のための一貫したプロセス ・解決したインシデントに対する説明責任 ・インシデント解決の進捗の明確な追跡	・資源の非効率な利用 ・サービスデスクのための資源の可用性の欠如 ・インシデント解決に対してフォローアップする能力の欠如

コントロール設計のテスト

- サービスデスクが、顧客に関連する要求とインシデントのオーナーシップを維持しているかどうかを調査して、それを確認する。
- 要求/インシデントの端から端までのライフサイクルが、サービスデスクによって適切にモニタリングされ、上申されていることを確かめる。
- 重要なインシデントがマネジメント層に報告されていることを、マネジメント層のメンバーに確かめる。
- 重要なインシデントをマネジメント層に報告するための手続をレビューする。
- それぞれの問い合わせに対する日付と時刻およびIT担当者の割り当てを示すために、インシデント記録が更新されるプロセスの存在を確かめる。
- IT担当者が問い合わせとインシデントの扱いに関与し、インシデント要求記録がそのライフサイクルを通じて更新されるプロセスが存在するかどうかを調査して、それを確認する。

コントロール目標

DS8.4 インシデントのクローズ

顧客からの問い合わせへの対応完了をタイムリーにモニタリングするための手続を確立する。インシデントが解決された段階で、サービスデスクが問題解決に向けて講じたステップを記録し、顧客と合意した対応が取られていることを確認する。また既知のエラーやワークアラウンド(回避策)といった未解決のインシデントについては、適切な問題管理に関する情報を提供できるように、記録と報告を行う。

価値のドライバー

- 顧客満足度の向上
- 一貫していて体系的なインシデント解決プロセス
- 問題の再発防止

リスクのドライバー

- 誤った情報収集
- よく起きるインシデントが適切に解決されない状態
- タイムリーに解決されないインシデント

コントロール設計のテスト

- それぞれのインシデントの解決を管理するためのプロセスがあるかどうかを調査して、それを確認する。
- 解決されたインシデントのすべてで、インシデントを解決するためのすべてのステップの詳細なログを含めて、詳細が記述されているかどうかを調査して、それを確認する。
- インシデントのサンプルを調査して、解決とクローズを含むインシデントのライフサイクルの管理状況が報告されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS8.5 報告と傾向分析 サービスデスクのアクティビティに関する報告書を作成する。この報告書により、マネジメント層がサービスの成果と対応時間を測定して、傾向や再発性のある問題を特定できるようになり、サービスの継続的な改善が可能になる。	・サービス中断時間の減少 ・顧客満足度の向上 ・提供されているサービスに対する信頼 ・測定され最適化された、ヘルプデスクのパフォーマンス	・ビジネス活動をサポートしていないサービスデスク活動 ・提供されているサービスに満足していない顧客 ・タイムリーに解決しないインシデント ・顧客向けのサービス中断時間の増加

コントロール設計のテスト
・解決のための合意されたタイムフレームを超過した問い合わせのすべてを特定し、さらに調査し、報告するためのプロセスがあるかどうかを調査して、それを確認する。 ・問題の特定をサポートすべく、繰り返されるインシデントとパターンを特定するために、すべての問い合わせに対して傾向分析を行っているかどうかを調査して、それを確認する。 ・インシデントと傾向の分析データを問題管理に定期的に提供しているかどうかを確かめる。 ・サービスデスクが提供するサービスに対する満足度を評価するために、顧客から受け取ったフィードバックに対する分析を実施しているかどうかを調査して、それを確認する。 ・顧客のフィードバックに対する分析報告が存在することを確かめ、サービスを改善するために是正措置を取っているかどうかを確かめる。 ・サービスデスクのパフォーマンスが業界基準と比較されていることを確かめる。 ・継続的な改善のためにベンチマーク分析を用いているかどうかを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・顧客とユーザがサービスデスク基準についてどのように知らされているかを確かめ、それらの方法（サービスデスクやオンラインでの掲示など）の存在を調査する。
・ユーザフィードバックログの存在を確かめる。
・顧客満足度のモニタリングと改善の点からシステムの有効性について調査する。
・サービスデスクパフォーマンス報告の存在について調査する。
・直ちに解決しなかったコールのログへの入力のサンプルを閲覧して、適切なエスカレーション手続に従ったかどうかを確認する。
・報告された測定指標が、サービスデスクでの関連する到達目標に対処しているかどうかを調査する。誰が何の目的で報告を利用するかについて調査する。
・サービスデスクコールのいくつかをモニタリングして、既存の手続に従っているかどうかを確かめる。サービスインシデント追跡システムと観察されたコールを突合する。
・ポリシーにしたがって、インシデントに適切に優先順位をつけているかどうかを調査して、それを確認する。
・インシデントチケットのサンプルをレビューして、ポリシーへの遵守を確かめる。
・問い合わせのサンプルを選び、それぞれの問い合わせに対して日付と時刻とIT担当者の割り当てを示すようにインシデント記録が更新されていることを確かめる。
・トラブルインシデントの文書のサンプルを閲覧して、そのようなインシデントがポリシーによって設定されている優先レベルに従っていることを確かめる。
・ユーザがインシデント解決の進捗について知らされているかどうかを調査して、それを確認する。
・すべての要求書とインシデント記録が、そのライフサイクルを通じてモニタリングされ、定期的にレビューされ、顧客の問い合わせをタイムリーに解決することが保証されているかどうかを調査して、それを確認する。
・要求した人が確認した後でのみ要求とインシデントがクローズされるかどうかを調査して、それを確認する。

- インシデントのサンプルを調査して、解決のためのマニュアルや自動化されたフォローアップが存在することを確かめる。
- インシデントがレビューされ、次善策、既知のエラー、根本原因を含めて知識ベースへ更新されて、将来に生じる同様のインシデントに備えていることを、閲覧を通じて確かめる。知識ベースを物理的に閲覧して、入力のサンプルを閲覧して、次善策、もしわかれば根本原因も含まれていることを確かめる。
- インシデント記録のサンプルを閲覧して、それがSLAにしたがってモニタリングされ記入されているかどうかを確かめる。
- 記録のサンプルを選び、それがクローズのために閲覧されたかを要求者と確かめる。
- （影響度や緊急度などによる）インシデント分類のための適切な定義が存在するかどうかを特定する。
- 機能的および階層的なエスカレーションが定義されているかどうかを特定する。
- インシデント管理が、継続/緊急事態対応計画と明確にリンクしているかどうかを調査して、それを確認する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- サービスデスクへのコールのいくつかを観察して、文書化されていない手続を確かめる。文書化されていないエスカレーション手続では、サービスデスクが解決できないというトラブルチケットを、適切なIT担当者に割り当てるべきである。
- すべての重大なサービスコールに対して、サービスデスク・マネージャーやシニアスタッフメンバーが優先順位をつけていることを確かめる。
- ITサポートチームの業務を観察して、インシデントのログを取り優先順位をつけるための、文書化されていない手続を記録する。

DS9 構成管理

ハードウェアとソフトウェアの構成のインテグリティを確保するには、正確かつ網羅された構成管理用リポジトリの作成と保守が必要である。このプロセスには、初期構成情報の収集、ベースラインの設定、構成情報の検証と監査、および必要に応じた構成管理用リポジトリの更新が含まれる。効果的な構成管理により、システムの可用性が向上し、作業上の課題が最小限に抑えられ、課題を速やかに解決できるようになる。

コントロール目標	価値のドライバー	リスクのドライバー
DS9.1 構成リポジトリとベースライン 構成管理アイテムに関するあらゆる関連情報を含む集中管理リポジトリと支援ツールを作成する。すべての資産と資産の変更を監視し記録する。あらゆるシステムとサービスに対する構成管理アイテムについて、変更後に復元するためのチェックポイントをベースラインとして保持する。	・ビジネスサービスを維持するための効果的に計画されたハードウェアとソフトウェア ・企業全体にわたって一貫して展開している構成 ・変更が全体のアーキテクチャに従うよう拡張された計画 ・供給業者を集約することによる費用の節約 ・迅速なインシデント解決	・変更が全体の技術アーキテクチャを遵守できない状態 ・適切に保全されていない資産 ・ハードウェアとソフトウェアに対する承認されていない変更が発見されず、セキュリティ違反になりうる状態 ・文書化されているが現在のアーキテクチャを反映していない情報 ・フォールバックする能力の欠如

コントロール設計のテスト
・上級マネジメント層が、構成管理部門の対象範囲と評価基準を設定し、パフォーマンスを評価しているかどうかを調査して、それを確認する。 ・リポジトリ内の構成管理情報のログを効果的に取ることができるようにするためのツールを用いているかどうかを調査して、それを確認する。 ・そのツールへのアクセスが適切な人員に制限されていることを判断する。 ・構成項目のサンプルをレビューして、一意的な識別子が割り当てられていることを確かめる。 ・構成ベースラインが構成要素ごとに定義され文書化されているかどうかを調査して、それを確認する。 ・ベースラインによって、特定の時点でのシステム構成情報を特定できるようになっていることをレビューする。 ・ベースラインの構成へと戻すための文書化されたプロセスが存在するかどうかを調査して、それを確認する。 ・システムとアプリケーションをベースライン構成へと戻すことができることを確かめることによって、システムとアプリケーションのサンプルをテストする。 ・定義されたリポジトリとベースラインに対する変更をモニタリングするためのメカニズムが存在するかどうかを調査して、それを確認する。 ・マネジメント層が定期的な報告を受けており、このような報告によって、継続改善計画が策定されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS9.2 構成管理アイテムの識別と保守 構成リポジトリに対するすべて変更の管理とログ記録をサポートする構成管理手続を策定する。これらの手続と、変更管理、インシデント管理、および問題管理の手続を統合する。	・効果的な変更管理とインシデント管理 ・会計要件の遵守	・ビジネスにとって重大な構成要素を特定できていない状態 ・コントロールされていない変更管理と、それによるビジネスの中断 ・不正確な情報による、変更の影響を評価する能力の欠如 ・資産を正確に計上する能力の欠如

コントロール設計のテスト

・すべての構成項目とその属性が特定され維持されるようにするためのポリシーがあるかどうかを調査して、それを確認する。
・物的資産にタグをつけるためのポリシーが存在するかどうかを調査して、それを確認する。
・ポリシーにしたがって、資産に物理的にタグをつけられていることを確かめる。
・役割に基づくアクセスポリシーが存在するかどうかを調査して、それを確認する。
・ポリシーの通りに、承認され適切な人員が構成リポジトリへのアクセスを指名することを確かめる。
・変更管理と問題管理の手続が構成リポジトリの維持と統合されるようにするためのポリシーがあるかどうかを調査して、それを確認する。
・新規の構成項目、改変された構成項目、削除された構成項目を記録して、構成リポジトリでの構成項目相互の関係を特定し維持するプロセスがあるかどうかを調査して、それを確認する。
・関連する文書、プロセスのタイムリーな実行、およびプロセスのデータインテグリティを調査する。
・重大な構成項目を特定するための分析がなされるようにするためのプロセスがあるかどうかを調査して、それを確認する。
・将来の処理要請と技術調達の変更管理および分析を、プロセスでサポートしていることを確かめる。
・調達手続で、新規の資産を構成管理ツールに記録するようになっているかどうかを調査して、それを確認する。
・確認管理データが調達記録と適合することを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
DS9.3 構成のインテグリティのレビュー 検証すべき構成データを定期的にレビューして、現在と過去の構成にインテグリティが保持されていることを確認する。現在インストールされているソフトウェアについて、ソフトウェア使用ポリシーに照らし合わせて定期的にレビューを行い、個人的に使用しているソフトウェアやライセンスのないソフトウェア、またはライセンス契約の規定数を超えるソフトウェアがないことを確認する。。不備や逸脱がある場合は報告、対処と修正を行う。	・ベースラインからの逸脱の特定 ・問題の特定と解決の向上 ・承認されていないソフトウェアの特定	・ビジネスにとって重大な構成要素を特定できていない状態 ・コントロールされていない変更管理と、それによるビジネスの中断 ・資産の不正利用 ・問題解決のための費用の増加

コントロール設計のテスト

- すべての構成データのインテグリティを定期的に保証するためのプロセスがあるかどうかを調査して、それを確認する。
- 記録されたデータを物理的環境と比較する報告書をレビューする
- 逸脱が報告され是正されていることを確かめる。
- ハードウェアとソフトウェアの照合が、構成データベースと照らし合わせて定期的に実施されていることを確かめる。
- 自動化ツールが利用されている場合には、自動化された記録と照らし合わせて手作業での照合を実施する。
- ソフトウェアの私的利用、ライセンスを受けていないソフトウェアの利用、また現在のライセンス合意を超過するソフトウェアの事例を発見するために、ソフトウェア利用ポリシーと照らし合わせて定期的なレビューが実施されていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
- 構成変更の失敗やセキュリティ違反が今まで起きたかどうかをマネジメント層に尋ね、そのような問題点が企業資産の損失や情報漏洩やサービス中断を引き起こしたかどうかを確認する。
- ログツールへのアクセスが適切な人員に制限されていることを判断する。
- 構成項目のサンプルをレビューして、一意的な識別子が割り当てられていることを確かめる。
- ベースラインによって、特定の時点でのシステム構成情報を特定できるようになっていることを確かめる。
- ベースラインの構成へと戻すための文書化されたプロセスが存在するかどうかを調査して、それを確認する。
- 構成の変更を発見するために設計されているツールの出力結果を閲覧して、そのような変更が組織の設計仕様とセキュリティ戦略と整合的であるかどうかを評価する。
- 構成管理データベース（CMDB）のために用いるツールを調査して、CMDBが提供する情報の量と質が、すべてのITプロセスにとって適切であることを確かめる。
- 構成情報が、冗長な情報システムによって保持されているかどうかを判断する。
- デスクトップのサンプルを選び、構成および配置されているソフトウェアを、ベースライン基準と照らし合わせて調査して、承認されていない変更がなされていないことを確かめる。
- ライセンスを受けていないソフトウェアの利用が防止されているか、および承認されていないソフトウェアを発見するための手続が存在するかどうかを特定する。
- マネジメント層が定期的な報告を受けており、このような報告によって、継続改善計画が策定されていることを確かめる。
- システムとアプリケーションをベースライン構成へと戻すことができることを確かめることによって、システムとアプリケーションのサンプルをテストする。
- 展開している技術に対する脆弱性評価ツールを入手して、それを実行して、既知の脆弱性が是正されているかどうかを確認する。
- 構成情報をレビューし、構成項目相互の関係を文書化するために、何を文書化すべきかを決定する（構成項目、インシデント記録、変更記録、変更スケジュール、可用性情報、サービスレベルなど）

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 構成変更の失敗やセキュリティ違反が今まで起きたかどうかをマネジメント層に尋ね、そのような問題点が企業資産の損失や情報漏洩、サービス中断を引き起こしたかどうかを確認する。
- 構成の評価についての内部または外部の報告書のコピーを閲覧して、構成上の欠陥が特定されているかどうかを確認する。
- 展開している技術に対する脆弱性評価ツールを用いて、既知の脆弱性が是正されているかどうかを確認する。

DS10 問題管理

効果的な問題管理を実施するには、問題を特定および分類し、根本原因を分析し、問題を解決する必要がある。問題管理プロセスには、改善のための提案事項の策定、問題の記録保持、および是正措置の状況のレビューも含まれる。効果的な問題管理プロセスにより、システムの可用性が最大限に確保されるほか、サービスレベルの向上、費用削減、および顧客の利便性と満足度の向上を実現できる。

コントロール目標	価値のドライバー	リスクのドライバー
DS10.1 問題の特定と分類 インシデント管理の過程で特定された問題を報告、分類するためのプロセスを導入する。問題分類の手続はインシデント分類の手続に類似しており、カテゴリ、影響度、緊急度、優先度の決定が含まれる。問題は、関連するグループやドメイン(ハードウェア、ソフトウェア、サポートソフトウェアなど)別に適切に分類する。各グループは、ユーザ/顧客ベースに対して組織上の責任を負うものとし、このグループを基準にそれぞれの問題を各サポートスタッフに割り当てる。	・サービスデスクのパフォーマンスをサポートするツール ・積極的な問題管理 ・エンドユーザ研修の向上 ・効率的かつ効果的な問題とインシデントの取り扱い ・タイムリーに解決される問題とインシデント ・ITサービスの質の改善	・ITサービスの中断 ・問題の再発の可能性の増加 ・タイムリーに解決されない問題とインシデント ・積極的な問題管理とインシデント管理のための、問題及びインシデント、その解決策に関する監査証跡の欠如 ・インシデントの再発

コントロール設計のテスト
・問題を特定し分類するのに適切なツールにサポートされた十分なプロセスがあるかどうかを調査して、それを確認する。 ・問題を分類して優先順位をつけるための確立した基準をレビューして、それによってサービス義務および問題を解決したり封じ込めたりすることに責任を持つ組織単位に沿って問題が分類されるようになっていることを確かめる。 ・分類の正確性のためのプロセスがあることを確かめ、分類の誤りに対処できるよう、その理由を特定する。 ・問題データベースから代表的なサンプルを取り、問題が適切に分類されカテゴリー分けされていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS10.2 問題の追跡と解決 問題管理システムは、報告されたすべての問題を追跡、分析し、その根本原因を判別するための、適切な監査証跡機能を次の情報に対して提供する必要がある。 ・関連するすべての構成管理アイテム ・未解決の問題とインシデント ・既知のエラーとエラーの疑い ・問題の傾向の追跡 根本原因に対処する維持できる解決策を特定して実施し、確立されている変更管理プロセスに従い変更要求を提出する。解決プロセス全体にわたって、問題管理は、変更管理から問題やエラーの解決状況に関する報告を定期的に受ける必要がある。問題管理は、問題と既知のエラーのユーザサービスに対する継続的な影響をモニタリングする。この影響が深刻化した場合は、問題管理はその問題を適切な会議体にエスカレーションして、変更要求(RFC)の優先順位を上げるか、または必要に応じて緊急の変更措置を実施する。問題解決の進捗状況は、SLAに照らし合わせてモニタリングする必要がある。	・ITサービスの中断やITサービスの品質の低下が限定された状態 ・問題とインシデントの効率的かつ効果的な取り扱い ・問題発見から解決までの経過時間の最小化 ・合意済みのサービスレベルに関する適切な問題解決 ・ITサービスの品質の改善	・問題とインシデントの再発 ・情報の紛失 ・適切に解決されない重大インシデント ・ビジネスの中断 ・不十分なサービスの品質

コントロール設計のテスト
・問題を登録し、分類し、優先順位をつけ、解決まで追跡するためのプロセスとツールが用いられていることを確かめる。 ・問題についての管理レポートを作成するために用いる報告機能がツールに含まれていることを確かめる。 ・問題報告のサンプルを選び、以下が十分かどうかを確かめる。 – 根本原因を分析するための問題の文書化 – 問題のオーナシップと解決の実行責任の特定 – 問題の状況についての情報

コントロール目標	価値のドライバー	リスクのドライバー
DS10.3 問題のクローズ 既知のエラーを成功裡に取除いたことを確認した後、または別の方法で問題を処理することをビジネス部門と合意した後、その問題の記録をクローズするための手続を整備、運用する。	・合意済みのタイムフレーム内で解決する問い合わせ ・顧客とユーザの満足度の改善 ・効率的かつ効果的な問題とインシデントの取り扱い ・将来、類似する問題が生じたときに過去からの教訓を応用する能力	・未処理の問い合わせ ・サービス中断の増加 ・適切に解決されない重大インシデント ・ITサービスに対する不満

コントロール設計のテスト

・利害関係者が解決を確認した後でのみ問題がクローズするかどうかを調査して、それを確認する。
・問題の代表的なサンプルを選び、利害関係者へのインタビューを通じて、利害関係者が問題のクローズを完全かつタイムリーに知らされていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS10.4 構成管理、インシデント管理、および問題管理の統合 関連する構成管理、インシデント管理、および問題管理のプロセスを統合して、問題を効果的に管理し、改善を図れるようにする。	・顧客満足度の改善 ・効率的かつ効果的な問題とインシデントの取り扱い ・文書化された問題とインシデントの報告 ・効果的なサービス管理	・情報の紛失 ・適切に解決されない重大インシデント ・ビジネスの中断 ・問題の件数の増加 ・ITサービスへの満足度の低下

コントロール設計のテスト

・構成管理、インシデント管理、問題管理のプロセスをレビューして、それらが適切に統合されていることを確かめる。
・記録をレビューして、異なるエリアに責任を持つ管理者が定期的に会合を持ち、共通の問題点を解決していることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・インシデントリストをインシデント報告とエラーログと比較して、インシデントプロセスが正しく機能していることを確かめる。
・問題の特定と取り扱いの文書の存在を確かめる。
・報告書のサンプルを閲覧して、それがしかるべきときに用いられ、必要な情報を含んでいることを確かめる。
・既知のエラー、インシデント分析ツール、および根本原因が、インシデント管理プロセスへと伝達されていることを確かめる。
・問題処理プロセスの状況が、変更管理と構成管理からのインプットを含めて、そのライフサイクルを通じてモニタリングされていることを確かめる。
・構成管理、インシデント管理、問題管理のプロセスオーナーの間で行なわれた会合のスケジュールと議事録をレビューする。
・問題の総費用についての記録と報告を閲覧しレビューする。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

・ ITサービスの全体的な改善を判断するために、問題管理プロセスから生じた変更がモニタリングされているかどうかを調査して、それを確認する。

DS11 データ管理

効果的なデータ管理を実施するには、データ要件を特定する必要がある。データ管理のプロセスには、メディアライブラリ、データのバックアップと復元、およびメディアの適切な廃棄に関する管理手続の確立も含まれる。効果的なデータ管理は、ビジネスデータの質、適時性、および可用性の保証に有用である。

コントロール目標	価値のドライバー	リスクのドライバー
DS11.1 データ管理におけるビジネス要件 処理すべきデータがすべて完全で正確で、しかも遅延なく受信、および処理され、出力がすべてビジネス要件に従って提供されていることを検証する。再開と再処理の要件をサポートする。	・ビジネス要件をサポートするデータ管理 ・データの取り扱いのためのガイダンス ・承認されたデータトランザクション ・ソースの保護された保管	・ビジネス要件をサポートしないデータ管理 ・セキュリティ違反 ・ビジネス、法律、規制の要件への不適合

コントロール設計のテスト
・データ要素の棚卸を入手する ・それぞれのデータ要素について、機密性、インテグリティ、可用性の要件が定義され、このような要件がデータオーナによって検証されていることを確かめる。 ・要件に見合ったコントロールが定義され文書化されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS11.2 データの保管および保持の調整 ビジネス目標をはじめ、組織のセキュリティポリシー、および法的要件に適合するために、効果的で効率的なデータ保管、ログ保持、アーカイブを行うための手続を定義し導入する。	・ビジネス要件をサポートするデータ管理 ・データの取り扱いのためのガイダンス ・ソースの保護された保管 ・効率的な方法で取り出されるデータ	・承認されていない閲覧や改変から保護されていないデータ ・必要なときに取り出せない文書 ・規制と法律の義務への遵守違反 ・承認されていないデータアクセス

コントロール設計のテスト
・データモデルをレビューして、保管の技法がビジネス要件を満たしていることを確かめる。 ・データの保持期間をレビューして、それが契約、法律、規制の要件に沿っていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS11.3 メディアライブラリ管理システム 保存/アーカイブされたメディアの一覧を維持し、メディアの使用可能性とインテグリティを確保するための手続を定義し導入する。	・すべてのメディアの台帳記入 ・バックアップ管理の改善 ・データ可用性の保護 ・データ復元時間の短縮	・危険に晒されたメディアインテグリティ ・必要なときに利用できないバックアップメディア ・データテープへの承認されていないアクセス ・バックアップの破損 ・バックアップメディアの場所を特定する能力の欠如

コントロール設計のテスト
・メディアの棚卸をサンプルベースで入手して、棚卸一覧にあるメディアが特定され、保管されている項目が棚卸と突合できることを確かめる。 ・サンプルベースで、外部のラベルが内部のラベルと対応していることを確かめるか、あるいは、外部のラベルが正しいメディアに添付されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS11.4 廃棄 データやハードウェアを処分または譲渡する際の、機密データやソフトウェアを保護するというビジネス要件に適合する手続を定義し導入する。	・企業情報の適切な保護 ・バックアップ管理の向上 ・データ可用性の保護	・企業情報の漏洩 ・重要なデータの損なわれたインテグリティ ・データテープへの承認されていないアクセス

コントロール設計のテスト
・以下を調査して確認する。 – 廃棄についてのポリシーの策定と伝達の責任が明確に定義されている – 重要な情報を含んでいる設備とメディアが、再利用や廃棄に先立って、「削除」「廃棄予定」とマークされているデータを取り出せないようにするといったような方法で削除されている（高度に重要なデータを含むメディアは物理的に破壊されているなど） – 重要な情報を含む廃棄された設備とメディアのログをとって、監査証跡を維持している – 利用されてきたメディアを廃棄する際にメディア棚卸リストから削除するための手続が存在する。ログの中に最近の廃棄を反映するように、現在の棚卸が更新されていることをチェックする。 – 削除されていない設備とメディアが、廃棄プロセスを通じて安全な方法で輸送されている – 廃棄契約に、廃棄の前および最中に設備とメディアを保存して処理するために必要な物理的セキュリティとそのためのプロセスがある

コントロール目標	価値のドライバー	リスクのドライバー
DS11.5 バックアップと復元 ビジネス要件と継続計画に沿った、システム、アプリケーション、データ、および文書のバックアップと復元の手続を策定し導入する。	・適切に復元される企業情報 ・ビジネス要件とバックアップ計画と整合的なバックアップ管理の向上 ・データの可用性とインテグリティの保護	・企業情報の漏洩 ・バックアップデータを必要なときに復元する能力の欠如 ・ビジネスの要件に合致していない回復手順 ・災害のときにデータを復元する能力の欠如 ・バックアップを実施する際の時間に関する不適切な要件

コントロール設計のテスト

・以下を調査して確認する。
- ビジネスの業務に影響する重大なデータが、リスク管理モデルとIT サービス継続性計画に沿って定期的に特定される
- システム、アプリケーション、データ、文書のための十分なポリシーと手続が存在し、以下を含む要因を考慮している

バックアップの頻度（ディスク・ミラーリングを取ってリアルタイムでバックアップしているのか、あるいはDVD-ROMで長期保存のためにバックアップしているのかなど）
バックアップのタイプ（全部か増加分のみかなど）
メディアのタイプ
自動化されたオンラインバックアップ
データタイプ（音声データ、光学データなど）
ログの作成
エンドユーザの重大な計算データ（スプレッドシートなど）
データソースの物理的および論理的な位置
セキュリティとアクセス権
暗号化

- バックアップを取ることとモニタリングすることの責任が割り当てられている
- 確立したポリシーと手続にしたがってバックアップを取り、そのログを取るためのスケジュールが存在する
- サードパーティが維持したり処理したりしているシステム、アプリケーション、データ、文書のバックアップを十分に取るか、他の方法で安全を確保している。サードパーティからのバックアップの返還を要求し、第三者預託や前払い金の手配を検討すべきである。
- バックアップデータのオンサイトとオフサイトでの保管の要件が、バックアップデータのアクセスを含むビジネス要件に合致するように定義されている
- バックアップのすべての構成要素を効果的に復元できるよう、十分な復元テストが定期的に実施されている
- 復元に要する時間がビジネスオーナやIT プロセスオーナと合意済みであり、伝達されている。データ復元の優先順位は、ビジネス要件とIT サービス継続手続に基づいている。

コントロール目標	価値のドライバー	リスクのドライバー
DS11.6 データ管理におけるセキュリティ上の要件 ビジネス目標、組織のセキュリティポリシー、および法的要件に適合させるために、データの受信、処理、保管、および出力に適用するセキュリティ要件を特定して適用するためのポリシーと手続を定義し導入する。	・ 安全が適切に確保され保護されるような重要な情報 ・ 情報を閲覧したり改変する能力が、承認されたユーザに与えられた状態 ・ 送信されたデータの網羅性と正確性	・ 不正利用されたり破壊されたりする重要データ ・ 承認されていないデータアクセス ・ 送信されたデータの不完全さと不正確さ ・ 承認されていないユーザによるデータ改変

コントロール設計のテスト

・ 以下を調査して確認する。
  - 重要なデータを特定し、データの機密性に対するビジネスでの必要性に対処し、該当する法規制を遵守し、データ分類がビジネスプロセスオーナと合意済みであるようなプロセスがある
  - 承認されていないアクセスと誤った送信と転送から重要なデータとメッセージを保護するためのポリシーが定義され導入されている。これには、暗号化、メッセージ認証コード、ハッシュ合計、物理的な輸送のための保証つきの輸送業者と不正開封防止包装が含まれるが、これに限定されるわけではない
  - データ出力への物理的および論理的なアクセスのための要件が確立しており、出力の機密性が明確に定義され考慮されている
  - データへのエンドユーザのアクセスと重要なデータの管理とバックアップのためのルールと手続が確立している
  - エンドユーザのコンピュータにあるデータ、またはネットワークに接続されたアプリケーションやデータに悪影響を及ぼすようなエンドユーザアプリケーションのためのルールと手続が確立している（ネットワーク接続の PC へのユーザの権利についてのポリシーを検討するなど）
  - 重要なデータの扱いや処理におけるセキュリティへの注意を促し維持するための意識喚起プログラムが策定されている
  - 重要な情報を処理する施設が、適切な監視、セキュリティバリア、入館コントロールを組み合わせて定義されたセキュリティによって保護された安全な場所にある
  - 物理的インフラストラクチャの設計が、火災、障害、外部からの攻撃や承認されていないアクセスからの損失を防止している。重要なデータ出力やサードパーティへのデータの移送のための出力の安全な引渡し場所がある。

コントロール目標の達成をテストするために以下のステップを踏む。
・ ビジネス要件の文書をレビューして、文書化メカニズムが設計通りに用いられていることを確かめる。
・ データ管理ツールを調査して、それが説明通りに用いられていることを確かめる。
・ メディアとシステムへのアクセスが承認された人員に制限されていることを確かめる。
・ テープのような損傷しやすいメディアが日常的に置き換えられているかどうかを確かめる。
・ メディア廃棄リストのサンプルを選び、廃棄されたメディアがメディア棚卸リストにないことを確かめる。
・ オンサイトとオフサイトの保管施設を調査し、アクセス性をチェックする。
・ テスト結果のサンプルをレビューして、復元に成功し、復元に要した時間がSLAと継続性の要件と照合されていることを確かめる。
・ 継続プロセスで要求されている通りに、バックアップ情報が遠隔地で保管されていることを確かめる。
・ アーカイブされた情報のインテグリティを保証するためのプロセスがあり、それに従っていることを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
・ 重要なデータが承認されていない人員に晒されるリスクを最小化するために、設備とデータの廃棄と再

利用についてのビジネス用件に合致するポリシーがあるかどうかを調査して、それを確認する。
- 業務に影響する重大なデータが、リスク管理モデルとITサービス継続計画に沿って定期的に特定されているかどうかを調査して、それを確認する。
- データの機密性、インテグリティ、可用性および該当する法律と規制を考慮していることを確かめる。

DS12 物理的環境の管理

コンピュータ機器と要員を保護するには、適切に設計および管理されている物理的施設が必要である。物理的環境を管理するプロセスには、物理的なサイト要件の定義、適切な施設の選定、および環境要因をモニタリングし物理的アクセスを管理するための効果的なプロセスの設計が含まれる。物理的環境を効果的に管理することで、コンピュータ機器と要員にかかわる障害に起因するビジネスの中断が減少する。

コントロール目標

DS12.1 サイトの選定と配置

ビジネス戦略に関連付けられた技術戦略を支援するIT機器のための物理的サイトを定義および選定する。サイトの選定と配置設計では、関連法令（労働安全衛生に関する規制など）を考慮する一方で、自然災害や人的災害に関連するリスクを考慮する必要がある。

価値のドライバー

- 物理的セキュリティへの脅威の最小化
- 攻撃を行うかもしれない、承認されていない人物にITサイトを特定される可能性を減らすことによる、サイトへの物理的な攻撃リスクの減少
- 最適な物理的セキュリティの管理の結果としての、保険の費用の減少

リスクのドライバー

- 物理的セキュリティへの脅威が特定されない状態
- サイトの立地ないしレイアウトによる、セキュリティリスクに対する脆弱性の増加

コントロール設計のテスト

- 以下を調査して確認する。
  - 地理的条件、近隣環境、インフラストラクチャ、リスク（盗難、温度、火、煙、水、振動、テロリズム、破壊行為、化学物質、爆発物）といった問題点を考慮しながら、ビジネス要件とセキュリティポリシーに合致する技術戦略にしたがって、IT設備のための物理的なサイトが選択されている
  - 組織のITサイトに対する潜在的なリスクと脅威を特定し、天災と人災に関連するリスクを考慮しながらビジネスへの影響を継続的に評価するプロセスが定義され導入されている
  - サイトの選定と設定で、建築基準法、環境、火災、電気工学、労働衛生、安全規則といった、関連する法律と規制を考慮している

コントロール目標	価値のドライバー	リスクのドライバー
DS12.2 物理的なセキュリティ対策 場所や物理的資産を保護するためのビジネス要件に合致した物理的なセキュリティ対策を定義し導入する。物理的なセキュリティ対策では、盗難、温度、火災、煙、水、振動、テロ、破壊行為、停電、薬物、爆発物などに関連するリスクを効果的に防止、検出、および緩和できなければならない。	・重大なITシステムの、物理的な脅威からの保全 ・物理的セキュリティ対策の効果的な展開 ・スタッフとマネジメント層への、物理的セキュリティに関する組織の要件に対する注意喚起	・物理的セキュリティへの脅威が特定されない状態 ・承認されていない人物によるハードウェアの盗難 ・ITサイトに対する物理的な攻撃 ・承認なしに再設定された機器 ・コンピュータが発信する電波を読むように設定された機器によってアクセスされる機密情報

コントロール設計のテスト

・以下を調査して確認する。
- ITサイトが従うべき、物理的セキュリティとアクセスコントロールの手段のためのポリシーが定義され導入されている。ポリシーが妥当であり最新の状態を保っていることを確かめるために、ポリシーを定期的にレビューしている。
- 重要なITサイトとその設計計画についての情報へのアクセスが限定されている
- 重要なITサイトが外から容易に識別できないようになっている
- 組織のディレクトリ/サイトマップでITサイトの位置を特定できないようになっている。
- 物理的セキュリティ対策の設計で、ビジネスとオペレーションに関連するリスクを考慮している。必要に応じて、警報システム、建物の強化、有刺鉄線による保全、安全な区画割りなどを、物理的セキュリティ対策に含める。
- 設計、実装、有効性を確かめるべく、防止的、発見的、修正的な物理的セキュリティ対策のテストが定期的に実施されている
- サイトの設計で、物理的な通信回線と上下水道と電力の配管が考慮されている
- IT機器の安全な除去のために、適切な権限に基づいたサポートされているプロセスが定義され導入されている。
- IT機器の物品の受け渡しエリアが、通常のITサイトの運用と同様の方法と対象範囲で保護されている。
- 機器を安全に輸送し貯蔵するためのポリシーとプロセスが定義されている
- 重要な情報を含んでいる貯蔵機器が物理的に破壊されるか洗浄されるようにするためのプロセスが存在する
- ITインシデント管理プロセス全体に沿って物理的セキュリティ・インシデントを記録し、モニタリングし、管理し、報告し、解決するためのプロセスが存在する
- 特に重要なサイトが、セキュリティ担当者によって頻繁にチェックされる（週末と祝日を含む）

コントロール目標	価値のドライバー	リスクのドライバー
DS12.3 物理的アクセス ビジネス上の必要性に基づき、緊急事態発生時を含めた施設、建物、敷地への立ち入りの許可、制限、取り消し手続を定義および導入する。施設、建物、敷地への立ち入りに際しては、正当性の評価、認可、記録、およびモニタリングを行う必要がある。これは、施設に立ち入るすべての人員（スタッフ、臨時スタッフ、取引先、ベンダ、訪問客、およびその他のサードパーティ全員）に適用される。	・ 重大インシデントをタイムリーに解決するための適切なアクセス ・ すべての訪問者を特定でき追跡できる状態 ・ 訪問者に関する職責を意識しているスタッフ	・ IT機器や情報に対して承認されていないアクセスを得る訪問者 ・ 保護区域への承認のない立ち入り

コントロール設計のテスト

・ 以下を調査して確認する。
  - コンピュータ施設へのアクセス権の要求と授与に関するプロセスがある
  - 正式なアクセス要求が完了し、ITサイトの管理者によって承認され、記録が保持され、個人がアクセスを認められた区域をフォームで具体的に特定している。これは、承認を観察したりレビューしたりすることで確かめることができる。
  - アクセスプロファイルが最新の状態を保つようにするための手続がある。ITサイト（サーバルーム、建物、区域や区画）へのアクセスが職務機能と責任に基づいていることを確かめる。
  - 請負業者やベンダを含むサイトへの訪問者のすべてを登録し、ITサイトへのすべての立ち入りの記録を取りモニタリングするためのプロセスがある
  - すべての人員に対して、常時IDカードを見えるようにして、適切な承認のないIDカードやバッジの発行を防止するように指示するポリシーが存在する。実際にバッジを着用しているかどうかを観察する。
  - 訪問者に対して、サイト内のIT運用グループのメンバーが常時同伴することを要求するポリシーが存在し、適切なIDを着用していない個人をセキュリティ担当者が見つけられる。
  - フェンスや壁と内部と外部の扉にあるセキュリティ機器といったような、境界での制限によって、重要なITサイトへのアクセスが制限されている。機器が立ち入りを記録し、承認されていないアクセスが発生したら警報音を発生させることを確かめる。このような機器の例としては、バッジやキーカード、キーパッド、有線テレビ（CCTV）、生体認証スキャナが含まれる。
  - セキュリティに対する定期的な意識喚起のための研修が実施される。研修ログをレビューすることで確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
DS12.4 環境的要因からの保護 環境的要因から保護するための対策を確立および導入する。環境をモニタリングおよびコントロールするための特別な設備やデバイスを導入する。	・IT施設に対する潜在的な環境上の脅威すべての特定 ・環境上の脅威からの保護やタイムリーな発見 ・保険ポリシーの要件を遵守しないために保険会社への保険金の請求を却下されるリスクの減少と、保険料の最小化 ・環境的要因に対する適切な保護	・環境的な影響の危険に晒されている施設 ・環境的脅威の不十分な検知 ・環境的脅威からの保護の不十分な手段

コントロール設計のテスト

・以下を調査して確認する。
- 重要なIT施設が立地している区域で発生する自然災害と人災を特定するためのコンティンジェンシープランがある。報告書をレビューして、潜在的な影響が、事業継続性計画のプロセスに従って評価されていることを確かめる。
- 移動機器や遠隔地の機器を含むIT機器が、盗難や環境的脅威からどのように保護されているかを概説するポリシーがある。文書をレビューして、たとえば、重要な区域内での飲食と喫煙を禁止しており、文房具や他の備品がコンピュータルーム内の火災の原因となることを禁止していることを確かめる。
- 環境的要因による危険を最小化し緩和するような方法で、IT施設が立地し建設されている
- 環境的な脅威を発見するのにふさわしい装置がある。このような装置に対して行われている継続的なモニタリングを調査する。
- 環境的な危険が生じたときには警報やその他の通知が生じて、そのような自体に対応する手続が文書化されテストされ、人員が適切な研修を受けている
- 対策と継続性を保険契約と照らし合わせるためのプロセスがある。報告書と保険契約をレビューして、遵守を確かめる。
- 遵守していない部分が少しでもあればそれにタイムリーに対処できるよう、マネジメント層が行動を取っている
- 盗難、空気、火、煙、水、振動、テロリズム、破壊行為といった環境的リスクの影響を最小化するようにITサイトが建造されている。ITサイトの立地を物理的に調査して、その設計が適切に実装されていることを確かめる。サイトの設計と建造に先立って行われたリスク評価の報告書をレビューする。
- ITオペレーションの近くで継続的な清掃と片付けが行われるようにするためのポリシーがある。ITサイトとサーバルームをチェックして、常に清潔で整理整頓されており安全になっていることを確かめる（散らかっている手紙類、紙類や段ボール箱、満杯のゴミ箱、可燃性の化学物質や可燃物がないなど）。サイトが常に清潔に保たれているかどうかを調査する。

コントロール目標	価値のドライバー	リスクのドライバー
DS12.5 物理的施設の管理 法律、規制、技術要件、ビジネス要件、ベンダの仕様、および安全衛生ガイドラインに従って、電源装置や通信機器などの設備を管理する。	・ 重要なITシステムの、停電や施設に関連する他のリスクの影響からの保護 ・ 施設の資源の効果的かつ効率的な利用	・ 健康と安全に関する規制の遵守違反 ・ 停電と施設に関連する他のリスクから適切に保護していないことによる、ITシステムの機能不全 ・ スタッフメンバーへの事故

コントロール設計のテスト

・ 以下を調査して確認する。
- 環境条件、電源変動、および停電からITシステムを保護する必要性を、他の事業継続計画の手続と同時に検証するプロセスが存在する
- 無停電電源装置（UPS）を調達し、それが可用性と事業継続性の要件に合致している
- UPSの運用を定期的にテストし、ビジネスのオペレーションに重要な影響を与えることなく電源が予備電源へと切り替わるようにするためのプロセスがある
- テストを実施し、必要に応じて是正措置を取っている
- 重要なITシステムを収容している施設では、複数の電源が利用できる
- 電源の物理的な入り口が分離されている
- ITサイトの外への配線が地下に埋設されていたり、ふさわしい代替的な保護策を取っていたりする
- 設計図と計画が存在する
- ITサイト内の配線が安全な配管に収容されている
- 配線が、環境的リスクから保護され、強化されている
- 配線盤が施錠されアクセスが制限されている
- 配線と物理的な補修（データと電話）が、うまく構成されよく整理されている
- 配線と配管についての文書を参照できるようになっている
- 可用性の高いシステムを収容している施設では、冗長性と障害迂回の配線の要件（外部と内部）のための分析がなされている
- 健康と安全に関連する法律、規制、ガイドラインまたはベンダ仕様をITサイトと施設継続的に遵守するようにするためのプロセスがある
- 人員に対して健康と安全に関する法律、規制、またはガイドラインを教育するためのプロセスがある。これには、火災や同様のインシデントについての知識とその場合にとる行動を確かなものにするための、火災の通報と避難訓練も含まれる。
- 研修プログラムで、ガイドラインの知識を評価し、その研修プログラムが文書化されている
- 施設でのインシデントをITインシデント管理プロセスに沿って記録し、モニタリングし、管理し、解決するためのプロセスがある
- 法律と規制の観点から開示が要求されるときに、インシデントの報告を提供できる
- ITサイトと施設が、供給者の推奨するサービスインターバルと仕様にしたがって維持されるようにするためのプロセスがある
- 維持管理が承認された人員によってのみ実行される。文書をレビューして、確認のために職員に質問する。
- 環境的なリスク（火災、水害など）を再評価するためにITサイトや建物に対する物理的な代替策が分析されている
- この分析の結果が、事業継続性と施設の管理部門に報告されている

コントロール設計のテスト（続き）

- 施設に対してウォークスルーを行い、その知見を健康と安全のガイドラインと比較する。
- 標準の違反の可能性について職員に尋ねる。
- 最近変更が加えられたサイトのウォークスルーを行い、変更後もリスクに関する標準に合致していることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。

- リスク分析報告をレビューして、その報告書が過去1年以内に更新されていることを確かめる。
- ポリシーをレビューして、新規の/更新された規制と法律がポリシーに反映されていることを確かめる。
- 区域に対してウォークスルーを行い、手続に従って安全が確保されていることを確かめる。
- セキュリティログをレビューして、最小限のセキュリティチェックを確認する。
- ログを閲覧して、そこに最低限、訪問者の氏名と所属企業、訪問目的、訪問を承認したIT運用グループ名とそのメンバー、訪問の日付、入館と退館の時刻が含まれていることを確かめる。
- バッジを着用している要員を抽出し、承認を確認する。
- 配線盤が施錠されアクセスが制限されているかどうかを確かめる。
- 配線と配管についての文書を参照できるようになっていることを確かめる。
- 施設に対してウォークスルーを行い、その知見を健康と安全のガイドラインと比較する。
- 職員にインタビューして、ガイドラインに対する知識を評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。

- 特別な事項を検討したことを確かめる（立地条件、周辺環境、インフラストラクチャなど）。他に検討すべきリスクとしては、盗難、温度、火、煙、水、振動、テロリズム、破壊行為、化学物質と爆発物がある。
- 環境条件、電源変動、および停電からITシステムを保護する必要性を、他の事業継続計画の手続と同時に検証するプロセスが存在するかどうかを調査して、それを確認する。

DS13 オペレーション管理

データを完全かつ正確に処理するには、データ処理手続の効果的な管理と、ハードウェアの綿密な保守が必要になる。このプロセスでは、計画された処理の効果的管理、機密性を有する出力の保護、インフラストラクチャ性能のモニタリング、およびハードウェアの予防的保守に適用する運用上のポリシーと手続を定義する。効果的なオペレーション管理により、データのインテグリティが維持され、業務の遅延やIT運用費用が削減される。

コントロール目標	価値のドライバー	リスクのドライバー
DS13.1 オペレーション手続と指示 ITオペレーションの手続を定義、導入、保守し、オペレーション担当スタッフメンバーが関連するすべてのオペレーション任務を熟知しているようにする。合意されたサービスレベルをサポートし、継続的なオペレーションを保証するために、オペレーション手続はシフト交代時の引継ぎ項目(アクティビティ、状況に関する最新情報、オペレーションの問題、エスカレーション手続、および現行の責任に関する報告)が含まれている必要がある。	・ ITオペレーションがSLAに合致していることの実証 ・ スタッフの経験を文書化し、それをナレッジベースで保持することによる、オペレーショナルサポートの継続性の促進 ・ 構造化され、標準化され、明確に文書化されたITオペレーション手続とサポートスタッフへの指示 ・ 技能のあるオペレーションサポートスタッフと新規採用者との間の知識の移転に要する時間の短縮	・ 手続を間違って理解していたために生じるエラーや手戻り ・ 不明確ないし標準化されていない手続による非効率性 ・ オペレーションの問題、新規のスタッフ、およびオペレーションでの変更に迅速に対応する能力の欠如

コントロール設計のテスト

・ITオペレーション標準手続のコピーを閲覧する。
・ オペレーション手順書を、網羅性に関してレビューする。その内容には、ITスタッフメンバーの役割と責任、組織図、直属の上司の役割と報告、オペレーティングシステムの異常終了の手続、緊急事態での連絡先リストなどが含まれるだろう。
・ 組織図を閲覧して、職務をレビューする。

コントロール目標	価値のドライバー	リスクのドライバー
DS13.2 業務のスケジュール策定 ビジネス要件を満たすために処理能力と稼働率を最大にしながら、ジョブ、プロセス、タスクのスケジュールを最も効率的な順序で構成する。	・ 負荷を平準化しオンラインユーザへの影響を最小化することによるシステムリソースの最適化された利用 ・ 本番環境の中断を避けるための、ジョブスケジュールへの変更の影響の最小化	・ 資源の活用におけるピーク ・ 臨時ジョブのスケジューリングによる問題 ・ ジョブの再実行やリスタート

コントロール設計のテスト

・以下を調査して確認する。
  - バッチジョブ実行手続が完全である
  - 日々の予想されているジョブスケジュール、ジョブに問題がある場合の連絡先、およびジョブ失敗コードの連続動作リストが手続に含まれている
  - コンピュータオペレータのそれぞれに、バッチジョブの職務と実行責任が存在する
  - コンピュータオペレータのシフトスケジュールが存在する
  - スケジュールに、開始と終了のシフトとオペレータ名が含まれている
  - バッチジョブの実行中に少なくとも一人のオペレータがいる

コントロール目標

DS13.3 ITインフラストラクチャのモニタリング

ITインフラストラクチャと関連イベントをモニタリングするための手続を定義し、導入する。運用と運用を取り巻き支援する他のアクティビティを時系列に再構成、レビュー、および調査可能にするために、十分な時系列情報が運用ログに保管されることを保証する。

価値のドライバー

・インシデントにつながる可能性のある、インフラストラクチャにおける問題の能動的な発見
・インフラストラクチャでの潜在的な問題が生じる前に、傾向をモニタリングし、対策を取る能力
・資源の配置と利用を最適化する能力

リスクのドライバー

・インフラストラクチャにおける発見されない問題と、インシデントの発生
・防止されたり早期に発見されたときよりも大きな影響をオペレーションとビジネスに及ぼすような、インフラストラクチャでの問題
・有効に活用され配置されていないインフラストラクチャ資源

コントロール設計のテスト

・以下を調査して確認する。
  - イベントログを取るための計画的なプロセスによって、リスクとパフォーマンスに基づいて記録する情報のレベルを特定している
  - サービスの重大性および、構成項目とそれに依存するサービスとの関係に基づいて、モニタリングする必要のあるインフラストラクチャ資産が特定されている
  - ログを取るためのプロセスに関する計画を文書化したものが存在する。文書を物理的に閲覧する。
  - 資産台帳が資産を適切に特定している。どの資産が最も重要かについて職員に尋ね、そのような資産を台帳に追跡する。

コントロール目標	価値のドライバー	リスクのドライバー
DS13.4 機密文書と出力デバイス 特殊書類、有価証券、特殊目的のプリンタやセキュリティトークンなどの機密性を有するIT資産について、適切な物理的保護策、責任割り当て、および在庫管理手続を確立する。	・特殊書類と商業的に重要な出力データに対する、棚卸管理を通じた追加的な保護 ・重要なIT資産に対する盗難や不正、改竄、破壊、その他の不正利用の防止 ・特殊書類と出力機器に対して物理的なアクセス権を与える際のアクセス権限の検証と、特別な出力機器のインテグリティに関する証拠の保全	・重要なIT資産の不正利用と、それによる財務上の損害およびその他のビジネスへの影響 ・すべての重要なIT資産を識別する能力の欠如

コントロール設計のテスト
・以下を調査して確認する。 – 組織の内外で出入りする特殊書類と、出力機器の受領や除去、廃棄に関する手続が存在する – 重要な資産へのアクセスに対して少なくとも半年おきのレビューが存在する – 重要な資産へのアクセスを獲得、変更、除去するための手続が存在する – 除去と廃棄の手続に関する文書が存在する

コントロール目標	価値のドライバー	リスクのドライバー
DS13.5 ハードウェアの予防的保守 インフラストラクチャのタイムリーな保守を保証するための手続を定義し導入する。これにより、障害やパフォーマンス低下の発生頻度と影響を低減できる。	・システムのパフォーマンスと可用性の最適化 ・予防的なインシデント管理と問題管理 ・保証契約の保全	・事前に回避または予防できたはずのインフラストラクチャ上の問題 ・保守要件を遵守しないことによる、保証契約への違反

コントロール設計のテスト
・以下を調査して確認する。 – 重要なハードウェアに対する予防的保守計画があり、費用便益分析、ベンダの推奨内容、サービス中断のリスク、適任者および他の関連する要素を考慮した計画が設計されている – 予防的保守の必要性を特定するために活動ログをレビューしており、保守活動での予想される影響（パフォーマンスの制限、SLA）が、影響を受ける顧客とユーザに伝達されている

コントロール目標の達成をテストするために以下のステップを踏む。
・合意済みのサービスレベルをサポートするITオペレーションの標準手続があるかどうかを調査して、それを確認する。
・サービス中断時間を追跡してモニタリングするためのトラブルエスカレーションシステムが手続に含まれているべきである。
・外部のサービスプロバイダを含む役割と責任が定義されているかどうかを調査して、それを確認する。関連する文書をレビューして、その存在を確かめる。

- 自らが責任を負うオペレーション手続と関連する作業をサポートスタッフメンバーが認識し、かつ理解しているかどうかを調査して、それを確認する。サポートスタッフの作業区域に対してウォークスルーを行い、オペレーション手続が正しく実施されていることを確かめる。
- ログをレビューすることによって、その手続が一貫して維持され実施されているかどうかを調査して、それを確認する。
- 引継時の伝達と関連する責任が定義されているかどうかを調査して、それを確認する。
- 例外処理のための手続が存在し、それがインシデント管理と統合されているかどうかを調査して、それを確認する。
- 職務と役割の記述書での職務の分離を確かめる。たとえば、コンピュータオペレータがプログラムにアクセスできてはならず、コンピュータプログラマは本番データにアクセスできたりメディアに直接書き込んだりできてはならない（BLP、ラベルバイパス処理）。
- 手続の文書の存在を確認するスタッフメンバーを観察しながらインタビューを行い、手続の遵守を確かめる。
- アクセス特権を調査して、職務の分離が適切であることを確かめる。
- 文書を閲覧した上で、オペレーション担当者にインタビューを行い、手続に従っていることを確かめる。
- 手続の利用を確認するため、オペレーション担当者を観察し、パフォーマンスを文書化する。
- バッチジョブのスケジュールが、ジョブスケジュールソフトウェアによってコントロールされているかどうかを調査して、それを確認する。承認されていないジョブが実行されることを防止するための適切なセキュリティコントロールがあることを確かめる。
- バッチジョブがスケジュールされているかどうかを調査して、それを確認する。
- スケジュールプロセスを評価し、バッチジョブのスケジュールが以下を考慮していることを確かめる。
  - ビジネス要件
  - ジョブの優先順位
  - ジョブ相互間の衝突
  - 負荷のバランス（パフォーマンスとキャパシティの管理の間）
- バッチジョブの結果がモニタリングされ検証されているかどうかを調査して、それを確認する。
- バッチジョブに失敗したときに直ちに知らせるための自動化プロセスがあるかどうかを調査して、それを確認する。自動化された処理に関連するハードウェアとソフトウェアを調査して、存在を確かめる。
- バッチジョブのコントロールが技術的な情報（ジョブを完了するのに要する時間など）に限定されず、データに関するビジネスプロセスの要件がコントロールされている（処理されたデータの網羅性と正確性）ことを確かめる。
- 関連する文書を閲覧して存在を確かめ、正式な手続がバッチジョブのスケジュールに適切に対処していることを確かめる。
- 変更の文書を閲覧して、正確性を確かめる。
- スケジュールの存在を確認する。
- バッチジョブのインシデントが生じてタイムリーに解決したという文書と証拠を閲覧する。
- 必要なときに実際のイベントが引き起こされたことを確かめるべく、閾値とイベントの条件を網羅するルールが定義され、システムに導入されているかどうかを調査して、それを確かめる。
- 将来の調査とアクセスコントロールのモニタリングを支援するために、イベントログが作成され、適切な期間にわたって保存されているかどうかを調査して、それを確認する。
- イベントログをモニタリングするためのプロセスが確立しており、モニタリング活動の結果が定期的にレビューされ、必要に応じて、インシデントがサービスデスクにエスカレートされているかどうかを調査して、それを確認する。
- 発見されたすべての逸脱に対してインシデントが作成されているかどうかを調査して、それを確認する。
- イベントログを閲覧して、それが軽微なイベントで溢れておらず、主要なイベントが記録されていることを確かめる。
- イベントログを閲覧して、存在と適正性を確認する。
- サービスデスクチケットにつながったイベントログ入力の問い合わせのサンプルを入手する。イベントログ入力をサービスチケットログへと追跡する。
- 重要な文書と出力機器へのアクセス権が適切に割り当てられているかどうかを調査して、それを確認す

る。
- 重要な文書と機器に対して、定期的な照合作業を実施しているかどうかを調査して、それを確認する。実際の記録された数量と、重要な文書および機器のサンプルを照合する。
- 適切な物理的保護が確立しているかどうかを調査して、それを確認する。
- 重要な資産に対する物理的な保護を調査してテストする。
- 適切な重要機器が利用可能かどうかを調査する。
- 予防的保守を要するような重要なハードウェアの構成要素を特定するために、活動ログが定期的にレビューされているかどうかを調査して、それを確認する。
- 意思伝達手段が、サービス中断の影響をユーザに直ちに通知するのに効果的であるかどうかを調査して、それを確認する。
- ビジネス要件にしたがってスケジューリングが行われていることをビジネス部門とIT部門に確認する。本番のスケジュールをレビューし、すべての関連する機器が考慮され、スケジューリングでサービス要件を考慮していることを確かめる。
- ハードウェアを物理的に調査して、保守が行われていることを確かめる。計画を閲覧して、それが、費用便益分析、ベンダの推奨事項、サービス中断のリスク、適任者、その他の関連する要因を考慮して効果的に設計されていることを確かめる。
- 重要な保守に対して、適切な行動をタイムリーに取っているかどうかを判断する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 文書化された手続の欠如が継続的なオペレーションに影響を及ぼしているかどうかを調査する。すなわち、コンピュータオペレータが、オペレーションマニュアルなしに日々の業務を行うことができ、伝達経路が知られているかどうかを調査する。
- 文書化されていないITオペレーション手続が現在のオペレーションを反映しているかどうかを調査する。もしそうでなければ、クロストレーニングや新規雇用者の研修の妨げになり、シフトの交代の最中に不適切な手続に繋がりかねない。
- すべてのバッチジョブが報告その他の手段を経由して完了しているかどうかを調査して、それを確認する。
- コンピュータオペレータがバッチジョブをモニタリングし、スケジュール通りに完了していることを観察する。
- 最後のサービスの中断があったのはいつだったかについてITスタッフメンバーに尋ね、そのイベントログをレビューする。理由および解決策を含む記録が適切に文書化されていることを確かめる。
- 数週間にわたるイベントログを閲覧し、その存在を確認した上で、イベントログの解決についてITスタッフメンバーに尋ねる。
- 重要な資産へのアクセスを調査して、組織図へのアクセスを追跡することによって資産へのアクセスを評価する。
- 資産への物理的な保護を観察して、そのような保護が適切かどうかを判断する。
- ハードウェアを物理的に調査して、保守が行われていることを確かめる。計画を閲覧して、それが、費用便益分析、ベンダの推奨事項、サービス中断のリスク、適任者、その他の関連する要因を考慮して効果的に設計されていることを確かめる。

（空白ページ）

付録Ⅴ—モニタリングと評価（ME）

ME1　IT成果のモニタリングと評価
ME2　内部統制のモニタリングと評価
ME3　外部要件に対するコンプライアンスの保証
ME4　ITガバナンスの提供

付録Ⅴ—モニタリングと評価（ME）

プロセス保証のステップ

ME1 IT成果のモニタリングと評価

IT成果を効果的に管理するには、モニタリングプロセスが必要である。このプロセスには、妥当な成果達成指標の定義、体系的かつタイムリーな成果報告、および成果目標から逸脱した場合の迅速な対応が含まれる。指針やポリシーに沿って正しい運用が行われていることを確認するため、モニタリングが必要である。

コントロール目標	価値のドライバー	リスクのドライバー
ME1.1 モニタリングアプローチ ITソリューションやサービス提供の状況を測定するために準拠すべき対象範囲、方法論、およびプロセスを定義し、ビジネスに対するITの貢献度を監視するための総合的なモニタリングフレームワークとアプローチを確立する。モニタリングフレームワークは、企業の成果管理システムに組み込む。	・信頼できる情報に基づく、ITのパフォーマンスへの透明な見方 ・改善のための特定された機会 ・ビジネスとガバナンス要件の達成の促進 ・費用対効果の高いITサービス ・IT投資の意思決定のための情報が増え、価値の提供が改善されること ・成果達成指標の一貫した利用とインテグリティ	・古かったり、不正確であったり、信頼できなかったりするデータに基づいた成果報告 ・ビジネスとガバナンスの要件と整合しない成果測定指標 ・タイムリーに特定されていないITとビジネスの整合性に関する問題 ・顧客の期待とビジネスでの必要性が、十分に特定されていない ・モニタリングされたデータが、全体的なプロセスパフォーマンスの分析に役立たない

コントロール設計のテスト

- 重要なビジネスプロセス、戦略的業務、および主要なITプロセスに対する経営者の定義を入手してレビューして、それらが企業の成果管理システムをサポートしていることを確かめる。
- 重要なビジネスプロセス、戦略的業務、および主要なITプロセスを経営者が伝達する方法を理解する。
- ITの成果要因に対する測定指標ベースのモニタリングアプローチがあることを確かめる（企業のポリシーと他の関連する文書を閲覧するなど）。
- モニタリングアプローチが、ビジネス上の重要な問題を視野に入れることを考慮しながら、適切な達成目標と成果指標を提供しているかどうかを判定する。
- ITパフォーマンスをモニタリングするために適切なシステムを用いているかどうかを特定する。
- マネジメント層のメンバーにインタビューして、ITプロセス活動をモニタリングするときにITプロセス相互間の関係と依存関係に気づいているかどうかを特定する（期待ギャップ、定義されていないインターフェース、隙間に落ちた問題、努力の重複、非効率性など）。
- 主要なITプロセスをビジネスの達成目標と目的と整合させる上での関連性に対するレビューについての経営者のアプローチを理解する。

コントロール目標	価値のドライバー	リスクのドライバー
ME1.2 モニタリングデータの定義と収集 ビジネス部門と連携して、バランスの取れた成果目標を定義し、ビジネス部門やその他の利害関係者から承認を得る。目標の比較基準となるベンチマークを定義し、目標の測定のために収集するデータを特定する。達成目標に対する進捗を報告するため、タイムリーかつ正確なデータの収集が可能なプロセスを確立する。	・最も重要かつ有意義な測定指標の特定および測定 ・全てのITプロセスに関して、IT組織における強い顧客志向 ・顧客満足と顧客への焦点の改善 ・プロセスをモニタリングするのに要するデータをシステムによって効率的に提供できる能力 ・パフォーマンスの傾向と変化をモニタリングするための、組織のパフォーマンスの履歴	・ビジネスの目標と整合しない目標に基づく測定指標 ・間違ったデータや不完全なデータに基づいた測定指標 ・組織のITプロセスのパフォーマンス指標に対して効果的でない報告 ・特定されていない顧客の期待とビジネスでの必要性 ・全体的なプロセスパフォーマンスの分析をサポートしていないモニタリング・データ

コントロール設計のテスト

以下を質問して確認する。

・モニタリングフレームワークで定義された測定指標のカバー範囲と特徴に沿ってITの測定指標のターゲットを定義しているか。そのターゲットについて、IT部門とビジネス部門のマネジメント層の承認を得ているか。
・モニタリングアプローチに必要なパフォーマンスデータが十分に集められ、どこが脆弱であるか自動で検出しているか。測定されたパフォーマンスが、(事前に合意された期間で)定期的に目標と比較されていることを確かめる。
・パフォーマンスのモニタリングのためのソースデータの一貫性、網羅性、およびインテグリティを確保するための手続があるか。
・パフォーマンスのモニタリングのためのデータソースへの全ての変更をコントロールするためのプロセスがあるか。
・成果目標が定義され、労力当たりの知見が最も多いものに焦点を当てているか。
・事前に合意された間隔で照合とコントロールチェックを行うことによって、収集されているデータのインテグリティを評価しているか。

コントロール目標	価値のドライバー	リスクのドライバー
ME1.3 モニタリング方法 目標を記録し、測定結果を把握し、IT成果の全体像を簡潔に示す、企業のモニタリングシステムに適合する成果モニタリング方法(バランススコアカードなど)を展開する。	・モニタリングの方法およびアプローチと、マネジメント層の期待の合致 ・ITのための意思決定のサポートの強化 ・企業全体の意思決定プロセスとの整合 ・透明で信頼できるパフォーマンス情報	・組織のITプロセスのパフォーマンスの指標についての、効果的でない報告 ・ビジネスでの期待と必要性の不一致 ・信頼できないパフォーマンス情報に基づいた間違った意思決定

コントロール設計のテスト

- ITプロセスパフォーマンス報告がITモニタリングシステムへと統合されていることを確かめる。
- ITプロセスパフォーマンス報告でのデータが理解しやすく簡潔であり、マネジメント層とエンドユーザの、効果的でタイムリーな意思決定に対する要求に合致していることを確かめる。
- パフォーマンス報告を閲覧して、それがITの目標とその結果および成果の測定をカバーしており、原因と影響との関係を明らかにしていることを確かめる。

コントロール目標

ME1.4 成果評価
達成目標に対する成果を定期的にレビューし、逸脱の原因を分析することで、根本的な原因を解決する是正措置を講じる。適切な時期に、逸脱の根本的原因の分析を実施する。

価値のドライバー

- サービス品質と将来の変更の準備についての費用対効果の向上
- プロセスの継続的な改善
- 組織内でのパフォーマンスの説明責任とオーナシップのレベルの向上

リスクのドライバー

- 残留し、繰り返されるプロセスのパフォーマンスの弱点
- 改善のための機会の損失
- スタッフのモティベーションの低下につながる、良好なパフォーマンスに対する認識の欠如

コントロール設計のテスト

- プロセスオーナにインタビューして、主要なプロセスのターゲットとなるパフォーマンスレベルが確立され、業界や競合他社と比較していることを確かめる。
- パフォーマンス報告を閲覧して、測定の適時性とターゲットとの比較が有効であるか検証する。
- 非公式のフィードバックを得ることができ、それがサービス提供や報告の改善のために用いられていることを確かめる。
- パフォーマンス報告を分析して、結果がターゲットに対して事前に合意された間隔で一貫して評価されており、関連する利害関係者が報告データを受け取っていることを確かめる。
- パフォーマンス評価の証拠を閲覧して、評価と分析が完全かつ効果的かどうかを判定する。
- 適切なサンプルについて、原因が特定され、是正措置へと移行され、それが適切な権限と資源を持つ者に割り当てられ、フォローアップされていることを確かめる。
- 全ての逸脱について、根本原因が定期的に特定され、適切に対処されているかどうかを調査して、それを確認する。

コントロール目標	価値のドライバー	リスクのドライバー
ME1.5 取締役会と経営層への報告 企業ポートフォリオの成果、IT関連投資プログラム、各プログラムのソリューションとサービス提供の成果などの観点を中心に、ビジネスに対するITの貢献度について上級マネジメント層向けの報告書を作成する。状況報告には、計画された目標の達成度合い、投じられた予算資源、達成された成果目標、および低減されたリスクを記載する。規模の大きい逸脱に対する是正措置を提案して、上級マネジメント層によるレビューを求める。上級マネジメント層に報告書を提出し、レビュー結果のフィードバックを求める。	・取締役会のガバナンス要件に合致する品質報告 ・戦略的オペレーションや、管理的オペレーション、日常的オペレーションに効果的かつ効率的に用いることのできるパフォーマンス情報 ・ビジネスでの必要性と関心に対応し、プロセスを改善する機会に焦点を当てた、強化された意思決定プロセス ・マネジメント層と取締役会のパフォーマンス報告への満足の向上	・ビジネスでの必要性と関心と結びつかない意思決定 ・上級マネジメント層のITパフォーマンスに対する不満 ・マネジメント層とIT部門間の不十分な意思疎通 ・取締役会と役員の能力が、主要なIT活動を指示してコントロールするには不十分

コントロール設計のテスト
・取締役会と役員への報告プロセスが確立しているかどうかを調査して、それを確認する。 ・ITの達成目標の達成、ITリスクの低減、および資源の利用を測定することによって、報告が、ITのビジネスへの貢献をカバーしており、パフォーマンスモニタリングフレームワークに基づいていることを確かめる（バランススコアカード、傾向分析、エグゼクティブダッシュボードなど）。 ・取締役会と役員への報告が、ITパフォーマンスの測定の集約された情報に基づいていることを確かめる。 ・報告のバージョンと反復を管理するプロセスがあることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME1.6 是正措置 成果のモニタリング、評価、および報告に基づいて必要な是正措置を特定し、実行する。これには、全てのモニタリング、報告、および評価について、以下によるフォローアップが含まれる。 ・マネジメント層の対応についてのレビュー、協議、および確定 ・是正措置に関する実行責任の割り当て ・実施された是正措置の結果の追跡	・是正措置に対するマネジメント層の積極的な関与 ・効果的かつタイムリーな方法で解決される、パフォーマンス上の根本的な問題点 ・真剣に捉えられているプロセスのパフォーマンスと、継続的な改善が推奨されている文化	・未解決の問題によるインシデント ・解決策の取られない貧弱なパフォーマンスによる低下のスパイラル、 ・真剣に捉えられていないパフォーマンスの測定

コントロール設計のテスト

- 全ての是正措置に対して、その開始、優先順位付け、実行責任の割り当て、追跡を行うためのプロセス、ポリシー、および手続が存在するかどうかを調査する。アプローチについての文書を閲覧して、可能ならプロセスを閲覧することにり確かめる。
- サンプルした是正措置の作業が、パフォーマンスに関して発見された問題点に正確に対応しており、進捗状況のレビューが定期的に実施されているかどうかテストする。
- パフォーマンスの履歴報告を分析して、是正措置の実施に対する合意事項からの逸脱を含む、標準を下回るパフォーマンスの傾向が日常的に特定され、上級マネジメント層に一貫してエスカレートされていることを確かめる。
- 事前に特定された結果によって決定した是正措置の作業を満足に完了したことを示す活動ログ/報告を探し出し、このような是正措置の作業が原因に対処して適宜承認されていることを確かめる。
- パフォーマンスの測定に関する研修が実施されているかどうかを調査して、それを確認する。

コントロール目標の達成をテストするために、以下のステップを踏む。

- 利害関係者にインタビューして、主要なITプロセスおよび、それがどのように測定されモニタリングされているかについての知識と意識を評価して、モニタリングシステムが、企業の成果測定システムをサポートしていることを確かめる。
- 主要なITプロセスのパフォーマンスをモニタリングするための計画、ポリシー、および手続をレビューして、それらが重要なビジネスプロセスをサポートしていることを確かめる。
- ITモニタリングシステムが、現在のビジネス戦略をサポートし、効果的なモニタリングを活用しているかどうかを判定する。
- 独立した情報源（利害関係者の情報源とシステムに関連する情報源）により、マネジメント層が適切なパフォーマンス指標を測定していることの裏づけを得る。
- 主要なITプロセスのパフォーマンスをモニタリングするための計画、ポリシー、および手続をレビューして、企業全体の成果管理システムへと統合されているかどうかを見る。
- 主要なITプロセス相互間の関連と依存関係の文書と伝達状況、特にフローチャート、システム概要図、およびデータフロー図をレビューする。
- 文書化された成果測定指標をマネジメント層とともにレビューして、以下のようなものを適切にカバーしていることを確かめる。
  - 財務を含む（しかしそれに限定しない）事業継続性
  - ビジネスとITの戦略計画とを対比させたパフォーマンス
  - 関連する法律と規制のリスクとコンプライアンス
  - 内部と外部のユーザのサービスレベルに対する満足度
  - ソリューションとサービス提供を含む主要なITプロセス
  - 将来志向の活動、たとえば成長している技術、再利用可能なインフラストラクチャ、およびビジネスとITの人員のスキルセットに関連する予測など
- 文書化された成果測定指標をレビューして、以下を確かめる。
  - ビジネスとITの達成目標と目的を記述している
  - 受け入れられている優れた実践手法に基づいている
  - 最も重要なものに焦点を当てている
  - 内部と外部の比較に有用である
  - ビジネスでの期待を反映している
  - ITの顧客とスポンサーにとって有意義である
- ITパフォーマンスの要件が、ビジネスのマネジメントとともに確立しており、企業全体のマネジメント層の主要な成果測定指標と整合していることを確かめる。
- ITパフォーマンスの測定と全てのプロセスの利害関係者対する伝達計画に対する、上級マネジメント層とビジネスマネジメント層による適切な承認をレビューする。
- 成果の測定に関連する議事録、行動一覧、ポリシー、計画、および手続をレビューして、成果測定アプローチに対する定期的なレビューと更新の証拠を得る。

- パフォーマンスデータの収集が、ビジネス要件の文書で十分にカバーされているかどうかをレビューする。
- データ収集プロセスをレビューして、自動化が検討されていることを確かめる。
- ソースデータの一貫性、網羅性、およびインテグリティを評価する。
- ターゲットが定義され、ITマネジメント層、上級マネジメント層、ビジネスマネジメント層によって適切に承認されていることを確かめる。
- 組織の研修計画、ポリシー、および手続をレビューして、測定、データ収集、および分析のスキルを確かめ、スタッフメンバーが成果測定の文化を受け入れて促進していることを確かめる。
- 収集されたデータが、事前に合意された間隔でソースデータと照合されているかどうかを判定する。
- 企業全体およびIT部門の測定報告（バランススコアカード、円形グラフ、KPIマトリックスなど）を閲覧して、その方法が企業全体のモニタリングシステムに統合されているかどうかを判定する。
- 主要な担当者へのインタビューを通じて、モニタリングと報告の方法/システムが、成果測定の目標に適合し、関連性があるかどうかを確かめる。
- アウトプットの品質と網羅性が検証されているかどうかを調査して、それを確認する。（実際のアウトプットと期待された結果とを比較し、その結果をマネジメント層と確認するなど）
- 成果測定システムをレビューして、ターゲットと測定データが正確かつ完全であるかどうかを判定する。
- マネジメント層がデータ品質測定のインテグリティを定期的にレビューしているかどうかを調査して、それを確認する。
- パフォーマンス報告を閲覧して、測定の適時性とターゲットとの比較の有効性を見る。
- パフォーマンス報告を閲覧して、パフォーマンス結果がターゲットに対して事前に合意された間隔で一貫してかつ完全に評価されており、関連する利害関係者が報告データを受け取っていることを確かめる。
- 原因が特定され、是正措置へと移行され、それが適切な権限と資源を持つ者に割り当てられ、フォローアップされていることを確かめる。
- 逸脱全体にわたって根本原因が定期的に特定され、適切に対処されているかどうかを調査して、それを確認する。
- 独立した情報源を通じて、根本原因の分析が行われ、対応につながっていることを確かめる。
- 文書が存在することを点検して、根底原因について、責任者が問題点を認識していることを確かめる。
- ITのビジネスへの貢献と、特にITソリューションとサービス提供の能力とパフォーマンスへの貢献に一般的に関係する主要な問題点（肯定的なものと否定的なもの）を上級マネジメント層の報告で明らかにしていることを確かめる。
- ITパフォーマンスの測定が、ビジネスの結果およびITがビジネス戦略をどのようにサポートするかと明確にリンクしているかどうかを調査して、それを確認する。
- ITパフォーマンスの測定がビジネスの成果への影響へと移行され、取締役会への標準的定期報告へと取り込まれていることを確かめる。
- 集約された成果報告の正確性、網羅性、および合理性を評価するために、元データから集約された報告へと結果を追跡する。
- マネジメント層の報告をレビューして、期待された成果からの逸脱が特定され、マネジメント層が問題点に対処することにコミットしていることを確かめる（行動項目、提言に対するマネジメント層のコミットメント、解決の確立したタイムフレームなど）。
- プロジェクトの文書をレビューして、上級マネジメント層の報告で特定された是正措置が、組織の変更管理プロセスに従っており（AI6 変更管理など）、プロジェクト計画、適切な承認、進捗報告、プロジェクトの変更/逸脱の追跡、完了、および承認といったような変更管理の要素をカバーしていることを確かめる。
- プロジェクトの文書を閲覧して、是正措置の作業について見て、事前に合意された解決策と比較して、モニタリングに関する全ての不備が適切に緩和されていることを確かめる。
- 進捗レビューが定期的に実施されているかどうかを判定する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 成果の測定とモニタリングのアプローチを、同様の組織や適切な国際標準/業界で認知されているベス

トプラクティスに対して、独立したベンチマークを行う。
- 企業が用いる成果測定指標を、独立した情報源（優れた実践手法、内部と業界のベンチマークなど）によって裏付ける。
- 成果目標とモニタリングデータ収集のアプローチを、同様の組織や適切な国際標準/業界で認知されているベストプラクティスに対して、独立したベンチマークを行う。
- ITの全てのエリアで、実際のパフォーマンスと計画されたパフォーマンスとを比較する。
- ITの全てのエリアで、ユーザの実際の満足度と予想された満足度とを比較する。
- 企業全体、IT部門、およびビジネス部門のマネジメント層の裏づけを取って、IT成果報告が有用かつ理解しやすいかどうかを判定する。
- 成果目標とモニタリングデータ収集のアプローチを、同様の組織や適切な国際標準/業界で認知されているベストプラクティスと照らし合わせて、独立にベンチマークを取る。
- 上級マネジメント層が成果のモニタリングについての報告に満足しているかどうかを評価する。

ME2 内部統制のモニタリングと評価

ITのための有効な内部統制プログラムを確立するには、明確なモニタリングプロセスが必要である。このモニタリングプロセスには、セルフ評価やサードパーティによるレビューの結果、発見されたコントロールの例外事項が含まれる。内部統制のモニタリングの主要な利点には、効果的かつ効率的な業務運営の実現と法規制へのコンプライアンスの確保がある。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.1 内部統制フレームワークのモニタリング 組織の目標を達成するために、ITコントロール環境とコントロールフレームワークについて継続的な監視、ベンチマーク評価、改善を行う。	・ビジネスの目標に合致したIT ・ビジネスプロセスでのコントロールの機能不全や不備の影響の減少 ・業界慣行と比較したプロセスコントロールの継続的な改善 ・コントロールからの逸脱の能動的な発見と解決 ・法律と規制の遵守	・組織の業務や評判への悪影響の増加 ・ビジネスプロセスの効果的な実行の妨げになるコントロールの欠陥 ・内部統制の構成要素の隠された機能不全

コントロール設計のテスト

・内部統制とリスク管理のための組織のガバナンス標準に対する役員レベルのサポートがあるかどうかを評価する（議事録、企業のポリシー、CEOへのインタビューなど）。内部統制とリスク評価のガバナンスが、ポリシーと手続を含んでいることを確かめる（COSO *Internal Control—Integrated Framework*や、COSO *Enterprise Risk・Management—Integrated Framework*や、COBITなど）。
・内部統制のモニタリングに対する継続的な改善のためのアプローチがあるかどうかを評価する（バランススコアカード、自己評価など）。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.2 監督レビュー 社内のIT管理に関するレビューコントロールの効率と効果を、監視し評価する。	・ビジネスの達成目標の実現をサポートするITプロセスが、効果的かつ効率的にコントロールされていることの確認 ・レビューされた結果の、全体の意思決定プロセスへの提言	・ビジネスプロセスの妨げになるコントロールの不備 ・マネジメント層の意思決定を誤らせる、不正確もしくは不完全なコントロール不備のデータ

コントロール設計のテスト

・監督者の監視とレビューを要する内部統制が特定され、その内部統制でITプロセス活動に関連する重大性とリスクを検討していることを確かめる（主要なプロセス/コントロールにリスクのランク付けが存在するなど）。
・監督者のレビューで特定された問題点をエスカレートするプロセスが定義されていることを確かめる。
・コントロールのモニタリングと報告の自動化を理解する。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.3 コントロールの例外事項 コントロール例外事項を特定し、根本的な原因を分析して識別する。コントロール例外事項をエスカレーションし、利害関係者に適宜報告する。必要な是正措置を制度化する。	·例外事項の再発に対する防止的な手段を実施できる能力 · 修正手段をタイムリーな方法で適用できる能力 · 定義されたサービスレベルを遵守するための、影響を受けるすべての当事者への報告の強化 · 最小化されるコンプライアンスの違反の可能性	· タイムリーに特定されないコントロールの不備 · コントロールの不備を知らされていないマネジメント層 · 特定された問題点を解決するのに余計な時間を要し、それによりプロセスのパフォーマンスが低下すること

コントロール設計のテスト

· コントロールの例外事項とコントロールの機能不全について、受け入れ可能なレベルの閾値を確立することがポリシーに含まれていることを確かめる。
· コントロールの例外事項のエスカレーション手続が、ビジネスとITの利害関係者に伝達され報告されていることを確かめる（インターネットや文書化された手続などによって）。エスカレーション手続には、エスカレーションのための判断基準や閾値が含まれているべきである（特定の量の影響度を下回るコントロールの例外事項をエスカレートする必要はないが、特定の量の影響度を上回るコントロールの例外事項はCIOに報告する必要があり、特定の量の影響度を上回るコントロールの例外事項は、直ちに取締役会に報告しなければならないなど）マネジメント層にインタビューして、エスカレーション手続および、根本原因の分析と報告についての知識と意識を評価する。
· 根本原因の分析と報告および例外事項の解決のための説明責任が個人に割り当てられていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.4 コントロールセルフ評価 継続的なセルフ評価プログラムを導入し、マネジメント層によるITプロセス、ポリシー、および契約に関する完全性と有効性の評価を実施する。	・再発する例外事項に対する防止的な手段を実施できる能力 ・修正手段をタイムリーな方法で適用できる能力 ・定義されたサービスレベルを遵守するための、影響を受けるすべての当事者への報告の強化 ・悪影響が生じる前に発見されるコントロールの不備 ・サービスの品質を改善するための能動的なアプローチ ・最小化されたコンプライアンスの失敗の可能性	・タイムリーに特定されないコントロールの不備 ・コントロールの不備を知らされていないマネジメント層 ・特定された問題点を解決するのに余計な時間を要し、それがプロセスのパフォーマンスを低下させること

コントロール設計のテスト

・コントロールセルフ評価手続をレビューして、対象範囲、セルフ評価のアプローチ、評価基準、自己評価の頻度、役割と責任、およびビジネス部門とIT部門の役員の利害関係者への結果報告といった関連する情報が含まれていることを確かめる（内部監査標準やセルフ評価の設計の際の慣例を参照するなど）。
・客観性を確かめ、内部統制の優れた実践手法を共有できるよう、業界の標準やベストプラクティスと対比した、コントロールセルフ評価の独立したレビュー(即ち、同様な企業や業界とのベンチマーク)が実施されているかどうかを判定するために、マネジメント層の裏づけを取る。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.5 内部統制の保証 必要に応じて、サードパーティのレビューにより内部統制のインテグリティと有効性の保証を強化する。	・ビジネスへのサービスを改善するプロセスコントロールの改善機会の特定 ・効果的な内部統制フレームワークの確立及び維持 ・組織内で伝達され、内部統制の原理と実践への意識を向上させる、コントロールの技能と知識	・効果的にコントロールされておらず、ビジネス要件に合致しないプロセス ・客観的な提言を得ることができず、その結果、ITコントロールの整備が最適化されないこと ・隠されたコントロールの不足 ・規制、契約、法律の要件の遵守を達成できていないこと

コントロール設計のテスト

- 独立したコントロールレビュー、認証、または認定が、リスクとビジネスの目標にしたがって、必要な外部のスキルセットとともに、定期的に実施されていることを確かめる（年次リスク評価を実施して、レビューのためのリスクのエリアを定義するなど）。
- レビュー結果が適切なマネジメントレベル（監査委員会など）に報告され、是正措置が開始されていることを確かめる

コントロール目標

ME2.6 サードパーティにおける内部統制

外部サービスプロバイダの内部統制の状況を評価する外部サービスプロバイダが法規制要件や契約上の義務を遵守していることを確認する。

価値のドライバー

- サードパーティのサービスの改善機会の特定
- サードパーティのサービスプロバイダに対する効果的な内部統制フレームワークの確認
- サービスプロバイダのパフォーマンスと内部統制の遵守のために提供された保証

リスクのドライバー

- サービスプロバイダのコントロールフレームワークとコントロールパフォーマンスに対する不十分な保証
- 本番の基幹システムの重大な障害
- サービス仕様を満足しないITサービス
- タイムリーに特定されない、プロバイダからのサービスの障害や劣化
- プロバイダのサービスパフォーマンスの低下による、評判の低下

コントロール設計のテスト

- サードパーティとの契約において、ポリシーと手続で内部統制要件が記載されており、監査する権利についての適切な規定が含まれていることを確かめる。
- 全てのサードパーティの内部統制を評価するために定期的にレビューが実施され、コンプライアンス違反の問題が伝達されるようにするためのプロセスがあることを確かめる。
- 業務に影響を及ぼすサードパーティサービスプロバイダから、法律や規制で要求される内部統制のアサーションを受け取ったことを確認するためのポリシーと手続があることを確かめる。
- 例外事項を調査し、適切な是正措置が実施されているという保証を得るためのポリシーと手続があることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME2.7 是正措置 コントロールの評価と報告で明らかになった是正措置について、識別、実施、追跡、および導入を行う。	・特定されたコントロールの不足が必要に応じて是正される保証 ・ビジネスにとって重要なアプリケーションの機能を継続させるための保護 ・組織全体のリスク管理プロセスのサポート ・合意されたサービスレベルの維持	・問題を引き起こし続けている、以前から特定されたコントロールの不足 ・ビジネスにとって重要なアプリケーションの不具合 ・サービスプロバイダのコントロールの不備を修正しないことによる評判の低下

コントロール設計のテスト

・全ての是正措置に対して起案、優先順位つけ、責任の割り当て、適切に行動を追跡するための手続が確立されていることを確かめる。
・標準を下回るパフォーマンスの是正措置を発見するための仕組みがあり、追加の是正措置がマネジメント層によって識別されレビューされていることを確かめる（プロジェクトマイルストーンなど）。是正措置のパフォーマンスが継続して標準を下回る場合には、上級マネジメント層にエスカレートされ、さらなる措置が取られることを確かめる（プロジェクト状況報告、IT運営委員会の議事録など）。
・是正措置の作業が、事前に特定された成果と照合して満足に完了したときに承認されることが、確立した手続で要求されていることを確かめる。

コントロール目標の達成をテストするために以下のステップを踏む。
・内部統制のモニタリングのポリシーと手続をレビューして、それが組織のガバナンス標準、業界で受け入れられているフレームワーク、および業界のベストプラクティスに従っていることを確かめる。
・ITコントロールに対する独立した評価が要求されており、IT内部統制システムについての報告がマネジメント層のレビューのために作成されているかどうかを判定する。
・アウトソースした開発や生産活動のT内部統制システムに対する独立した評価報告をレビューして、適切なアウトソーシング領域が、役員レベルで検討され承認されているかどうかを判定する。
・コントロールの例外事項を迅速に報告し、フォローアップし、分析するためのプロセスと手続の確立をレビューしていることを確認する。
・コントロールの例外事項に対処するための是正措置が選定され、実施されていることを確かめる。
・コントロールの例外事項についての活動ログとそれに関連する文書をレビューして、例外事項が迅速に報告され、フォローアップされ、分析され、追跡され、是正されていることを確かめる。
・ITの内部統制システムが、最近のビジネスでの変化とそれに関連するビジネスとITのリスクに対して最新の状態を保っているようにするために、定期的なレビューを実施していることを確かめる。
・フレームワークとビジネスプロセスとの間のギャップが特定され、適切な勧告に沿って評価されていることを確かめる。たとえば、業務のためのビジネスシステムがIT部門によって維持されておらず、IT部門が用いる確立したコントロールポリシーと手続が適用されていないことを確かめる。
・ITコントロールフレームワークのパフォーマンスが定期的にレビューされ、評価され、業界標準と業界のベストプラクティスと比較されていることを確かめる。
・コントロールの例外事項の解決の進捗状況報告をレビューして、コントロールの例外事項のモニタリングがタイムリーかつ効果的であることを確かめる。
・コントロールのセルフ評価のスケジュールをレビューして、コントロールのセルフ評価の計画と報告のサンプルを選び、効果的かつ継続的なモニタリングのための評価手続にしたがっているかどうかを判定する。
・独立したレビュー、ベンチマーキング、および指摘されたコントロールの不備の是正措置のためのコントロールセルフ評価の報告のサンプルをレビューする（コントロールの例外事項の重要性にランクをつけて、そ

れにしたがって是正措置に優先順位をつけることを検討する）。
- コントロールのセルフ評価の結果と例外事項が報告されており、コントロールの例外事項と是正措置を追跡するためのプロセスがあることを確かめる。
- 独立したレビューを行う外部の専門家やスタッフメンバーの、関連する監査経験、関連する業界の知識、および適切な認証/訓練について、その能力を評価する。
- レビューを行う人員が独立していることを確かめる（署名された機密保持契約をレビューする）。
- ITコントロールにおけるサードパーティサービスの既存の契約書をレビューして、明確な対象範囲、契約上の義務の割り当て、および機密性を契約条件でカバーしていることを検証する。
- 特定された内部統制の重要な欠陥が、マネジメント層の注意を直ちに引くために報告されていることを確かめる。
- マネジメント層のメンバーの裏づけを得て、マネジメント層がサードパーティのコンプライアンスレビューをレビューして、サードパーティが法律、規制、および契約で要求されている義務を遵守していることを確かめているかどうかを判定する。
- サードパーティ契約のサンプルを選び、内部統制要件の仕様と、必要に応じて、監査する権利の規定の確立状況を調査する。
- 以下のいずれかを実施しているかどうかを判定するために裏づけを取る。認証/認定のレビュー、適切な監査契約（SAS 70タイプ2の監査契約など）、またはITマネジメント層によるサービスプロバイダに対する直接の監査。
- サンプル対象のサードパーティについて、内部統制遵守のテスト報告を入手してレビューして、サードパーティサービスプロバイダが該当する法律、規制、および契約上のコミットメントを遵守していることを確かめる。
- 証拠をレビューして、コンプライアンス違反の問題点が伝達され、その問題点に対処するための是正措置の計画（タイムフレームを含む）があることを確かめる。
- コントロールの不備の是正に優先順位をつけるために用いる方法が合理的かどうかレビューする。
- 是正対象の問題点リストをレビューして、そのような問題点に対して適切に優先順位をつけているかどうかを判定する（重要、高、中、および低など）
- プロジェクトのスケジュール管理ツールをレビューして、それを是正措置と比較して、リスクが高いと特定されたエリアに対して十分に優先順位をつけていることを確かめる。
- 承認を調査して、それがタイムリーに行われたかどうかを判定する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- 実際の主要なコントロールの不備のそれぞれについて、組織への影響度を計算する。
- 潜在的な主要なコントロールの不備のそれぞれについて、組織への影響のリスクと発生可能性を定量化する。

ME3 外部要件に対するコンプライアンスの保証

コンプライアンス要件への監督を効果的に行うには、法律、規制、および契約に対するコンプライアンスを確保するための、独立したレビュープロセスを確立する必要がある。このプロセスには、監査の憲章、監査人の独立性、監査人の職業倫理と規範、計画策定、監査の実施、および監査活動に関する報告とフォローアップが含まれる。このプロセスの目的は、ITのコンプライアンスを積極的に保証することである。

コントロール目標	価値のドライバー	リスクのドライバー
ME3.1 外部法律、規制、および契約のコンプライアンス要件の特定 組織のITポリシー、標準、手続、および方法論を適合させるために、遵守すべき国内外の法律、規制、その他の外部要件を継続して特定する。	・法律と規制に対応するための優れた実践手法の特定 ・諸規制要件に対する要員の意識改善 ・プロセス・パフォーマンスと、法律や規制に関する遵守の向上 ・企業の業績改善	・関連する法律や規制が見落とされ、コンプライアンス違反につながること ・財務上の損失と処罰につながる潜在的領域が特定されないこと ・顧客とビジネスパートナーの満足度の低下 ・顧客や規制当局との係争の可能性の増加 ・規制当局の課す制裁による事業継続に対するリスクの増加 ・企業の業務および財務のパフォーマンスの貧弱さ

コントロール設計のテスト

・ITに影響を及ぼす法律、規制、および契約上の義務をレビューする手続があることを確かめる。このような規制遵守手続で以下を行うべきである。
  - IT組織に関連する適用法や規制の影響を特定し評価する
  - 法律と規制の要件の影響を受ける関連するITのポリシーと手続を更新する
  - 電子商取引、トランスボーダーデータフロー、プライバシー、内部統制、財務報告、業界特有の規制、知的財産としての著作権、健康と安全等に関する法律と規制の領域が含まれている
  - 法律や規制の要件のレビューの頻度が含まれている（年次または、法律、規制、契約上の要件が新規に制定されたり改正された時など）
・該当する法律、規制、および契約の要件の全てのログ、その影響、および要求されている行動が維持され最新の状態を保っていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME3.2 外部要件への対応の最適化 ITのポリシー、標準と手続をレビューおよび最適化し、法規制要件に対して効率的な対応を確実に行う。	・標準と方法論の利用により、適用される法や規制を企業が遵守することのサポート ・定期的にレビューされ、組織の目標と整合性のあるポリシー ・法律と規制の遵守要件に対する要員の意識改善 ・法律と規制の遵守に関連するプロセスのパフォーマンスの向上	・識別されていないコンプライアンス違反の領域 ・陳腐化したにもかかわらず効力を持ち続けているコンプライアンス要件 ・企業のコンプライアンスの必要性に合致していないポリシー ・法律と規制の要件を遵守するための手続と活動を要員が知らないこと

コントロール設計のテスト

・法律、規制、および契約上の要件の遵守を確実にするための手続と活動があることを確かめる。
・適切な部門が含まれていることを確かめる（法務、製造、経理、人事など）

コントロール目標	価値のドライバー	リスクのドライバー
ME3.3 外部要件に対するコンプライアンスの評価 ITのポリシー、標準、手続、および方法論について、法律や規制の要件に対するコンプライアンス状況を確認する。	・法律と規制に対応するために、企業全体で効果的に導入されている優れた実践手法 ・法律と規制の遵守およびプロセスのパフォーマンスの向上 ・タイムリーな是正措置をサポートするような逸脱の特定	・財務上の損失と処罰 ・顧客とビジネスパートナーの満足度の低下 ・コンプライアンス違反のインシデントが特定されず、企業全体の業績と評判に悪影響が及ぶこと ・係争の可能性の増加

コントロール設計のテスト

・IT組織のポリシー、標準、手順書をレビューして、特定されたコンプライアンス違反（法律と規制）のギャップに対処するため、定期的かつタイムリーに更新されていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME3.4 コンプライアンスの積極的な保証 コンプライアンスの保証をはじめ、社内命令や外部の法律、規制、/契約上の要件に起因する内部ポリシーへの全面準拠を確認し、報告する。また担当のプロセスオーナにより、コンプライアンスが不十分な場合に取るべき是正措置がタイムリーに講じられていることを確認する。	・標準と方法論の利用を通じて、適用される法と規制を企業が遵守することの確認 ・法律と規制に対応するため、企業全体で効果的に導入されている優れた実践手法の識別 ・適用される法と規制の遵守に関連するプロセスのパフォーマンスの向上 ・コンプライアンス要件からの逸脱が特定されタイムリーに是正されていることの確認	・コンプライアンス違反のインシデントを報告せず、企業全体の業績と評判に悪影響が及ぶこと ・係争の可能性の増加 ・コンプライアンス違反が特定されず報告されない領域 ・是正措置がタイムリーに開始されず、組織全体の業績に悪影響が及ぶこと

コントロール設計のテスト

・適用される法、規制、および契約上のコミットメントの遵守をプロセスオーナが定期的に確認しているという証拠を、プロセスオーナからレビューする（財務報告および、レビューを完了したことを認める規制当局からの手紙など）
・内部と外部のレビューを追跡し実行するためのプロセスがあることをレビューして、レビューを支援/完了するための十分な計画と資源配分があることを確かめる（規制要件の棚卸、内部のコンプライアンスレビューのスケジューリング、レビューを支援するのに必要な資源のスケジューリングなど）。
・法律と規制の要件遵守のレベルを、独立した第三者によって定期的に評価するための手続があるかどうかを調査する。
・ポリシーと手続をレビューして、適用される法、規制、契約上のコミットメントの遵守を定期的に確認すること（アサーションの受け取りなど）が、サードパーティサービスプロバイダとの契約で要求されていることを確かめる。
・コンプライアンス違反のインシデントをモニタリングして報告するためのプロセスが導入されており、そこには、必要に応じて、発生したインシデントの根本原因をさらに調査することが含まれていることを確かめる。

コントロール目標	価値のドライバー	リスクのドライバー
ME3.5 報告の統合 法律、規制、および契約要件に関するIT部門の報告と、その他のビジネス部門からの類似報告を統合する。	・コンプライアンスの問題点についての企業の報告の活用 ・他のビジネスの機能の妨げになっている場合にコントロールギャップをタイムリーに発見できるようにしていること ・効果的なコンプライアンス対応の確立にあたっての、組織の標準と方法論のサポート ・企業が直面するコンプライアンスリスク全体の減少	・企業がコンプライアンスに違反する危険の増加 ・他のビジネス部門がITプロセスに関連するコンプライアンス要件とその遵守状況に気づいていないこと ・ITに関連するコンプライアンスの問題点が、全体報告へと統合されず、経営陣の戦略的な意思決定の誤りにつながること

コントロール設計のテスト

・以下を質問して確認する。
  – 全ての履歴情報を保持する要件を含め、要件が法律と規制の遵守に関する企業の報告のために調整されている
  – ITコンプライアンス報告が、配布、頻度、対象範囲、内容、および形式といった企業の報告要件にしたがっており、報告の一貫性と網羅性を確保している

コントロール目標の達成をテストするために以下のステップを踏む。

・特定のコンプライアンス要件を、コンプライアンス違反を防止し、また発見するための手続まで、認識と文書化から追跡する。関連する担当者にインタビューして評価して、特定された法律、規制、および契約上の要件に気づいていることを確かめる。
・内部と外部の専門家の助言から、該当する法律、規制、標準および、企業のコンプライアンスの状況の証拠やログをレビューする。コンプライアンス違反の領域については、要件に対処するためのマネジメント層の是正措置を特定する。
・コンプライアンスのカバー範囲、手続、活動が、内部と外部の専門家によって定期的にレビューされていることを確かめる（セキュリティ監査、SAS 70など）
・必要に応じて、該当するサードパーティからの助言を得ていることを確かめる。
・法律と規制の遵守の定期的なレビューの証拠のためにITプロセスの文書をレビューして、その文書が必要に応じて更新されていることを確かめる。
・コンプライアンス違反で再現するパターンを探し、その原因が定期的に評価されているかどうかを調査する（その評価の結果として、ポリシー、標準、手続、プロセス、活動への変更が実施されているかどうかを判定する）。
・独立した内部または外部の当事者が実施する、法律と規制の要件についてのコンプライアンス評価報告をレビューして、定期的なレビューが行われていることを確かめる。
・サードパーティ契約のサンプルをレビューして、該当する法律、規制、契約上のコミットメントの遵守を定期的に確認することを要求するような規定があるかどうかを判定する。
・サードパーティサービスプロバイダからサンプルを選び、コンプライアンスのアサーションの証拠を入手して、コンプライアンスを定期的に確認するという契約上の要件を遵守しているかどうかを判定する。
・サードパーティのコンプライアンス報告からの知見と、コンプライアンス違反とその解決からの知見をレビューして、運用の有効性の不備に対処しているかどうかを判定する。
・ITコンプライアンス報告のための標準が、対象範囲、内容と形式を含む、一貫性と網羅性を確実にするための合意済みの形式にしたがっていることを確かめる（合意手続をレビューするなど）。
・コンプライアンス報告をレビューして、ITコンプライアンス評価の結果が取り入れられ、他のビジネス部門か

らの同様の報告と整合的に提示されたことを確かめる。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- コンプライアンス違反の結果として企業に課される罰金やその他の処罰の費用を特定して数量化する。
- 規制要件（“Statement of the Securities and Exchange Commission Concerning Financial Penalties,” US Securities and Exchange Commission [SEC], 2006など）のコンプライアンス違反のリスクと発生可能性を数量化して、企業への影響についての理解を促進する。

ME4 ITガバナンスの提供

効果的なガバナンスフレームワークの確立には、組織構造、プロセス、リーダシップ、役割、および責務を定義し、企業の戦略と目標に沿った企業のIT投資を確実に実現することが含まれる。

コントロール目標	価値のドライバー	リスクのドライバー
ME4.1 ITガバナンスフレームワークの確立 全社的な企業ガバナンスと統制環境に合わせてITガバナンスフレームワークを定義、確立し、整合を図る。フレームワークは、適切なITプロセスとコントロールモデルを基準として定義し、明確な説明責任と実践方法を定めて、内部統制や監督における機能停止を回避できるようにする。ITガバナンスフレームワークでは、法規制へのコンプライアンスが企業の戦略や目標と整合するように保証され、確実に達成されることを確認する。ITガバナンスの状況と問題点を報告する。	・企業の戦略と目標に沿っているITの意思決定 ・企業のアプローチと整合性のあるガバナンスフレームワークのための一貫したアプローチの達成 ・効果的かつ透明に監視されるプロセス ・法律と規制要件の遵守の確認 ・ガバナンスに対する取締役会の要求への高い満足度の可能性	・ITプロセスのために確立された、効果的でない実行責任と説明責任 ・企業全体の目標と戦略をサポートしていないITポートフォリオ ・ITプロセスの有効性と効率性を維持して改善するための是正措置が、特定されなかったり実施されなかったりすること ・期待通りに機能していないコントロール

コントロール設計のテスト

・以下を質問して確認する。
  - ITガバナンスフレームワークを企業全体のガバナンスとコントロールの環境と整合させるための合意済みのプロセスが存在する
  - フレームワークが包括的なITプロセスとコントロールのモデルに基づいており、リーダーシップ、明確な説明責任、役割と実行責任、情報要件、組織構造といった、内部統制と監督の機能停止を防止するための活動を定義している
  - IT戦略委員会、IT運営委員会、技術委員会、ITアーキテクチャレビュー委員会、およびIT監査委員会といったようなマネジメント層による適切なガバナンス構造が存在する。これらのそれぞれについて、業務指示書が存在することを確かめる。
  - ITガバナンスフレームワークが、戦略的な整合性、価値の提供、資源管理、リスク管理、成果の測定に焦点を当てている
  - ITの戦略と目標の提供を測定し、評価し、ITガバナンスの全ての問題点と是正措置を、集約されたマネジメントリポジトリや追跡メカニズムへと集計するためのプロセスが存在する
  - ITリスク管理に対する明確な実行責任が確立している
  - ITガバナンスの状況と問題点が、企業のガバナンス監督体制に報告されている

コントロール目標	価値のドライバー	リスクのドライバー
ME4.2 戦略との整合 ITの役割、技術の現状、運用能力などのITに関する戦略的な課題について、取締役会や経営層の理解を得る。ビジネス戦略に対するITの潜在的貢献に関する理解を、ビジネス部門とIT部門の間で確実に共有する。取締役会や管轄のIT戦略委員会などの管理組織と連携して、マネジメント層にITに関連する戦略的指針を示す。これにより、戦略と目標を、各ビジネス部門とIT部門に浸透させ、ビジネス部門とIT部門間の信頼関係が確立されるようにする。戦略上の決定やIT関連の投資による便益享受において、ビジネス部門とIT部門による共同責任を強調し、戦略とその実施においてIT部門とビジネス部門の連携を図る。	・企業の目標に対する責任が増加しているIT ・ビジネスの達成目標を効率的かつ効果的な方法で容易にするのを手助けするIT資源 ・ビジネス戦略のための機会を実現可能とするITの能力 ・IT投資の効率的な配分と管理	・IT投資の非効率的な配分と管理 ・企業の目標をサポートしていないIT ・企業全体の戦略と整合していないIT戦略計画 ・定義されておらず、ビジネスの達成目標をサポートしていないIT指針

コントロール設計のテスト

・IT戦略の文書を閲覧して、それが取締役会/上級マネジメント層の提供する方向性をサポートしているかどうかを評価する。IT戦略は、ビジネス戦略と、ITとビジネスの業務との適切な整合性を反映すべきである。
・IT戦略計画プロセスに、ビジネス部門からの関与が含まれており、ビジネスの戦略と目標との整合性が示されているかどうかを判定する。
・IT戦略の文書をレビューして、ITの役割、ビジネスの原理からのIT指針、ITインフラストラクチャとアプリケーションポートフォリオのビジネスへの影響を、ITがどのようにモニタリングするか、ビジネス全体の戦略へのITの潜在的な貢献がIT戦略の文書に含まれているかどうかを評価する（ITプロジェクトの導入後に、ITプロジェクトが提供する便益を評価するなど）。

コントロール目標	価値のドライバー	リスクのドライバー
ME4.3 価値の提供 IT関連の投資プログラムとその他のIT資産やサービスを管理し、企業の戦略と目標の実現を支援するにあたって、それらが最大限の価値を確実に発揮できるようにする。IT関連の投資に期待されるビジネス上の成果とそれらの成果の達成に必要な全ての取り組みが理解されていること、全体的かつ一貫したビジネスケースが作成され利害関係者によって承認されていること、資産と投資がその経済的ライフサイクルにわたり管理されていること、そして、新規サービスへの貢献、効率性の向上、顧客要望への対応力の強化など、便益の実現に向けた積極的な管理が行われていることを確認する。ポートフォリオ、プログラム、およびプロジェクトの管理に統制のとれたアプローチを用い、ビジネス部門が全てのIT関連の投資を主導し、IT部門がIT能力とサービスの提供費用の最適化を保証するようにする。	・高い費用効率による、ソリューションとサービスの提供 ・利用が最適化されているIT資源 ・ビジネスでの必要性が効率的にサポートされていること ・企業の利害関係者がITを利用する際のサポートの増加 ・ビジネスの目標に対し増加するIT貢献の価値 ・費用と予想される便益の把握が信頼でき正確であること	・間違った方向を向いているIT投資 ・ITの資産とサービスから価値を得ていないこと ・顧客満足の低下 ・ITへの投資とITオペレーションの費用の増加 ・ビジネスの目標とITアーキテクチャとの間に整合性がないこと ・期待される便益が実現しないこと

コントロール設計のテスト

・IT投資に対して、ビジネス部門とIT部門との間に連帯責任があることを確かめる。
・ITが戦略にどのような価値を提供するかを示す文書を閲覧する。それには、納期と予算を守り、適切な機能を持ち、意図した便益をもたらすことが含まれるべきである。
・発展中の新技術に関するビジネス部門と役員の期待に応えながら、ITの価値への貢献を増やすための方法を定期的に特定して評価するためのプロセスがあるかどうかを判定する（運営委員会の議事録など）。
・ビジネス部門とITプロバイダとの間のパートナーシップがあり、ソーシングの意思決定に対する責任を共有しているかどうかを判定する。
・ITの価値（市場に提供するまでの時間、費用と時間の管理、提携の成功など）に対するビジネス部門の期待をIT部門が意識しており（または文書化しており）、IT部門が継続的にITの価値に気づいているかどうかを判定する。
・ITとビジネスのアーキテクチャが、最大の価値を推進するよう設計されるための効果的なプロセスがあるかどうかを判定する。
・リスク、費用および便益に基づいて、IT投資を受け入れ可能な予算と調整し、IT投資の収益と競争的な側面を考慮するための効果的なプロセスがあるかどうかを判定する。
・ITの文書を閲覧して、ビジネス要件への合致、将来の要件を導入できる柔軟性、スループットと応答時間、使いやすさ、セキュリティ、および情報のインテグリティ・正確性・最新性を含む、ITの成果物の内容に対してビジネス部門が期待値を設けているかどうかを評価する。

コントロール設計のテスト（続き）

- 費用との関係で価値を最適化するために定期的に評価されており、競争優位、注文/サービスを満たすための経過時間、顧客満足、従業員の生産性、および収益性をもたらすような、効果的なITポートフォリオ管理プロセスがあるかどうか判定する。
- IT予算とIT投資計画に対するマネジメント層のモニタリングの結果をレビューして、それが現実的であり、全体的な財務計画（これは規制の要件の遵守も含むだろう）へと統合されていることを確かめる。
- IT資産ポートフォリオ管理プロセスが、実際の費用と投資の収益率を管理し報告していることを判定する。

コントロール目標

ME4.4 資源の管理

IT業務やIT運用について定期的な評価を実施し、IT資源の投資、利用、および割り当てを監督することにより、資源の運用や割り当てが、現在または将来的な戦略目標およびビジネス上の緊急課題に合わせて行われていることを確認する。

価値のドライバー

- IT資源の効率的かつ効果的な優先順位付けと活用
- 最適化されたITの費用
- 便益の実現の可能性の増加
- サポートされ最適化されたIT計画
- 将来の変化への準備

リスクのドライバー

- 断片化された非効率的なインフラストラクチャ
- 望ましい達成目標を実現するのに十分でない能力、技能および資源
- 達成されていない戦略目標
- 資源の配分に対する不適切な優先順位

コントロール設計のテスト

- 経営者への質問を通じて、IT資源を調達し利用するための高レベルの指示があることを確かめる。
- 上級取締役との会議の議事録をレビューして、このような指示活動の有効性を判定する。
- 戦略目標を満足させるITの資源、技能、インフラストラクチャが利用可能であり、継続的な可用性を実現するためのポリシーがあるかどうかを調査して、それを確認する。
- ビジネスの情報の作成と共有を促進するようなITインフラストラクチャが、最適な費用で、提供されているかどうかを調査して、それを確認する。
- 資源管理のためのポリシー、手続、プロセスがあることをレビューし、それが以下点で効果的に機能していることを確かめる。
  - 全体的なIT投資と資源の利用を最適化し、企業の成長と維持との間でバランスを取る
  - 情報と知識の資源から収益を得る
  - 効果的なITパフォーマンスを可能にする資源配分をするように、ビジネスの優先順位を確立する
- 全体的なIT投資と資源の利用の最適なバランスを独立に策定し評価し、それを実際の発見事項と比較する。
- ITインフラストラクチャを使って特定の項目を追跡し、情報の作成と共有が効果的に促進されているかどうかを判定する。
- 適切な人員配置と資源配分により、ITから最大の価値を得るために、主要な役割の割り当てと定義が行われているかどうかを調査して、それを確認する。
- 定義された役割をレビューし、それが効果的に割り当てられ実行されていることを確かめる。
- ビジネス戦略をサポートする能力を確保するために、能力評価の手続があり、それを定期的に実行しているかどうかを調査して、それを確認する。
- 能力評価を実施して、それを定義されたビジネス戦略と比較する。

コントロール目標	価値のドライバー	リスクのドライバー
ME4.5 リスクの管理 取締役会と連携して、企業のITリスク選好度を定義し、実際のITリスクが取締役の持っているリスク選好度を越えていないことを実証できるように、適切なITリスクマネジメントが実践されていることを合理的に保証する。リスクマネジメントの責務を組織に組み込み、ビジネス部門とIT部門がITにかかわるリスクとビジネスへの影響を定期的に評価、報告して、企業におけるITリスクの状況が、あらゆる利害関係者に明示されるようにする。	・具体化する前に特定されるリスク ・リスクへの注意が増すこと ・重大なリスクを管理するための明確な説明責任と実行責任 ・ITリスク管理のための効果的なアプローチ ・マネジメント層の期待と整合するITリスク・プロファイル ・最小化されるコンプライアンスの失敗の可能性	・効果的でないリスクの特定と管理 ・予想外のリスクを管理するための支出と費用の増加 ・重大なITアプリケーションとITサービスの不具合 ・ITリスクのオーナシップの欠如

コントロール設計のテスト

・以下を質問して確認する。
  - ITリスクの影響度、リスク管理の手段と関連する費用といったマネジメント層からの情報に基づいて、取締役会が、企業全体のリスク選好を定義し、定期的に再評価し、伝達している
  - マネジメント層がIT活動のリスク評価の結果をレビューして、リスクを低減するためのコントロールを検討しながら、総合的なリスクの影響度が定義されたリスク選好を越えていないことを確かめ、必要に応じて全体のリスクの影響度を減らすための追加コントロールの導入を監督している
  - ITリスク管理の問題点をITガバナンスの状況と問題点の報告に含めて、ITリスクの透明性を全ての利害関係者に提供するためのプロセスが存在する

コントロール目標	価値のドライバー	リスクのドライバー
ME4.6 成果の測定 合意されたIT目標が達成された、またはそれを上回る成果が達成されたか、あるいはIT目標に向けた進捗で期待以上の成果が上げられたかを確認する。合意された目標が達成されていない場合、あるいは進捗が期待どおりではない場合は、マネジメント層の是正措置をレビューする。取締役会に、関係するポートフォリオ、プログラム、およびIT成果を報告して、上級マネジメント層が当該の目標に向けた企業の進捗状況についてレビューできるように支援する。	・プロセスのパフォーマンスの向上 ・特定された改善の領域 ・企業の戦略との整合性を保ったITの目標と戦略 ・効果的かつ透明でに監視されたプロセス ・タイムリーで効果的なマネジメント層への報告が可能になること	・タイムリーに特定されないパフォーマンスのギャップ ・利害関係者の信頼の低下 ・サービスの逸脱と低下が認識されず対処されないことで、ビジネス要件を提供できなくなること ・法律と規制を遵守できなくなるおそれが生じるサービスパフォーマンスの低下

コントロール設計のテスト

・以下を質問して確認する。
  - ITスコアカードのパフォーマンスの達成度が、ビジネスのスコアカードの達成度と整合しており、ビジネス部門によって受け入れられている
  - マネジメント層が、IT戦略目標の達成と関連した、ITパフォーマンスの測定と報告のプロセスの有効性と成果物について、正確性と網羅性を評価して受け入れている。計画された目標が達成された度合い、獲得した成果物、および達成した成果目標が状況報告に含まれていることを確かめる。
  - 取締役会が、パフォーマンスに関する重要な問題に対しマネジメント層の是正措置の適正性を評価して、必要に応じて組織やシステムにおける原因を是正するための指示を提供している

コントロール目標

ME4.7 独立した保証

関連する法規制に対するITの準拠状況をはじめ、組織のポリシー、標準、手続、一般に受け入れられている実践方法、および効果的/効率的なIT成果について、(内外を問わず)独立した保証を確保する。

価値のドライバー

・特定されたサービス改善のための機会
・適時に発見されたギャップ
・効果的なガバナンス、リスク管理、および内部統制のメカニズムと手続に対する信頼できる保証
・取締役会と役員に対する、ガバナンスが有効に機能しているという保証

リスクのドライバー

・サービスパフォーマンスの低下を発見または防止できないことによる評判の低下
・効果的でないITガバナンス、リスク管理、内部統制の準備
・倫理に反する行動が取られ、受け入れられること

コントロール設計のテスト

・監査委員会が設置され、何が重要なリスクかを検討し、それをどのように特定し、評価し、管理するかを評価し、ITとセキュリティの監査を委任して、それに続く提案を厳格にフォローアップする権限を持っているかどうかを調査して、それを確認する
・監査委員会にインタビューして、自らの責任に対する知識と意識を評価する。確立された監査委員会が効果的に機能しているかどうかを判定する。
・ITのポリシー、標準および手続の遵守状況に対する独立したレビューや認証、承認を得ているかどうかを調査して、それを確認する。独立したレビューによって作成された文書が十分かどうか、実際に調査する。

コントロール目標の達成をテストするために以下のステップを踏む。
・取締役会/上級マネジメント層の会議の議事録をレビューして、企業でのIT資源とIT能力の利用に対してビジネス上の指示が与えられているかどうかを判定する。
・IT資源の利用に関連する企業全体のリーダーシップと組織構造をレビューして、企業全体との関連での適正性と、IT資源の監督と管理のカバー範囲の網羅性を判定する。
・ITガバナンスを確立しサポートするために用いられているプロセスモデルを特定し、その適用の十分性と有効性を評価する。
・IT戦略計画の議事録をレビューして、ITとビジネスの達成目標と目的が整合しているか確かめる。
・全ての主要なIT関連投資に対し、直接的で積極的な関与と説明責任を持つために指名されたビジネススポンサーがいることを確かめる。
・ITサービスの計画をレビューして、それをビジネス戦略と比較して、その指針によってITが最適なサポートを提供できるようになっているか評価する。
・IT戦略に責任を持つ人へのインタビューを通じて、IT戦略がビジネス全体の達成目標とうまく統合されて

いることを確かめる。
- ビジネスとITの達成目標と目的が、関連する当事者に明確に伝達され、適切な仲介（技術計画など）により有効に機能しているかどうかを評価する
- IT運営委員会が、IT戦略がビジネス戦略と整合するようにし、それを支える戦略と計画が一貫しており一体化されていることを確かにすることで、ビジネスとの整合性を向上しているかどうかを評価する。
- 役員がITガバナンスについての報告を定期的にレビューし、IT戦略の問題点とその解決策が報告されているかどうかを判断するためのプロセスがあるかどうかを判定する。そのような報告には、戦略計画の進捗状況や主要なサービス成果指標、重要なリスクの評価とリスク低減の側面が含まれているべきである。
- ITガバナンスの整備の確立と有効性に関連して、企業に提供される独立した保証の程度を特定して評価する。

コントロールの欠陥の影響を文書化するために以下のステップを踏む。
- ITが、新しい業務や重大なビジネスサービスをサポートできない場合の影響を定量化する。
- メディアの注目等を引きつけるようなIT関連のインシデントと問題点を特定する（失敗した主要なプロジェクト、コンプライアンス違反、セキュリティの不全など）。

付録Ⅵ—アプリケーションコントロール（AC）

AC1　ソースデータの作成と承認
AC2　ソースデータの収集と入力
AC3　正確性、網羅性、認証のチェック
AC4　処理のインテグリティと妥当性
AC5　出力のレビュー、照合、およびエラー処理
AC6　トランザクションの認証とインテグリティ

付録VI—アプリケーションコントロール（AC）

プロセス保証のステップ

AC1 ソースデータの作成と承認

コントロール目標	価値のドライバー	リスクのドライバー
原始帳票が、定められた手続に従い、該当文書の作成と承認に関する職務分離を十分に考慮した上で、許可を受けた資格のある要員によって準備されていることを確認する。入力ミスや入力漏れは、効果的な入力フォームを作成することで最小限に抑えることができる。入力ミスや不正データを検出して、報告、訂正できるようにする。	・ データのインテグリティ ・ 標準化され承認されたトランザクション文書 ・ アプリケーションのパフォーマンスの改善 ・ トランザクションデータの正確性	・ 重要なデータのインテグリティの毀損 ・ 承認されていないトランザクションもしくは間違ったトランザクション ・ 処理の非効率性と手戻り

コントロール設計のテスト

・ システムの設計が、識別と承認レベルの管理の機能を満たしていることを確かめる。
・ システムの設計が、事前承認済みのリストと関連する署名を用いた機能を使って、文書が適切に承認されたことを確定しているか、調査し確認する。
・ ソースドキュメントや入力画面が、予め記入済みのデータや選択肢を使って設計されており、短時間での入力完了と、エラーの可能性の最小化をしているか、評価する。
・ システムの設計が、フォームの完全性と承認のレビューを促し、不完全あるいは未承認文書を処理しようとした状況を識別をしやすくしているかどうか、調査し確認する。
・不完全あるいは未承認文書が拒否されたことが、ひとたび識別されたら、オーナーの所へ修正のために返送され、それを追跡し報告するように、システムが設計されているかどうかを調査し確認する。

コントロール目標達成のテスト

・ 承認リストを検査して、各トランザクションのグループについて、承認レベルが適切に定義されていることを確認する。承認レベルが適切に適用されていることを観察する。
・ データ作成とその手続きの文書を検査・観察して、その手続きが理解され、正しいソースメディアが用いられているかどうかを調査し確認する。
・ 手続きに規定されている場合には、起票者と承認者との間の適切な職務の分離が存在するかどうかを調査し確認する。
・ 承認アクセスコントロールが有効であることを確認するために、文書を検査し、プロセスに沿ってトランザクションを追跡する。可能な場合には、トランザクションを追跡するために、サンプルデータ、組み込み監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いる。
・ 承認された要員とその署名の一覧が適切な部門によって維持されているかどうかを、調査し確認する。可能な場合には、承認された要員の一覧が、要員がデータを入力するのを許可/制限するように有効に設計されていることを確認するため、サンプルデータ、組み込み監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いてトランザクションを追跡する。
・ 承認された要員を維持するためのプロセスと手続きが有効かつ適時であることを確認するために、承認された要員の一覧および他の文書を検査し、プロセスと手続きを観察する。従業員のサンプルを選び、彼らの承認レベルが役割と責任に対応しているか評価する。

コントロール目標達成のテスト(続き)

- すべてのソースドキュメントが、エラーを減らすために事前決定済みの入力コードとデフォルト値といった標準的な構成要素を含んでおり、モニタリングのためにトランザクションの日時を記録し、妥当性を確かにするために承認情報を含んでいるかを調査し確認する。
- 可能な場合には、正確性を向上し承認の証拠を提供するような標準化された構成要素を用いていることを確認するために、トランザクションを選び、サンプルデータ、組み込み監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いる。
- データ入力の最中に、ソースドキュメントをレビューし、不完全だったり、署名が無かったり、承認の不適切な文書が、修正のために起票者のもとへ返送され、それを記録して、修正された文書が起票者によって適時に返送されていることを確認するために、ログが定期的にレビューされているかを調査し確認する。不完全な文書が効果的に発見され、起票者が適時に完成させていることを確認するために、ソースドキュメントを検査し、ログとその他の文書をレビューする。
- ソースドキュメントのフォームをレビューし、それが利用可能で、エラー防止を活用しており、迅速で効率的な作成を可能にしているかどうかを確認する。

AC2 ソースデータの収集と入力

コントロール目標

データ入力は、許可を受けた資格のある要員によってタイムリーに実施されるように定める。誤入力されたデータの訂正と再送信は、元のトランザクションの許可レベルを損なうことのないように実施する。元の原始文書は、復元時に必要となる場合に備えて、一定期間にわたって保存しておくようにする。

価値のドライバー

- 正確なデータ入力と効率的な処理
- 適時に発見されるエラー
- 機密性の高いトランザクションデータの保護

リスクのドライバー

- 不完全なデータ入力による処理の非効率性
- 重要なデータのインテグリティの毀損
- アクセスコントロール違反
- 発見されないデータ入力のエラー

コントロール設計のテスト

- ソースドキュメントの適時性、網羅性および正確性についての判断基準が定義され伝達されているかどうかを調査し確認する。
- エラー修正、残高の不一致、および上書き入力のための文書化された手続きが存在するかどうかを調査し確認する。手続きが、適時なフォローアップや修正、承認、再提出のためのメカニズムを含んでいることを確かめる。エラーメッセージの記述内容や上書きメカニズムといったような要素について手続きを評価する。
- 予めシリアル番号を振ったソースドキュメントや、他の独自の方法を使って、当該データの識別を要するような重要なトランザクション区分を識別する基準の基となるポリシーと手続きが確立されているかを調査し確認する。
- 文書保存ポリシーを決定する基となるポリシーと手続きが存在しているかを調査し確認する。文書保存ポリシーを評価する際に考慮すべき要素は、トランザクションの重要性や当該データの形式、保存の方法、保存場所、保存期間、コンプライアンス、法的要件を含む。
- 主要なグループのトランザクションのそれぞれについて、入力や編集、受け入れ、拒否、上書きの承認を決定するための判断基準を文書化したものが存在するかを調査し確認する。
- ポリシーと手続きの文書を検査して、適時性や網羅性、正確性の判断基準が適切に記述されていることを確かめる。

コントロール目標達成のテスト

- 重要なソースドキュメントは予めシリアル番号が振られ、番号が飛んでいるときにそれが識別され考慮されているか調査し確認する。
- エラーメッセージが適時に生成され、エラーが修正されるか適切に上書きされない限りトランザクションが処理されず、直ちに修正されなかったエラーが記録されて正当なトランザクションの処理が続き、エラーログがレビューされ、特定の合理的な期間内に対応策が取られているか調査し確認する。
- エラーや残高の不一致なデータについての報告が適切な担当者によってレビューされ、合理的な期間内にすべてのエラーが識別され、修正され、チェックされ、エラーが修正されるまで報告され続けているか調査し報告する。
- トランザクションの流れのサンプルで、ソースドキュメントの保存が、ソースドキュメントの保存に関して定められた基準により定義され適用されているか調査し確認する。
- 一連の重要なトランザクションを選び、以下を実施する。
  - トランザクションの入力、編集および受け入れ等に対するアクセスコントロールの実際の状態を、定められた基準やポリシー、手続きと比較する。
  - 重要なソースドキュメントに予めシリアル番号が振られているか、もしくはソースデータを識別する他の独自の方法が用いられているかどうか調べる。
  - 文書を検査するかトランザクションのウォークスルーを行って、トランザクションの入力、編集、承認、受け入れ、拒否、およびエラーの上書きをできる人を識別する。
  - 特定の期間でのトランザクションのサンプルをとり、そのようなトランザクションのソースドキュメントを検査する。適切なソースドキュメントのすべて入手可能なことを確かめる。
- 自動化ツール（CAAT）を用いて、番号の飛びや欠落、重複を識別してレビューする。
- 承認コントロールが有効であり、十分な証拠が高い信頼性で記録されレビューされていることを確認するために、文書を閲覧し、プロセスに沿ってトランザクションを追跡し、可能な場合には、トランザクションを追跡するために、サンプルデータ、組み込み監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いる。
- 適時なエラーメッセージ、トランザクション・プロセス制限、エラーログが効果的に作成され、適用され、レビューされていることを確認するために、文書を検査し、プロセスに沿ってトランザクションを追跡し、可能な場合には、トランザクションを追跡するために、サンプルデータ、組みこみ監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いる。
- エラーと残高の不一致なデータの報告、エラー修正、その他の文書を検査して、エラーと残高の一致しない状況が効果的にレビューされ、修正・チェックされ、修正されるまで報告され続けることを確認する。

AC3 正確性、網羅性および真正性のチェック

コントロール目標	価値のドライバー	リスクのドライバー
トランザクションの正確性、網羅性、および妥当性を検証する。入力したデータを確認し、できるだけ作成された時点に近いところで編集する、または修正を求めるようにする。	・データ処理エラーの効率的な修復 ・処理の間、データの正確性、網羅性および実現性が維持される。 ・連続的なトランザクション処理 ・データの入力と処理の職務分離	・不完全であるか、無効であるか、もしくは不正確なデータ入力による、処理の非効率性および手戻り ・重要なデータのインテグリティの毀損 ・発見されないデータ入力のエラー ・承認されていないデータ入力

コントロール設計のテスト

・編集や妥当性チェックで摘出されたトランザクションを処理するためのポリシーと手続きが存在するか調査し確認する。
・トランザクションデータの入力や変更、承認に関する職務分離と、妥当性確認ルールのためのプロセスと手続きが確立されているか調査し確認する。職務分離ポリシーの評価の際に考慮すべき要素は、トランザクションシステムの重要性と、職務分離を実施する方法を含む。
・データ入力の際の妥当性確認の判断基準とパラメータを定期的にレビューし、確認し、適時、適切、かつ承認されたやり方で更新しているか調査し確認する。
・重要なシステムについては、データ入力の設計を検査して、承認コントロールによって、適切に承認された人だけがデータを入力または変更できることを確かめる。
・データ入力コントロールについての機能の説明と設計の情報を入手する。しかるべきコントロールの機能と設計を検査する。コントロールの例は、連番やリミット、範囲、妥当性、合理性、テーブル・ルックアップ、存在、キー検証、チェックディジット、網羅性（合計金額、項目数の合計、文書の合計、ハッシュトータル）、重複、論理関係チェック、タイムエディットの組込みを含む。
・データ入力承認コントロールについての機能の説明と設計の情報を入手する。承認チェックの存在について機能と設計を検査する。
・トランザクションデータの入力についての機能の説明と設計の情報を入手する。適時性と網羅性のチェックとエラーメッセージが存在するか、機能と設計を検査する。可能なら、トランザクションデータの入力を観察する。
・トランザクションデータの妥当性チェックについての機能の説明と設計の情報を入手する。

コントロール目標達成のテスト

- エラーと残高不一致データの報告、エラー修正、その他の文書を検査して、エラーと残高不一致の状況が効果的にレビューされ、修正され、チェックされ、修正されるまで報告され続けることを確認する。
- エラー修正、残高不一致の状況、入力の上書き、その他についての文書を検査し、手続きに従っていることを確認する。
- ソースドキュメントからソースデータの入力のサンプルを選び、検査、CAAT、その他の自動化された証拠収集と評価のツールを用いて、入力データが、ソースドキュメントを完全かつ正確に表したものであることを検証する。
- ソースデータの入力プロセスのサンプルを選び、ソースデータの入力プロセスが、適時性、網羅性、正確性についての定められた基準に沿って実施されていることを確実にするメカニズムが運用されているか調査し確認する。
- 編集と妥当性チェックのルーチンで摘出されたトランザクションが修復されるまで適切なフォローアップが行われるか調査し確認する。

AC4 処理のインテグリティと妥当性

コントロール目標	価値のドライバー	リスクのドライバー
処理サイクルを通じて、データのインテグリティと妥当性を維持する。 誤りのあるトランザクションが検出されても、有効なトランザクションの処理が中断されないようにする。	・ 処理のエラーが適時に発見される ・ 問題調査能力	・ エラーや不正の不十分な証拠 ・ データ入力エラーの見逃し ・ 承認されていないデータ処理

コントロール設計のテスト

・ 適切な承認が与えられた後でのみ、トランザクションの処理が行われるかを調査し確認する。
・ ツールとアプリケーションの文書をレビューして、それがその作業に適用でき、適合していることを確認する。重要なトランザクションの場合には、ソースコードをレビューして、ツールとアプリケーションのコントロールが設計通りに機能していることを確認する。代表的なサンプルを再処理して、自動化ツールが意図した通りに機能していることを確認する。
・ データ入力コントロールについての機能の説明と設計の情報を入手する。順序と重複のエラー、参照インテグリティのチェック、コントロール、ハッシュトータルのチェックが行われているか、機能と設計を検査する。検索ツールを用いて、エラーでないものがエラーとして識別されたケースや、エラーが発見されなかったケースがないかを識別する。
・ トランザクションデータ入力についての機能の記述と設計情報を検査して、編集と妥当性チェックのルーチンで摘出されたトランザクションが保留ファイルに送られるかどうか確かめる。保留ファイルが正しく一貫して作成されるかどうか確かめ、利用者がトランザクションが保留アカウントに送られたことを知らされていることを確かめる。トランザクションの処理が、データ入力やトランザクションの承認のエラーによって遅延しないことを確かめる。サンプルデータやベースケース（期待された結果を出すように準備されたトランザクション）、組みこみ監査モジュールないしCAATを含む、自動化された証拠収集ツールを用いて、トランザクションを追跡し、トランザクションが効果的に処理され、妥当なトランザクションが妥当でないトランザクションからの干渉を受けずに処理され、エラーのあるトランザクションが報告されることを確認する。
・ 保留アカウントと保留ファイルでのエラーのあるトランザクションの代表的なサンプルを分析し、妥当性チェックのルーチンで摘出されたトランザクションが、修復されるまでチェックされていることを確認する。・妥当性チェックルーチンで摘出されたトランザクションのための保留アカウントと保留ファイルが、最近のエラーのみを含んでいるかどうか確かめ、古いものが適切に修復されたことを確認する。
・ ジョブ・シーケンスがITオペレータに指示されているか調査し確認する。ジョブが、ジョブスケジューリングシステムに十分な指示を出し、データが処理中に不適切に追加されたり変更されたり失われたりしないようになっているか調査し確認する。ソースドキュメントを検査して、プロセスに沿ってトランザクションを追跡し、可能な場合には、サンプルデータ、組みこみ監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、トランザクションを追跡し、本番のジョブスケジューリング・ソフトウェアが効果的に用いられており、ジョブが正しいシーケンスで実行され、システムに十分な指示を与えていることを確認する。
・ それぞれのトランザクションに一意の連番や識別子（インデックスや日付、時間）が割り当てられているか調査し確認する。文書を検査し、プロセスに沿ってトランザクションを追跡し、可能な場合には、サンプルデータや組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、トランザクションを追跡し、一意のIDが付与されているトランザクションが重複しておらず、連番を要するようなデータに番号の抜けが存在しないことを確かめる。

コントロール設計のテスト（続き）

- 処理されたトランザクションの監査証跡が維持されているか調査し確認する。監査証跡やその他の文書を検査し、監査証跡が効果的に設計されていることを確認する。サンプルデータや組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、トランザクションを追跡し、監査証跡が効果的に維持されていることを確認する。変更前後のデータイメージが維持され、適切な担当者によって定期的にレビューされていることを確認する。
- トランザクションの監査証跡が維持され、通常とは異なる活動がないかどうか定期的にレビューされているか調査し確かめる。データ入力を行わない監督者がレビューを行っていることを確かめる。監査証跡、トランザクション（またはバッチ）、レビュー、およびその他の文書を検査し、プロセスに沿ってトランザクションを追跡し、可能な場合には、サンプルデータや組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、監査証跡を定期的にレビューして維持することにより、通常とは異なる活動が効果的に発見され、監督者のレビューが、修正や上書き、値の大きいトランザクションの妥当性を適時に検証する上で効果的であることを確かめる。
- 適切なツールの使用と、閾値の調整がセキュリティ要件を遵守しているか調査し確認する。監督者が定期的にシステムの出力と閾値をレビューしているか調査し確認する。サンプルデータや組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、トランザクションを追跡し、ツールが設計通りに機能していることを確認する。
- データ処理に計画外の中断が起きた時に、可能な場合には、データのインテグリティを自動的に維持するためのユーティリティが用いられているか調査し確認する。監査証跡とその他の文書、計画、ポリシー、手続きを検査し、システムの能力が、データのインテグリティを自動的に維持するのに効果的に設計されていることを確認する。データのインテグリティの問題に関する実際の中断の記録をレビューして、適切なツールが効果的に用いられていることを確かめる。
- 修正や上書き、値の大きいトランザクションが、データ入力を行わない監督者により、その適切性について迅速かつ詳細にレビューされているか調査し確認する。監査証跡、その他の文書、計画、ポリシー、手続きを検査し、修正や上書き、値の大きいトランザクションが、詳細にわたって迅速にレビューされるよう効果的に設計されていることを確認する。監査証跡、トランザクション（またはバッチ）、レビュー、およびその他の文書を検査し、プロセスに沿ってトランザクションを追跡し、可能な場合には、サンプルデータ、組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いて、監督者のレビューが、修正や上書き、値の大きいトランザクションの妥当性を適時に検証する上で効果的であることを確かめる。
- ファイルの合計の調整がルーチンベースで実施され、残高の不一致が報告されているか調査し確認する。突合とその他の文書を検査して、プロセスに沿ってトランザクションを追跡し、調整ファイルの合計がマッチするか、あるいは残高が不一致な場合について、しかるべき担当者に報告されているかが、調整によって効果的に判定されていることを確認する。

コントロール目標達成のテスト

- アプリケーションのサンプルについて、職務分離が実施されているか調査し確認する。トランザクションデータの入力、変更、承認および妥当性確認ルールについて、職務分離が導入されているか確かめる。
- 重要なトランザクション・プロセスのサンプルについて、アクセスコントロールによって承認を受けていないデータ入力を防止できるかどうかテストする。検索ツールを用いて、承認されていな要員がデータを入力したり改変したりできるようなケースを識別する。
- トランザクションシステムのサンプルについて、編集と妥当性確認ルーチンで摘出された保留アカウントと保留ファイルが最近のエラーのみを含んでいるかどうか確かめる。摘出されたトランザクションのうち古いものが適切に修復されたことを確認する。
- トランザクションのサンプルについて、データ入力がエラーのトランザクションによって遅延しないことを確認する。
- 高度に重要なトランザクションについて、本番システムと同様に動作するテスト・システムを立ち上げる。異なるタイプのエラーを入力する。
- エラーの発見と報告の適時性と完全性を確かめ、トランザクションを修正するのに十分な情報を提供しているかどうか確かめる。
- 高度に重要なトランザクションについて、本番システムと同様に動作するテスト・システムを立ち上げる。テスト・システムでトランザクションを処理して、有効なトランザクションが適切かつ適時に処理されることを確認する。
- エラーが適切かつ適時に報告されることを確認する。
- データ入力やオンライン処理の際のエラーメッセージを検査する。
- エラーメッセージがトランザクションの流れにふさわしいことを確認する。メッセージの適切な属性の例は、理解しやすさ、即時性、可視性を含む。
- 編集と妥当性確認のルーチンで摘出されたトランザクションが保留ファイルに送られるかどうかを判定する。
- 保留ファイルが一貫して正しく作成されるかどうか確かめる。
- ユーザが保留アカウントに送られたトランザクションについて連絡されているかを確認する。
- データ入力トランザクションのサンプルを取る。適切な自動化された分析・検索ツールを用いて、エラーでないものがエラーとして識別されたケースや、エラーが発見されなかったケースを識別する。
- サンプルデータや組み込み監査モジュールないしCAATを含む自動化された証拠収集ツールを用いてトランザクションが中断なしに処理されていることを確認する。エラーのトランザクションが適時なやり方で報告されているか調査し確認する。

AC5 出力のレビュー、調整、およびエラー処理

コントロール目標	価値のドライバー	リスクのドライバー
出力は、許可された方法によって扱われ、適切な受領者に送付され、送信中に保護されるように、手続とこれに伴う責任を定める。 出力の正確性について検証、検出、修正を行い、また、出力から得られる情報を利用できるように、手続とこれに伴う責任を定める。	・機密性の高いデータ出力の保護 ・完全でエラーのない処理結果の正しい受け手への送付 ・エラー発見の適時性	・機密性の高いトランザクションデータの間違った受け手への送付 ・データの機密性の毀損 ・非効率なトランザクション処理 ・トランザクションデータ出力のエラーの見逃し

コントロール設計のテスト

・設計基準をレビューして、ヘッダやトレラーの記録でコントロール・トータルを用いたり、出力をシステムが作成したコントロール・トータルと照合したりするといったような、インテグリティベースのコントロールプロセスを要求していることを確かめる。
・発見された残高不一致の状況が報告され、報告がシステムの設計に組み込まれ、適切なレベルの管理者に確実に報告する手続きが作られているかを調査し確認する。
・残高不一致やその他の異常に対し、迅速な調査と報告を要求する手続きがあるかを調査し確認する。
・文書をレビューして、機密性の高い主要な文書の保管について定期的に調査し、差異があれば調査する手続きが定められているかを確かめる。
・アプリケーションの出力が、エンドユーザの処理での利用を含むその後の処理で用いられるのに先立って、アプリケーションの出力の網羅性と正確性を確実に検証するための手続きが設計されているか調査し確認する。
・出力データが、利用に先立って、プロセスオーナーによって決められた合理性、正確性、その他の基準に基づいて確実にレビューするための手続きが作成されているかどうか調査し確認する。
・報告を配布する前に、潜在的なエラーのログを取り、その解決策を要求する手続きが定められているか評価する。

コントロール目標達成のテスト

- コントロール・トータルが、出力のヘッダないしフッタの記録に適切に表示され、それがシステムによって作成されたコントロール・トータルと照合されているか調査し確認する。
- 発見された残高不一致の状況が、適切なレベルの管理者に報告されているか調査し確認する。残高不一致のレポートを検査する。可能な場合には、自動化された証拠収集ツールを用いて、コントロール・トータルのエラーを探し、それに対して正しく適時な方法で対処していることを確かめる。
- 機密性の高い出力については、適切な期間ごとに実地棚卸をしているか調査し確認する。それが在庫記録と比較され、その差異に対処していることを確かめる。機密性の高い出力に関するアクセスの例外と拒否の監査証跡がアカウント毎に作成されているか確かめる。もし可能なら自動化された証拠収集ツールを用いて監査証跡の代表的なサンプルを調査して、例外を識別し、それが発見され、それに対処したかを確かめる。実地棚卸のサンプルを取り、それを関連する監査証跡と比較し、発見が有効に機能していることを確かめる。
- エンドユーザアプリケーションで再利用される電子的な出力のすべての一覧を入手する。電子的な出力が再利用され再処理される前に、その網羅性と正確性がテストされていることを確かめる。電子的な出力の代表的なサンプルを選び、プロセスに沿って選択した文書を追跡し、他の業務を実施する前に網羅性と正確性が検証されていることを確かめる。網羅性と正確性のテストを再実施して、それが有効であることを検証する。
- 出力の合理性と正確性がレビューされているか調査し確認する。出力レポートの代表的なサンプルを選び、その出力の合理性と正確性をテストする。潜在的なエラーが報告され、集中的に記録が取られていることを確かめる。代表的なトランザクションのサンプルを選び、エラーが識別されタイムリーな方法で対処されていることを確かめる。エラーログを閲覧して、エラーがタイムリーな方法で効果的に対処されていることを確かめる。
- 機密性の高い情報が定められ、プロセスオーナーによって合意され、適切に扱われているか調査しを確認する。これは、機密性の高いアプリケーションの出力にラベルをつけ、必要な場合には、機密性の高い出力を、アクセスコントロールされた特別な出力デバイスに送ることを含む。機密性の高いデータのサンプルについて、出力ファイルを探し、それに適切にラベルがつけられていることを確かめる。機密性の高い情報を配布する方法と、機密性の高い出力デバイスに対するアクセスコントロールメカニズムをレビューする。そのメカニズムが、事前に確立されたアクセス権を正しく実施していることを確かめる。

AC6 トランザクションの認証とインテグリティ

コントロール目標	価値のドライバー	リスクのドライバー
内部アプリケーションとビジネス機能／運用上の機能（企業の内外を問わず）の間でトランザクションデータをやり取りする前に、宛名が正しいかどうか、送信元の真正性、および内容のインテグリティをチェックする。送信または移送の間の真正性とインテグリティを維持する。	・ストレート・スルー・プロセッシング ・トランザクションの妥当性と真正性に対する信頼 ・エラーと不正の防止	・間違いや未承認のトランザクション ・トランザクションエラーの見逃し ・非効率性と手戻り

コントロール設計のテスト

- 重要なトランザクションについて、通信とトランザクション提示の標準や責任、認証、セキュリティ要件を含めて、取引先との間で適切な合意が確実になされるようにプロセスが設計されているか調査し確認する。
- 安全な標準や個別に認証を取得した製品を採用するといったように、インテグリティや真正性、否認防止のための適切なメカニズムを取り込むようにシステムが設計されているか調査し確認する。
- 認証された情報を識別するために業界標準の出力タグを取り込むようにシステムが設計されているか調査し確認する。
- 重要なアプリケーションのマニュアルと文書を検査し、設計仕様上、真正性のために入力を適切に認証することが要求されているか確かめる。
- 他の処理アプリケーションから受け取ったトランザクションを識別し、その情報を分析して、その情報が正しい発信元からで、伝送中の内容のインテグリティの維持を分析するようにシステムが設計されているか調査し確認する。
- 重要なトランザクションについて、取引先と交わした合意を入手して検査し、その合意内容として、伝送とトランザクション形式の標準や責任、認証、セキュリティの要件についての要求事項を定めていることを確かめる。
- 重要なトランザクションに関する取引先との合意のサンプルを選び、それが完全であることを確かめる。
- 認証の失敗のサンプルを選び、取引先との合意が有効に機能していることを確かめる。
- 文書のレビューとウォークスルーを実施し、トランザクションの真正性やインテグリティ、否認拒否に関する重要なアプリケーションを識別する。このようなアプリケーションについて、インテグリティや真正性、否認拒否に関する適切なメカニズム（安全な標準や個別に認証を取得した製品）を採用しているかどうか調査し確認する。
- 重要なアプリケーションについてアプリケーションマニュアルと文書を検査して、出力に認証情報を適切に付与することが、その仕様と設計に記述されているか確かめる。
- サンプルのアプリケーションに対しソースコードのウォークスルーを行い、この仕様と設計が適用されていることを確かめる。このような仕様がテストされ良好な結果が得られていることを確かめる。
- トランザクションの代表的なサンプルを選び、真正性とインテグリティの情報が処理のサイクルに沿って正しく送られていることを確かめる。
- 認証に失敗したトランザクションのエラーログをレビューして、その原因を確かめる。

コントロール目標達成のテスト

- サンプルのアプリケーションのソースコードに対するウォークスルーを行い、真正性に関する仕様が適用されていることを確かめる。このような仕様がテストされ良好な結果が得られていることを確かめる。
- 認証に失敗したトランザクションのエラーログをレビューして、その原因を確かめる。

付録Ⅶ—内部統制の成熟度モデル

付録Ⅶ—内部統制の成熟度モデル

この付録では、企業内での内部統制環境の状況と、内部統制の確立状況を示す汎用的な成熟度モデルについて説明する。この成熟度モデルは、内部統制の管理と、より優れた内部統制を確立する必要性の認識を、その場対応レベルから最適化レベルへ発展させる過程を示す。この成熟度モデルは、COBITのユーザがITにおける効果的な内部統制の実現に必要な要件を正しく認識し、自社の成熟度を判断する上で役立つ概略的な指針となる。

成熟度	内部統制環境の状況	内部統制の確立
0 不在	内部統制の必要性が認識されていない。企業文化または使命にコントロールが組み込まれていない。コントロールの不履行やインシデントが発生するリスクが高い。	内部統制の必要性を評価する意志がない。インシデントが発生した時点で、その都度対応している。
1 初期／その場対応	内部統制の必要性がある程度認識されている。リスク要件およびコントロール要件に対処するアプローチは場当たり的で一貫性がなく、周知やモニタリングが実施されていない。何らかの不履行があっても特定されない。従業員が各自の実行責任を認識していない。	IT コントロールに関する要件について、評価の必要性が認識されていない。評価が実施されたとしても、場当たり的かつ表面的なものであり、重大なインシデントに対応する形でのみ行われる。実際に発生したインシデントのみが評価の対象となる。
2 再現性はあるが直感的	コントロールが実施されているが、文書化されていない。運用は個々の担当者の知識と意欲に依存している。有効性が適切に評価されていない。コントロールに多くの不備があり、これらの不備への対応が適切に実施されておらず、重大な問題が生じる可能性がある。マネジメント層によるコントロールに関する問題の解決措置は後回しにされる傾向があり、継続的に実施されていない。従業員が各自の実行責任を認識していない可能性がある。	コントロールの必要性に関する評価は、選定された IT プロセスにおいて、現在のコントロールの成熟度、達成すべき成熟度レベル、およびその間の差異の判別が必要な場合のみ実施される。プロセスに関与しているチームや IT 管理者を対象にした非公式のワークショップが実施されている。このワークショップにおいて、プロセスのコントロールに対する適切なアプローチが定義され、合意された実行計画の実施に向けた動機付けが行われている。
3 定められたプロセスがある	コントロールが実施され、適切に文書化されている。運用の有効性が定期的に評価され、発見される問題は標準的な数である。ただし、評価プロセスは文書化されていない。マネジメント層は、ほとんどのコントロールに関する問題を事前に予測して対処できるが、コントロールにおける不備は残っており、依然として重大な問題が生じる可能性がある。従業員はコントロールに関する各自の実行責任を認識している。	価値要因とリスク要因に基づいて重要な IT プロセスが特定されている。詳細な分析が実施され、コントロール要件および逸脱の根本原因が特定され、改善の機会が設けられている。ワークショップの活用に加え、ツールの使用とインタビューの実施により分析が強化され、IT プロセスオーナが評価と改善のプロセスを確実に実施、促進している。
4 管理され、測定が可能である	効果的な内部統制およびリスクマネジメント環境がある。文書化された正式なコントロール評価が頻繁に実施されている。多くのコントロールは自動化されており、定期的なレビューの対象になっている。マネジメント層は、コントロールに関する問題をほとんど発見できるが、すべての問題が常に特定されるわけではない。特定されたコントロール上の不備に対応するため、一貫したフォローアップが行われている。コントロールの自動化に、限定的ではあるが戦術的に技術が使用されている。	関連するビジネスプロセスオーナの全面的な協力と同意を得て、IT プロセスの重要性が定期的に定義されている。主要な利害関係者が関与する詳細かつ正確な分析の実施後に、これらのプロセスの実際の成熟度とポリシーに基づいて、コントロール要件の評価が実施されている。評価の説明責任が明確に定められ、割り当てられている。改善戦略が投資対効果検討書によって裏付けられている。期待される結果を達成する過程における成果が、一貫してモニタリングされている。コントロールの社外レビューが時折行われている。
5 最適化	全社的なリスクおよびコントロールのプログラムが策定されており、コントロールとリスクの問題が継続的かつ効果的に解決されるようになっている。内部統制とリスクマネジメントは企業の活動指針に組み込まれており、コントロールのモニタリング、リスクマネジメント、および法令遵守の徹底に関して全面的な説明責任を負う、自動化された常時モニタリングシステムにより支援されている。セルフ評価、および差異分析と根本原因分析に基づいてコントロールが継続的に評価されている。従業員はコントロールの改善に積極的に関与している。	事業上の変更を行う際は、IT プロセスの重要性が考慮され、プロセスコントロール能力の再評価の必要性があれば、それが必ず実施される。IT プロセスオーナは、セルフ評価の定期的な実施により、コントロールの成熟度が適切なレベルにあり、事業上の必要性が満たされていることを確認している。また、IT プロセスオーナは、成熟度の特性を検討し、コントロールの効果と効率を向上させる努力をしている。組織は外部のベストプラクティスと比較したベンチマーキングを実施し、内部統制の有効性について外部からの助言を求めている。重要なプロセスについて独立したレビューが実施され、コントロールが望ましい成熟度レベルにあり、計画どおりに機能していることが確認されている。

付録Ⅷ—ITでの対象範囲の決定

付録Ⅷ—ITでの対象範囲の決定

1. イニシアティブを定義する

イニシアティブの目的、ビジネスでの目標、予想される収益の価値を定義する。イニシアティブが対象とし、影響を受ける企業の領域を文書化する。成功要因、法令遵守の要件、潜在的なリスク、プロジェクト完了基準を列挙する。このようなプロジェクトのドライバーに対する変更と結果をどのように扱うかを確立する。

ステップ	活動	成果物
ステップ1.1 **目標を定義する。** イニシアティブの主要な目標と達成目標を識別する。価値ある提案を作成し、その目標が企業の達成目標をいかに支援し促進するかを示す。	・プロジェクトに着手する理由とその目的を識別し、経営者と共にレビューする。 ・主要な課題と懸念事項を調査して文書化する。 ・先行している同様のプロジェクトから学ぶ。 ・関連する文書を識別し入手する。 ・イニシアティブで期待されている結果と成果物を識別する（高レベルで）。 ・市場勢力図を識別する。	・ビジネスで的な価値を文書化したもの ・ITイニシアティブの目的を文書化したもの ・期待されている結果を文書化したもの
ステップ1.2 **境界を定義する。** ITプロジェクトとその境界、すなわち何が含まれており、何が含まれていないのかを定義する。そこに含まれている組織単位、ビジネスの活動とプロセスと、プロジェクトの対象範囲から除外されているものとを識別する。	・プロジェクトの対象範囲に含める主要な活動、ビジネスユニット、企業の組織・部門、業務等を識別する。 ・通常はこのようなプロジェクトの対象範囲に含まれるが、今回は対象範囲から除外するような項目を識別し文書化する。 ・持分法適用会社、外国の司法権適用範囲、対象外とした項目といった対象範囲の課題を識別する。 ・入手した結果が、目標と期待されている成果物に確実に合致するように、対象範囲が十分であることを確かめる。 ・確実な協力が得られるように、影響を受ける企業との連携を確立する。	・ITイニシアティブの対象範囲を文書化したもの ・境界に関する課題とその扱いについてを文書化したもの ・境界について、主要な利害関係者に伝える。
ステップ1.3 **標準を定義する。** イニシアティブが遵守する必要のある標準、参照フレームワーク、ポリシー、ないし契約を識別する。標準は、業界での要請事項、規制による基準、および企業のポリシーを含む可能性がある。測定のための指標を識別し、標準の遵守のための主要な成功要因を確立する。	・企業とプロジェクトが遵守すべき契約、法律、規制、業界、その他の標準を識別する。 ・プロジェクト/イニシアティブが考慮すべき基準やフレームワークを識別する。 ・標準の遵守を可能にするための成功要因と、その証拠となる主要な測定指標を文書化する。	・プロジェクトを開始する際に用いる文書化された標準 ・プロジェクトの結果を評価する際の主要な成功要因と測定指標を文書化したもの

ステップ	活動	成果物
ステップ1.4 **リスクを定義する。** プロジェクトリスクやビジネスリスクを含む、プロジェクトに関連するリスクを識別して評価する。リスク評価とリスク低減の程度は、プロジェクトの規模、もたらされる価値、および影響に依存する。	・イニシアティブが目標達成に失敗したり遅れたりする潜在的な理由を識別する。 ・このイニシアティブが企業の他の目標に与える悪影響だけでなく、業務の目的を脅かすであろう重要なシナリオも識別する。 ・リスクの重要度と発生可能性を識別する。 ・リスクを管理し低減するための計画を作成する。	・文書化されたITイニシアティブのリスク評価 ・リスク低減計画（必要に応じて）と推定費用
ステップ1.5 **変更プロセスを定義する。** プロジェクトへの変更を起こしうる内的要因と外的要因を識別し、プロジェクトの目標、対象範囲、リスク、成功要因に対してどのように変更を加えるかを定義する。	・プロジェクトへの変更をもたらしうる内的要因と外的要因を識別して分析する。 ・ドライバーと結果に対する変更を承認、採択、伝達するためのプロセスと手続きを定義して文書化する。 ・変更プロセスを管理するのに適切なツールと技法を識別する。	・変更プロセスの記述 ・ツールと技法の利用法を含む、変更管理ガイダンス
ステップ1.6 **成功を定義する。** プロジェクトを完了させるのに要するアクティビティ、タスク、成果物を含め、プロジェクトが完了のための条件を識別する。イニシアティブの退出規準（目標を達成したかどうかを決定するための条件）を定義する。	・プロジェクト完了承認後のアクティビティを識別する。 ・プロジェクトの成果物がプロジェクトオーナおよびプロジェクトが作成する継続的なアクティビティに対して責任を持つ人に、提示され受け入れられたということを示すのに必要な証拠を識別する。	・プロジェクトが成功裏に完了したことを示すのに要する証拠（測定指標、品質基準等） ・完了後のアクティビティが識別されしかるべき組織単位に提示された証拠
ステップ1.7 **資源を定義する。** 人員、技術、予算、技能を含む、イニシアティブを成功裏に完了させるのに要する資源を識別する。	・イニシフティブの目的を達成するのに必要な資源の数とレベル（技能）を定義する。 ・イニシフティブをサポートするために必要な技術と設備を評価する。	・資源モデル ・資源と費用の計画
ステップ1.8 **成果物を定義する。** イニシアティブの期間に作成される成果物を定義する。	・イニシアティブから生じる外部の成果物を識別する。 ・成果物の具体的なサンプルを作成する。	・プロジェクト成果物の一覧 ・選択された成果物のサンプル

2. イニチアチブ（プロジェクト）の計画を立てる。

成果物を詳細に定義する。それに基づいて、成果物を作成するのに要する資源、サポート、説明責任を識別する。イニシアティブを開始できるように、承認を得て、イニシアティブ内での優先順位を決めて、資源を有効化し、伝達計画を作成する。

ステップ	活動	成果物
ステップ2.1 **経営陣のサポートを得る。** イニシアティブにとって適切なプロジェクトスポンサーを識別し、面会する。	・潜在的なスポンサーがプロジェクトに適合しているかどうかを決定する。 ・要件を満たすような潜在的なスポンサーがいるかどうかを評価する。 ・プロジェクトの目的と利益に基づいて、経営者向けのプレゼンテーションマテリアルを作成する。	・イニチアチブのスポンサー/オーナー ・完全なプロジェクト文書と規定

ステップ	活動	成果物
ステップ2.2 **資源の要件を最終決定する。** 資源モデルで定義された必要な予算と資源を獲得する。	・予定した資源モデルと費用計画をレビューする。 ・詳細な調達スケジュールを作成する。 ・資源の消費/利用と予算の要件を含む、カレンダーベースの詳細なプロジェクト予算を作成する。	・更新された資源モデル ・詳細な資源調達スケジュール ・詳細なプロジェクト予算
ステップ2.3 **イニシアティブの組織を定義する。** イニシアティブを成功させるのに必要な組織構造を定義し、実際に組織する。これは、リーダーシップ、人員、主要なスポンサー等を含み、プロジェクトマネジメントオフィスを含むこともある。	・役割と責任を文書化する。 ・リーダーシップに対する期待事項を定義する。 ・組織構造を作成し確立する。 ・最初に組織に主要な人員を配置する。 ・職務記述、役割、責任を作成する。	・組織モデル ・報告権限 ・役割と責任
ステップ2.4 **スケジュールを定義する。** イニシアティブについて予定した資源と成果物を与件として、記述されている達成目標と目標に合致するために、イニシアティブを完了させるための具体的なスケジュールを定義する。主要なマイルストーンを含め、クリティカルパスを識別する。	・達成目標と目標および期待された資源モデルをレビューする。 ・そのレビューをもとに、成果物のための主要なマイルストーンと、イニシアティブの主要なチェックポイントを、プロジェクトのスポンサーと共に定義する。 ・高レベルのスケジュール表を作成し、潜在的なクリティカルパスとアクティビティの相互依存関係を識別する。 ・サブプロジェクトの主要なフェーズのそれぞれについて、クリティカルパスとスラックパスの分析、スキル要件、資源計画を含む、ガントチャートを作成する。 ・スケジュールが、ビジネスサイクル内の重要な外部への報告、資金調達、その他の期限に合致することを確かめる。 ・プロジェクト内および主要な外部の利害関係者、および影響を受ける人員に対する継続的な状況報告のやり方を定義する。	・資源計画の情報に統合された文書化されたスケジュール ・以下を含む、プロジェクトスケジュールの文書 – アクティビティとタスク – アクティビティの相互依存関係 – 主要なマイルストーンの日付 – 主要なプロジェクトチェックポイント – 主要な成果物提供の日付 – 状況および報告の日付 – ビジネスアクティビティ、その他主要な日付 ・伝達に関して定義した文書
ステップ2.5 **アプローチと方法論を定義する。** プロジェクトがその目標に合致することができるように、利用する方法論を決定し、フェーズ、サブフェーズ、アクティビティ、タスクを完全に備えた詳細計画を作成する。	・目標、アクティビティ、成果物を伴うプロジェクトのフェーズとサブフェーズを作成する。 ・利用するアプローチと方法論および入手する情報を決定する。 ・それぞれのフェーズ、サブフェーズ、アクティビティについて詳細な作業計画を作成する。	・詳細なプロジェクト計画
ステップ2.6 **伝達計画を作成する。** イニシアティブのライフサイクルを通じて、イニシアティブについての情報を伝達し、期待事項を管理し、イニシアティブの目標をサポートするための計画を設計する。主要なマイルストーンと異なる聴衆とを考慮する。	・プロジェクトの状況、資源計画、費用（必要に応じて）を連絡する。 ・リスク管理計画の状況を伝達する。 ・プロジェクトの達成目標と目標への変更を連絡する。 ・プロジェクトの進捗を伝達する。	・スケジュールと主要なマイルストーンを含む、伝達計画の文書

付録Ⅸ—COBITと関連する製品

付録Ⅸ—COBITと関連する製品

COBITフレームワーク（4.0版以降）には、次の製品がすべて含まれる。
- フレームワーク – COBITにおいて、ITガバナンス管理、コントロール目標、および優れた実践方法（手法）が、ITドメインごとおよびプロセスごとにどのように編成され、ビジネス要件と対応付けられるか説明する。
- プロセスの説明 – ITの実行責任に伴う領域に全面的に対応した34のITプロセスについて説明する。
- コントロール目標 – すべてのITプロセスについて、管理目標に関する一般的なベストプラクティスを規定する。
- マネジメントガイドライン – 責任の割り当て、成果の測定、およびベンチマーク評価と能力とのギャップの解消を支援するツールを提供する。
- 成熟度モデル – ITプロセスの現状と将来見込まれる状態を記述したプロファイルを提供する。

COBITでは設立以来、コアコンテンツが進化を続け、COBITから派生する成果物が増加している。現在、COBITからは次の資料が発行されている。
- 取締役会のためのITガバナンスの手引き 第2版 — ITガバナンスの重要性、ITガバナンスの課題、およびその管理に対する経営者の責任の理解を支援するように編纂されている。
- COBIT Online（COBITオンライン） — ユーザ自身の組織に向けてCOBITのバージョンをカスタマイズし、必要に応じて当該バージョンを保存、操作することができる。オンラインによるリアルタイム調査、FAQ（よくある質問）、ベンチマーキング、経験と質問を共有するための会議室が提供される。
- COBIT Control Practices（COBITコントロールプラクティス）:Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition（効果的なITガイダンスに向けたコントロール目標を達成するためのガイダンス 第2版） — 回避すべきリスク、およびコントロール目標の実施から得られる価値に関するガイダンス、ならびに目標の実施方法に関する説明を提供する。IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition（ITガバナンス導入ガイド:COBITとVal ITの使用 第2版）と併せて読まれることを強くお勧めする。
- IT Assurance Guide: Using COBIT — COBITをどのように利用して多様なIT統制の保証に関するアクティビティをサポートするかに関するガイダンス、およびあらゆるCOBIT ITプロセスやコントロール目標のために推奨されるテストのステップを提供する。COBIT 4.1のコントロール目標に照らした監査とセルフ評価について『Audit Guidelines（監査ガイドライン）』に記載する情報を置き換える。
- IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition（サーベインズオクスリー法（企業改革法）遵守のためのIT統制目標） — COBITコントロール目標に基づいてIT環境のコンプライアンスを保証する方法についてガイダンスを提供する。
- IT Governance Implementation Guide: Using COBIT and Val IT, 2nd Edition（ITガバナンス導入ガイド:COBITとVal ITの使用 第2版） —COBIT、Val ITリソース、およびこれを支援するツールキットを利用して、ITガバナンスを導入するための一般的なロードマップを提供する。
- COBIT Quick start — 小規模組織向けおよび大企業の導入初期向けのコントロール基準を提供する。

現時点で第2版の作成が進められている。
- COBIT Security Baseline — 企業内で情報セキュリティを導入するための必須のステップに焦点を当てる。本書を執筆している時点で、第2版が作成の最終段階にある。
- COBIT マッピング — 現在、www.isaca.org/downloadsで公開されている。
  - *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*
  - *COBIT Mapping: Overview of International IT Guidance, 2nd Edition*
  - *COBIT Mapping: Mapping of CMMI® for Development V1.2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT Mapping: Mapping of ISO/IEC 17799:2005 With COBIT 4.0*
  - *COBIT Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT Mapping: Mapping of PMBOK With COBIT 4.0*

  - *COBIT Mapping: Mapping of PRINCE2 With COBIT 4.0*
  - *COBIT Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
- Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition (情報セキュリティガバナンス: 取締役会および経営幹部に向けたガイダンス 第2版) – 情報セキュリティについてビジネス用語で解説し、セキュリティに関連する問題の解決に向けて利用できるツールや手法を紹介する。

Val ITは、Val ITフレームワークに関連する発行物をはじめ、追加的な製品やアクティビティを表す包括的な用語である。
現在、Val ITに関する次の資料が発行されている。

- Enterprise Value: Governance of IT Investments ー The Val IT Framework(IT投資の企業価値ガバナンス Val ITフレームワーク)、企業がIT関連の投資からどのように最適な価値を引き出すかについて、COBITフレームワークを基準として説明する。次の2部から構成される。
  - 価値ガバナンス、ポートフォリオ管理、投資管理からなる3つのプロセス
  - 重要なIT管理施策 ー 期待される成果、あるいは特定のアクティビティに伴う目標を達成する上で効果的な影響をもたらす重要なマネジメントプラクティス。Val ITプロセスをサポートすると同時に、COBITのコントロール目標とほぼ同様の役割を果たす。
- Enterprise Value: Governance of IT Investments ー The Business Case(IT投資の企業価値ガバナンス ビジネスケース)、投資管理プロセスに伴う特定の主要要素に焦点を当てる。
- Enterprise Value: Governance of IT Investments—The ING Case Study, グローバルな金融機関がVal ITのフレームワークを使ってIT投資のポートフォリオを管理したかのケーススタディ

COBIT、Val ITと関連資料、ケーススタディ、教育コース、ニュースレター及び他のフレームワークの、最新の全ての資料については、次のURLを参照されたい。

www.isaca.org/cobit
www.isaca.org/valit