



ISMSロゴマークは、情報セキュリティは人によって守られることをイメージしています。

ISMSに関する情報(JIPDEC)
<http://www.isms.jipdec.jp/>



財団法人 日本情報処理開発協会

〒105-0011 東京都港区芝公園3丁目5番8号 機械振興会館内
TEL 03-3432-9386 FAX 03-3432-6200
URL <http://www.jipdec.jp/>



ISMS **JIPDEC**

情報セキュリティマネジメントシステム
適合性評価制度の概要

財団法人 日本情報処理開発協会

1

ISMS適合性評価制度の目的

情報セキュリティマネジメントシステム(Information Security Management System:以下ISMSという)適合性評価制度は、国際的に整合性のとれた情報セキュリティマネジメントに対する第三者適合性評価制度である。本制度は、わが国の情報セキュリティ全体の向上に貢献するとともに、諸外国からも信頼を得られる情報セキュリティレベルを達成することを目的としたものである。

2

ISMS認証取得の必要性

インターネットの急速な普及を背景に、わが国においても、電子政府実現に関連する法規の整備、技術的な検証、情報通信インフラの整備等を積極的に推進しており、今後は電子申請など国と民間の電子的なやり取りも急速に進展する見込みである。しかしながらネットワーク社会の進展や、パソコンや情報通信システムの普及は、利用者に大きな利便性をもたらす一方で、コンピュータウイルス・不正アクセス行為やシステムダウンによる業務中断、故意や不注意による情報漏洩など、さまざまなセキュリティ事件・事故の新たな脅威を生んでいる。また自社のみならず、取引先や顧客も含めて被害が急速に拡大する傾向にある。このようなことから、以下のメリットを期待し、ISMS認証を取得する組織が増えている。

ISMSを構築・運用するメリット

- 技術面及び人間系の運用・管理面の総合的なセキュリティ対策が実現できる。
社員のスキル向上、責任の明確化、緊急事態の対処能力の向上など。
- 総合的なマネジメントの視点から、効率的なセキュリティ対策が実施できる。
費用対効果を考えて資産管理、リスクマネジメントの定着など。
上記の活動を継続することにより、セキュリティ意識の向上などの効果が期待される。

ISMS認証を取得するメリット

- 対外的には、情報セキュリティの信頼性を確保できる。
顧客や取引先からのセキュリティに関する要求事項の満足など。
- 内部的には、事業競争力の強化につながる。
入札条件や電子商取引への参加の条件整備など。
特定システムオペレーション企業等認定制度での申請時における必要条件となっている。

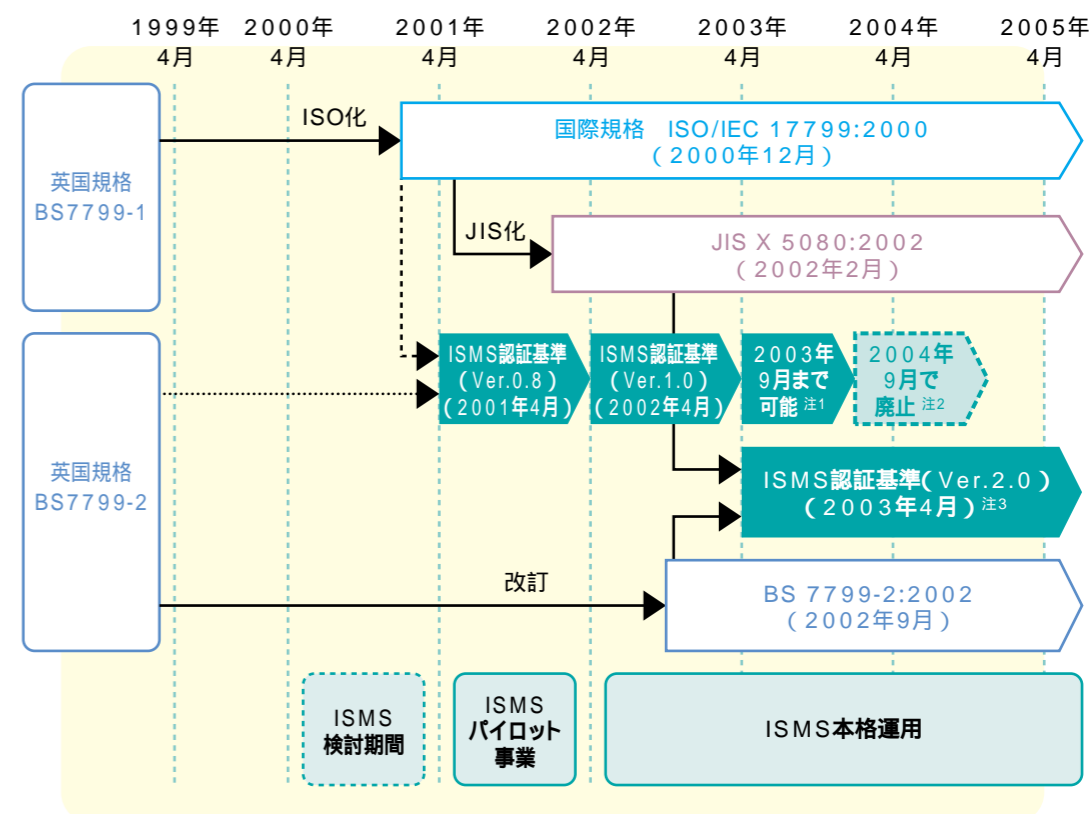
3

ISMS認証基準

ISMS認証基準(Ver.2.0)は、ISMS適合性評価制度において、第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための認証基準である。本基準は、英国規格BS 7799-2:2002に基づき作成したもので、本基準で使用する用語、表現については、JIS X 5080:2002(国際規格ISO/IEC 17799:2000)との互換性を確保した。

- BS 7799-2:2002(Information security management systems - Specification with guidance for use:情報セキュリティマネジメントシステム 仕様及び利用の手引)は、BS 7799の認証を取得するための英国規格である。
- JIS X 5080:2002(ISO/IEC 17799:2000(Information technology - Code of practice for information security management:情報技術 情報セキュリティマネジメントの実践のための規範)は、組織の情報セキュリティに責任を持つ人々に向けた効果的なISMSを実施するための規範(ベストプラクティス-最良の慣行)をまとめた国内規格である。

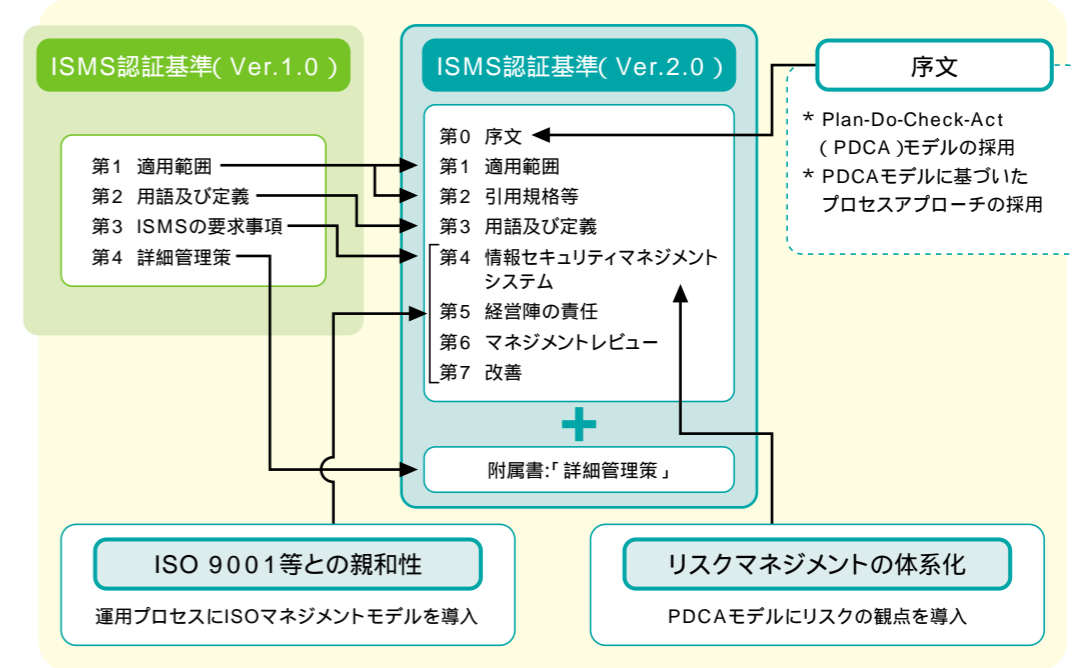
ISMS認証基準制定の経緯



注1:Ver.1.0による初回審査は2003年9月30日まで可能。 注2:Ver.1.0は、2004年9月30日で廃止。
注3:ISMS認証基準(Ver.2.0)は、英国規格 BS 7799-2:2002をベースとし、用語、表現についてはJIS X 5080:2002との互換性を確保。

ISMS認証基準(Ver.2.0)の特徴

- マネジメントプロセスを導入することで、ISMS運用プロセスが体系化された。
- JIS Q 9001:2000(ISO 9001:2000)及びJIS Q 14001:1996(ISO 14001:1996)規格との整合性がとられている。
- 経営陣の責任と関与の必要性が明確になり、ISMSの運用効果が高まる。
- リスクマネジメントにおけるPDCAモデルを明確化することにより、ISMSの有効性が高まる。



4 ISMSのポイント

ISMSとは、個別の問題毎の技術対策の他に、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。組織が保護すべき情報資産について、機密性、完全性、可用性をバランス良く維持し改善することがISMSの基本コンセプトである

情報セキュリティの3要素(機密性、完全性、可用性)

JIS X 5080:2002では、情報セキュリティの3要素を次のように定義している。

機密性:アクセスを認可された者だけが情報にアクセスできることを確実にすること。

完全性:情報および処理方法が、正確であること及び完全であることを保護すること。

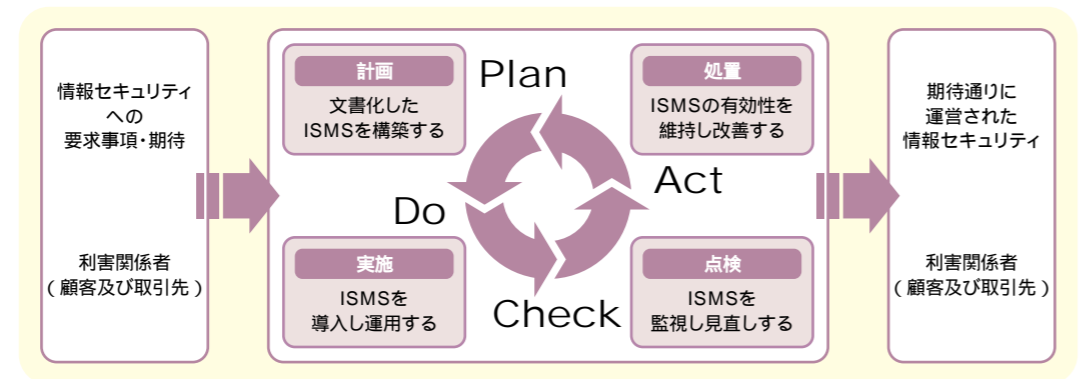
可用性:認可された利用者が、必要なときに、情報及び関連する資産にアクセスできることを確実にすること。

PDCAモデルによるプロセスアプローチ

組織は、ISMSを有効に機能させるために、多くの活動を明確にし、運営管理しなければならない。ISMS認証基準(Ver.2.0)では、組織においてISMSを確立、導入、運用、監視、維持し、かつそのISMSの有効性を改善する際に、プロセスアプローチを採用することを奨励している。プロセスアプローチとは、インプットをアウトプットに変換するために、経営資源を使用して運営管理されるあらゆる活動をプロセスとみなし、組織内のプロセスを明確にし、その相互関係を把握し、これら一連のプロセスをシステムとして適用して、運営管理することである。

プロセスアプローチを採用するメリットは、個々のプロセス間のつながりを管理し、プロセスの組合せや相互作用を管理することにより、ISMSを有効に機能させることができることである。

ISMS認証基準(Ver.2.0)では、情報セキュリティに関連するプロセスに対し、「Plan-Do-Check-Act(PDCA)」モデルを適用することで、「利害関係者の情報セキュリティ要求事項および期待」をインプットに、これらの要求事項および期待を満たす情報セキュリティの成果(運用管理された情報セキュリティ)をアウトプットとして生み出すプロセスを継続的に改善していくことがポイントである。



Plan - 計画 (ISMSの確立)	組織の全般的な基本方針及び目標に沿った結果を出すための、リスクマネジメント及び情報セキュリティの改善に関連する情報セキュリティ基本方針、目標、対象、プロセス及び手順を確立する。
Do - 実施 (ISMSの導入及び運用)	その情報セキュリティ基本方針、管理策、プロセス及び手順を導入し運用する。
Check - 点検 (ISMSの監視及び見直し)	情報セキュリティ基本方針、目標及び実際の経験に照らしてプロセスの実施状況の評価し、可能な場合これを測定し、その結果を見直しのために経営陣に報告する。
Act - 処置 (ISMSの維持及び改善)	ISMSの継続的な改善を達成するために、マネジメントレビューの結果に基づいて是正処置及び予防処置を講ずる。

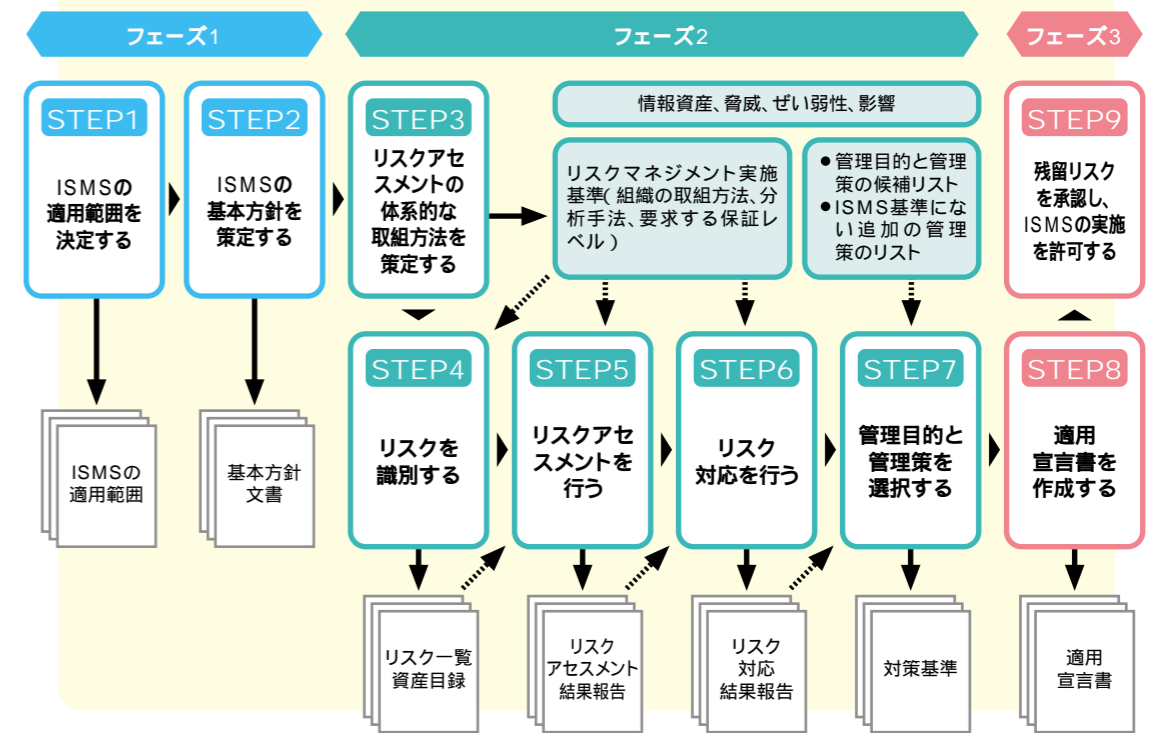
5 ISMSの確立

ISMSの確立は、3つのフェーズに分けて考えることができる。

フェーズ1:ISMSの適用範囲及び基本方針を確立する。(STEP1~STEP2)

フェーズ2:リスクアセスメントに基づいて管理策の選択をする。(STEP3~STEP7)

フェーズ3:リスクについて適切に対応する計画を策定する。(STEP8~STEP9)



フェーズ1:ISMSの適用範囲及び基本方針を確立する。(STEP1~STEP2)

ISMSの適用範囲は、事業の特徴、組織、その所在地、資産及び技術の観点から定義する。ISMSの基本方針は、事業上及び法的要求事項やリスクアセスメントなどから導かれる情報セキュリティに対する要求事項を考慮し、リスクマネジメント環境、ISMSを確立し維持する組織環境、情報セキュリティの全般的な方向性及び行動指針を確立する。

フェーズ2:リスクアセスメントに基づいて管理策の選択をする。(STEP3~STEP7)

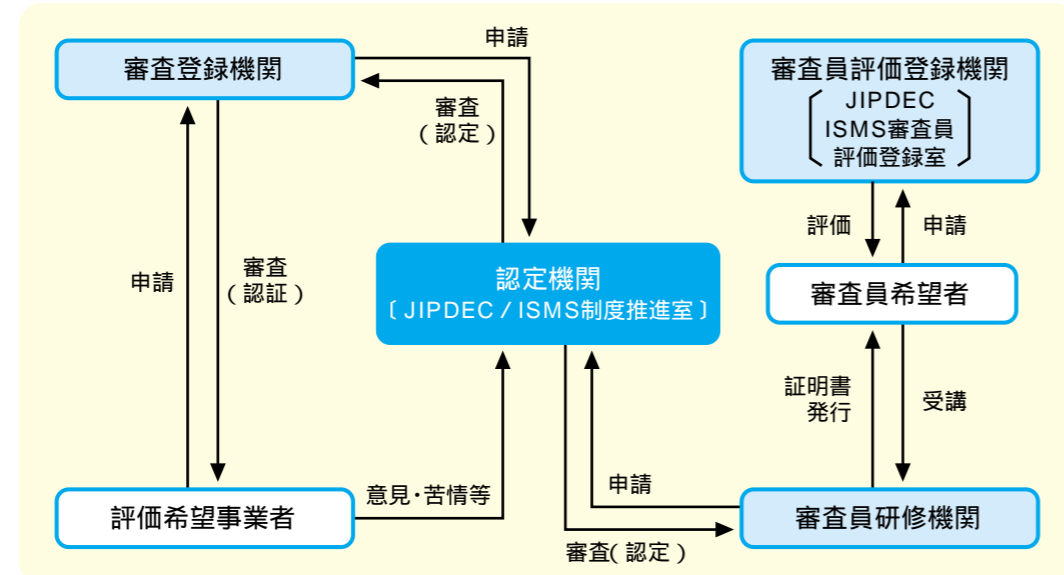
決定したISMSの適用範囲及び基本方針に基づき、リスクアセスメントの体系的な取組方法を策定する。リスクの識別では、保護すべき情報資産に対して機密性、完全性、可用性を喪失させる脅威、ぜい弱性及びそれらが事業に及ぼす潜在的な影響の大きさを識別する。リスクアセスメントでは、セキュリティ障害による事業上の損害及び発生可能性を評価した結果でリスクの度合いを算定し、リスクの評価基準を使用してリスクの受容ができるか、リスク対応が必要かどうかを判定する。リスクの受容ができない場合、リスク対応として、管理策の採用、リスク保有、リスク回避、リスク移転の選択をする。リスク対応の結論に従って、附属書「詳細管理策」のリストから、適切な管理目的と管理策を選択する。また、組織の必要に応じて追加の管理目的と管理策を採用することもできる。

フェーズ3:リスクについて適切に対応する計画を策定する。(STEP8~STEP9)

選択した管理目的及び管理策並びに選択の理由を記載した適用宣言書を作成し、附属書の「詳細管理策」で適用除外とした管理策を記録する。経営陣は、適用宣言書及び残留リスクを承認しISMSを実施する許可を与える。

ISMS適合性評価制度の運用

ISMS適合性評価制度は、組織が構築したISMSが認証基準に適合しているか審査し登録する「審査登録機関」、その審査員になるために必要な研修を実施する「審査員研修機関」及び審査員の資格を付与する「審査員評価登録機関」、そしてこれら各機関がその業務を行う能力を備えているかをみる「認定機関」からなる総合的な仕組みである。



ISMS制度運用体制

認定機関:(財)日本情報処理開発協会(JIPDEC)ISMS制度推進室

- ISMS適合性評価制度の運用と維持管理を行う。
- 審査登録機関の認定と定期的なサーベイランス、3年毎の更新審査を実施する。
- 審査員研修機関の認定と定期的なサーベイランス、3年毎の更新審査を実施する。
- ISMS適合性評価制度に関する情報を提供する。
- ISMS適合性評価制度に関する意見や苦情等の受付を行う。

審査登録機関

- ISMS審査登録機関認定基準に基づいて、認定を受ける。
- ISMS認証基準により、評価希望事業者の審査・登録を行う。
- 登録した事業者の定期的なサーベイランス、3年毎の更新審査を行う。

評価希望事業者:ISMS認証取得を希望する事業者

- ISMSの適用範囲及び基本方針を確立する。
- 審査登録機関を選択し申請する。
- ISMS認証基準に適合しているかどうか本審査(Stage1、Stage2)を受け、審査結果に基づき認証・登録される。
- 登録された場合、ロゴマークを商業文書に使用することができる。

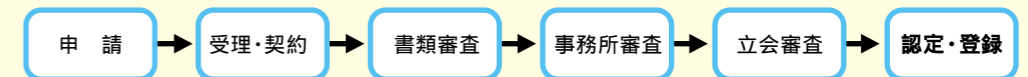
審査員研修機関

- ISMS審査員研修機関認定基準、ISMS審査員研修コース基準に基づいて、認定を受ける。
- 審査員を養成するため、ISMS審査員研修を実施する。
- 受講者の観察評価、最終試験の結果を総合的に判断し、可否を判定する。

審査員評価登録機関:(財)日本情報処理開発協会(JIPDEC)ISMS審査員評価登録室

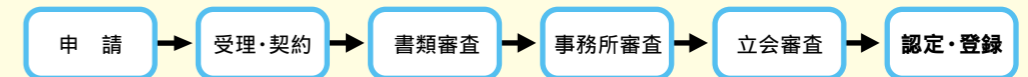
- ISMS審査員資格基準に基づいて、ISMS審査員(審査員補、審査員、主任審査員)を評価・登録する。
- ISMS審査員の登録の有効期限は3年間で、3年毎に再登録の評価を実施する。

審査登録機関の認定・登録の流れ



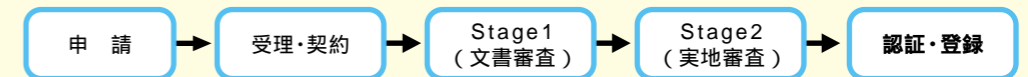
- 審査に用いられる基準は、ISMS審査登録機関認定基準による。
- 申請に必要な条件や手順はISMS審査登録機関認定の手順による。
- 認定審査において不適合の指摘事項があった場合は、是正処置または是正計画を提出し、妥当性が確認された後に認定となる。

審査員研修機関の認定・登録の流れ



- 審査に用いられる基準は、ISMS審査員研修機関認定基準及びISMS審査員研修コース基準による。
- 申請に必要な条件や手順はISMS審査員研修機関認定の手順による。
- 認定審査において不適合の指摘事項があった場合は、是正処置または是正計画を提出し、妥当性が確認された後に認定となる。

評価希望事業者の認証・登録の流れ



- 審査に用いられる基準は、ISMS認証基準による。
- 申請に必要な条件や審査手順は審査登録機関により異なる。
(認証の審査・登録のプロセスの詳細は審査登録機関に問い合わせてください。)

ISMS制度運営の公平性・透明性・客観性の確保

ISMS適合性評価制度の運営については、その公平性・透明性及び客観性を確保するために、JIPDEC組織運営機構の中に学識経験者及び業界団体の有識者等から構成される運営委員会及びその下部組織である技術専門部会を設置している。これら委員会活動の詳細は、URL : <http://www.isms.jipdec.jp/comm/> をご参照ください。

ISMS制度の基準・規程・手順・ガイド等

ISMS認証基準	第三者である審査登録機関が本制度の認証を希望する事業者の適合性を評価するための認証基準である。
ISMSガイド	ISMS認証基準に沿って、解説、例示等を含んで構成されており、審査業務を実施する上での参考ガイド。なお、本書内の例示はあくまでも審査のイメージを伝えることを目的としており審査方法を規定するものではない。
ISMS審査登録機関認定基準	審査登録機関の認定審査及び登録を行う際の認定基準である。
ISMS審査登録機関認定の手順	審査登録機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの。
ISMS審査員研修機関認定基準	審査員向けの研修を行う研修機関の認定審査及び登録を行う際の認定基準である。
ISMS審査員研修コース基準	審査員研修コースの内容について、その要求事項等を定めた研修コースの認定基準である。
ISMS審査員研修機関認定の手順	ISMS審査員研修機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの。
ISMS審査員資格基準	各審査員(審査員補、審査員、主任審査員)についての資格基準を規定したもの。
ISMS審査員登録の手順	各審査員の資格要件に基づいて評価登録する際の手順を規定したもの。
ISMS認定マーク使用規程	ISMS認定マークを使用する場合の、ISMS認定マークの表示及び適用条件等について規定したもの。

備考:上記の他、ISMS適合性評価制度の普及促進のためのガイド等がある。例えば、ISMSを構築するためのポイントを分かり易く説明した解説書や、ISMS認証基準の考え方を説明した解説書などである。