金融検査マニュアル　新旧対照表

現行	改正後
顧客保護等管理態勢の確認検査用チェックリスト **Ⅰ．（略）** **Ⅱ．各管理責任者による顧客保護等管理態勢の整備・確立状況** **【検証ポイント】** **（略）** **１．～２．（略）** **３．顧客情報管理態勢** **⑴　（略）** **⑵　顧客情報管理の実施** **①～②（略）** **③【システム対応】** 顧客情報統括管理責任者は、システム担当部門又はシステム担当者を通じて、以下のような対応を行っているか。 （ⅰ）～（ⅱ）（略）	**顧客保護等管理態勢の確認検査用チェックリスト** **Ⅰ．（略）** **Ⅱ．各管理責任者による顧客保護等管理態勢の整備・確立状況** **【検証ポイント】** **（略）** **１．～２．（略）** **３．顧客情報管理態勢** **⑴　（略）** **⑵　顧客情報管理の実施** **①～②（略）** **③【システム対応】** 顧客情報統括管理責任者は、システム担当部門又はシステム担当者を通じて、以下のような対応を行っているか。 （ⅰ）～（ⅱ）（略）

現行	改正後
（新設）	（iii）顧客の重要情報について、アクセス記録を保存し、検証しているか。
（新設）	（iv）顧客の重要情報へのアクセスについて、管理者と担当者の分離等により相互牽制を図っているか。
（iii）～（iv）（略）	（v）～（vi）（略）
④～⑧（略）	**④～⑧（略）**
⑶　（略）	**⑶　（略）**
４．～５．（略）	**４．～５．（略）**
Ⅲ．（略）	**Ⅲ．（略）**

現行	改正後
オペレーショナル・リスク管理態勢の確認検査用チェックリスト （別紙２） Ⅰ．　経営陣によるシステムリスク管理態勢の整備・確立状況 【検証ポイント】 ・　（略） ・　（略） （新設） ・　（略） ・　（略） ・　（略） ・　（略） ・　（略） ・　（略） ・　（略）	オペレーショナル・リスク管理態勢の確認検査用チェックリスト （別紙２） Ⅰ．　経営陣によるシステムリスク管理態勢の整備・確立状況 【検証ポイント】 ・　（略） ・　（略） ・　インターネットを利用したサービスの普及等に伴い顧客利便性が飛躍的に向上する一方で、サイバー攻撃の手口が巧妙化し影響も世界的規模で深刻化しており、金融機関においてはサイバーセキュリティを確保することが喫緊の課題となっている。 　経営陣においては、サイバー攻撃による顧客、取引先の被害を防止し、安定したサービスを提供するため、サイバーセキュリティ管理態勢を構築し、状況の変化に対応し継続的に改善していくことが求められている。 ・　（略） ・　（略） ・　（略） ・　（略） ・　（略） ・　（略） ・　（略）

現行	改正後
１．方針の策定 **①【取締役の役割・責任】** （ⅰ）取締役は、システムリスク管理（システム障害の未然防止及び発生時の迅速な復旧対応を含む。以下同じ。）を軽視することが戦略目標の達成に重大な影響を与えることを十分に認識し、システムリスク管理を重視しているか。 （新設） （新設） （ⅱ）～（ⅲ）（略）	**１．方針の策定** **①【取締役の役割・責任】** （ⅰ）取締役は、システムリスク管理（システム障害やサイバーセキュリティ事案[1]（以下「システム障害等」という。）の未然防止及び発生時の迅速な復旧対応を含む。以下同じ。）を軽視することが戦略目標の達成に重大な影響を与えることを十分に認識し、システムリスク管理を重視しているか。 （ⅱ）取締役は、システム障害等発生時において、自らの果たすべき責任やとるべき対応について具体的に定めているか。また、自らが指揮を執る訓練を行い、その実効性を確保しているか。 （ⅲ） 取締役会等は、サイバー攻撃が高度化・巧妙化していることを踏まえ、サイバーセキュリティの重要性を認識し必要な態勢を整備しているか。 また、取締役会等は、サイバーセキュリティについて、例えば、以下のような態勢を整備しているか。 ・ サイバー攻撃に対する監視体制 ・ サイバー攻撃を受けた際の報告及び広報体制 ・ 組織内 CSIRT（Computer Security Incident Response Team）等の緊急時対応及び早期警戒のための体制 ・ 情報共有機関等を通じた情報収集・共有体制 等 （ⅳ）～（ⅴ）（略）

現行	改正後
（新設）	脚注１　サイバーセキュリティ事案とは、情報通信ネットワークや情報システム等の悪用により、サイバー空間を経由して行われる不正侵入、情報の窃取、改ざんや破壊、情報システムの作動停止や誤作動、不正プログラムの実行やDDoS攻撃等の、いわゆる「サイバー攻撃」により、サイバーセキュリティが脅かされる事案をいう。
②（略）	**②（略）**
③【システムリスク管理方針の整備・周知】 取締役会は、システムリスク管理に関する方針（以下「システムリスク管理方針」という。）を定め、組織全体に周知させているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。 ・　（略） ・　（略） ・　（略） ・　セキュリティポリシー(組織の情報資産を適切に保護するための基本方針であり、①保護されるべき情報資産、②保護を行うべき理由、③それらについての責任の所在等の記載がなされたもの。)[1]	**③【システムリスク管理方針の整備・周知】** 取締役会は、システムリスク管理に関する方針（以下「システムリスク管理方針」という。）を定め、組織全体に周知させているか。例えば、以下の項目について明確に記載される等、適切なものとなっているか。 ・　（略） ・　（略） ・　（略） ・　セキュリティポリシー(組織の情報資産を適切に保護するための基本方針であり、①保護されるべき情報資産、②保護を行うべき理由、③それらについての責任の所在等の記載がなされたもの。)[2]
脚注1　（略）	脚注2　（略）
④【方針策定プロセスの見直し】	**④【方針策定プロセスの見直し】**

現行	改正後
取締役会は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、方針策定のプロセスの有効性を検証し、適時に見直しているか。	取締役会は、定期的に又は必要に応じて随時、システムリスク管理の状況に関する報告・調査結果等を踏まえ、方針策定のプロセスの有効性を検証し、適時に見直しているか。 また、取締役会等は他社における不正・不祥事件も参考に、情報セキュリティ管理態勢を PDCA サイクルにより継続的に改善しているか。
２．内部規程・組織体制の整備 **①（略）** **②【システムリスク管理部門の態勢整備】** （ⅰ）取締役会等は、システムリスク管理方針及びシステムリスク管理規程に則り、システムリスク管理部門を設置し、適切な役割を担わせる態勢を整備しているか[2]。 （ⅱ）（略） （ⅲ）取締役会等は、システムリスク管理部門に、その業務の遂行に必要な知識と経験を有する人員を適切な規模で配置し、当該人員に対し業務の遂行に必要な権限を与えているか[3]。 （ⅳ）（略） 脚注 2　（略） 脚注 3　（略） **③～④（略）** **⑤【監査役への報告態勢の整備】**	**２．内部規程・組織体制の整備** **①（略）** **②【システムリスク管理部門の態勢整備】** （ⅰ）取締役会等は、システムリスク管理方針及びシステムリスク管理規程に則り、システムリスク管理部門を設置し、適切な役割を担わせる態勢を整備しているか[3]。 （ⅱ）（略） （ⅲ）取締役会等は、システムリスク管理部門に、その業務の遂行に必要な知識と経験を有する人員を適切な規模で配置し、当該人員に対し業務の遂行に必要な権限を与えているか[4]。 （ⅳ）（略） 脚注 3　（略） 脚注 4　（略） **③～④（略）** **⑤【監査役への報告態勢の整備】**

現行	改正後
取締役会は、監査役へ直接報告されるべき事項を特定した場合には、報告事項を適切に設定した上で管理者から直接報告を行わせる態勢を整備しているか。[4]	取締役会は、監査役へ直接報告されるべき事項を特定した場合には、報告事項を適切に設定した上で管理者から直接報告を行わせる態勢を整備しているか。[5]
脚注4　（略）	脚注5　（略）
⑥【内部監査実施要領及び内部監査計画の策定】 取締役会等は、内部監査部門に、システムリスク管理について監査すべき事項を適切に特定させ、内部監査の実施対象となる項目及び実施手順を定めた要領（以下「内部監査実施要領」という。）並びに内部監査計画を策定させた上で承認しているか。[5]例えば、以下の項目については、内部監査実施要領又は内部監査計画に明確に記載し、適切な監査を実施する態勢を整備しているか。 ・　（略） ・　（略） ・　（略） ・　（略）	**⑥【内部監査実施要領及び内部監査計画の策定】** 取締役会等は、内部監査部門に、システムリスク管理について監査すべき事項を適切に特定させ、内部監査の実施対象となる項目及び実施手順を定めた要領（以下「内部監査実施要領」という。）並びに内部監査計画を策定させた上で承認しているか。[6]例えば、以下の項目については、内部監査実施要領又は内部監査計画に明確に記載し、適切な監査を実施する態勢を整備しているか。 ・　（略） ・　（略） ・　（略） ・　（略）
脚注5　（略）	脚注6　（略）
⑦（略）	**⑦（略）**
３．（略）	**３．（略）**

現行	改正後
Ⅱ．管理者によるシステムリスク管理態勢の整備・確立状況 **【検証ポイント】** **（略）** **１．（略）** **２．システムリスク管理部門の役割・責任** **⑴　【システムリスクの認識・評価】** （ⅰ）～（ⅱ）（略） （ⅲ）システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害の影響の複雑化・広範化など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。 （ⅳ）～（ⅵ）（略） **⑵ ～⑷　（略）** **Ⅲ．個別の問題点** **【検証ポイント】**	**Ⅱ．管理者によるシステムリスク管理態勢の整備・確立状況** **【検証ポイント】** **（略）** **１．（略）** **２．システムリスク管理部門の役割・責任** **⑴　【システムリスクの認識・評価】** （ⅰ）～（ⅱ）（略） （ⅲ）システムリスク管理部門は、顧客チャネルの多様化による大量取引の発生や、ネットワークの拡充によるシステム障害等の影響の複雑化・広範化など、外部環境の変化によりリスクが多様化していることを踏まえ、定期的に又は適時にリスクを認識・評価しているか。 （ⅳ）～（ⅵ）（略） **⑵ ～⑷（略）** **Ⅲ．個別の問題点** **【検証ポイント】**

現行	改正後
（略）	（略）
１．情報セキュリティ管理	１．情報セキュリティ管理
⑴　セキュリティ管理者等の役割・責任	⑴　セキュリティ管理者等の役割・責任
①【セキュリティ管理者の役割・責任】	①【セキュリティ管理者の役割・責任】
（ⅰ）～（ⅳ）（略）	（ⅰ）～（ⅳ）（略）
（新設）	（ⅴ）セキュリティ管理者は、セキュリティ意識の向上を図るため、全役職員に対するセキュリティ教育（外部委託先におけるセキュリティ教育を含む）を行っているか。
②～④（略）	②～④（略）
（新設）	⑵　【情報資産の保護】 （ⅰ）金融機関が責任を負うべき顧客の重要情報を網羅的に洗い出し、把握、管理しているか。 顧客の重要情報の洗い出しにあたっては、業務、システム、外部委託先を対象範囲とし、例えば、以下のようなデータを洗い出しの対象範囲としているか。 ・　通常の業務では使用しないシステム領域に格納されたデータ ・　障害解析のためにシステムから出力された障害解析用データ ・　ＡＴＭ（店舗外含む）等に保存されている取引ログ　等 （ⅱ）洗い出した顧客の重要情報について、重要度判定やリスク評価を実施しているか。 また、それぞれの重要度やリスクに応じ、以下のような情報管理ル

現行	改正後
	ールを策定しているか。 ・　情報の暗号化、マスキングのルール ・　情報を利用する際の利用ルール ・　記録媒体等の取扱いルール　等 （ⅲ）機密情報について、暗号化やマスキング等の管理ルールを定めているか。また、暗号化プログラム、暗号鍵、暗号化プログラムの設計書等の管理に関するルールを定めているか。 なお、「機密情報」とは、暗証番号、パスワード、クレジットカード情報等、顧客に損失が発生する可能性のある情報をいう。 （ⅳ）機密情報の保有・廃棄、アクセス制限、外部持ち出し等について、業務上の必要性を十分に検討し、より厳格な取扱いをしているか。 （ⅴ）情報資産について、管理ルール等に基づいて適切に管理されていることを定期的にモニタリングし、管理態勢を継続的に見直しているか。
⑵～⑶　**（略）**	⑶～⑷　**（略）**
⑷　**【インターネットを利用した取引の管理】** （新設）	⑸　**【インターネットを利用した取引の管理】** （ⅰ）インターネットバンキングの犯罪手口が高度化・巧妙化し、被害が拡大していることを踏まえ、リスク分析、セキュリティ対策の策定・実施、効果の検証（顧客に対する対策普及状況を含む）、対策の評価・見直しなどを行う態勢を整備しているか。 その際、情報共有機関等を活用して、犯罪の発生状況や犯罪手口に関する情報の提供・収集を行うとともに、有効な対応策等を共有し、

現行	改正後
（新設）	自らの顧客や業務の特性に応じた検討を行った上で、今後発生が懸念される犯罪手口への対応も考慮し、必要な態勢の整備に努めているか。 （ⅱ）セキュリティ対策については、犯罪手口に対する個々のセキュリティ対策の強度を検証した上で、顧客属性を勘案し、複数の対策を組み合わせるなど、犯罪手口の高度化・巧妙化（例えば「中間者攻撃」や「マン・イン・ザ・ブラウザ攻撃」など）に対応した対策を講じているか。 認証方式や不正防止策として、以下のような対策事例がある。 ・　可変式パスワードや電子証明書などの、固定式の ID・パスワードのみに頼らない認証方式 ・　取引に利用しているパソコンのブラウザとは別の携帯電話等の機器を用いるなど、複数経路による取引認証 ・　ハードウェアトークン等でトランザクション署名を行うトランザクション認証 ・　取引時においてウィルス等の検知・駆除が行えるセキュリティ対策ソフトの利用者への提供 ・　利用者のパソコンのウィルス感染状況を金融機関側で検知し、警告を発するソフトの導入 ・　電子証明書を IC カード等、取引に利用しているパソコンとは別の媒体・機器へ格納する方式の採用 ・　不正なログイン・異常な取引等を検知し、速やかに利用者に連絡する体制の整備　等
（ⅰ）顧客からの苦情・相談等を受け付ける態勢を整備しているか。	（（ⅴ）へ変更）

現行	改正後
（ⅱ）（略）	（（ⅳ）へ変更）
（ⅲ）（略）	（ⅲ）（略）
（ⅳ）当該金融機関の財務や業務の内容に関する情報及びインターネットを利用した取引において提供するサービスの内容について、例えばホームページにおいて開示しているか。	（削除）
（新設・（ⅱ）より）	（ⅳ）（略）
（新設・（ⅰ）より）	（ⅴ）顧客からの苦情・相談（不正取引の発生を含む）等を受け付ける態勢を整備しているか。
（ⅴ）～（ⅶ）（略）	（ⅵ）～（ⅷ）（略）
（ⅷ）利用者自身が使用状態を確認できる機能を設け、利用者を不正使用から守っているか。	（ⅸ）顧客に求められるセキュリティ対策事例を顧客に対して十分に周知しているか。顧客自らによる早期の被害認識を可能とするため、顧客が取引内容を適時に確認できる手段を講じているか。また、新たな犯罪の手口が発生するなど必要な場合、速やかにかつ顧客が容易に理解できる形で周知しているか。 不正取引を防止するための対策が利用者に普及しているかを定期的にモニタリングし、普及させるための追加的な施策を講じているか。
（ⅸ）フィッシング詐欺対策については、利用者がアクセスしているサイトが真正なサイトであることの証明を確認できるような措置を講じる等、業務に応じた適切な不正防止策を講じているか。	（削除）
（新設）	（ⅹ）不正取引に係る損失の補償については、預貯金者保護法及び全国銀行協会の申合せの趣旨を踏まえ、顧客対応方針を定め、顧客対応態勢を整備しているか。

現行	改正後
⑸（略）	⑹（略）
（新設）	２．サイバーセキュリティ管理 ⑴　【サイバーセキュリティ対策】 （ｉ）サイバー攻撃に備え、入口対策、内部対策、出口対策といった多段階のサイバーセキュリティ対策を組み合わせた多層防御を講じているか。 ・　入口対策（例えば、ファイアウォールの設置、抗ウィルスソフトの導入、不正侵入検知システム・不正侵入防止システムの導入等） ・　内部対策（例えば、特権 ID・パスワードの適切な管理、不要な ID の削除、特定コマンドの実行監視　等） ・　出口対策（例えば、通信ログ・イベントログ等の取得と分析、不適切な通信の検知・遮断　等） （ⅱ）サイバー攻撃を受けた場合に被害の拡大を防止するために、以下のような措置を講じているか。 ・　攻撃元の IP アドレスの特定と遮断 ・　DDoS 攻撃に対して自動的にアクセスを分散させる機能 ・　システムの全部又は一部の一時的停止　等 （ⅲ）システムの脆弱性について、OS の最新化やセキュリティパッチの適用など必要な対策を適時に講じているか。 （ⅳ）サイバーセキュリティについて、ネットワークへの侵入検査や脆弱性診断等を活用するなど、セキュリティ水準の定期的な評価を実施し、

現行	改正後
	セキュリティ対策の向上を図っているか。 ⑵　【コンティンジェンシープランの策定】 サイバー攻撃を想定したコンティンジェンシープランを策定し、訓練や見直しを実施しているか。また、必要に応じて、業界横断的な演習に参加しているか。 ⑶　【人材育成】 サイバーセキュリティに係る人材について、育成、拡充するための計画を策定し、実施しているか。
２．システム企画・開発・運用管理等 ⑴～⑵　（略） ⑶　システム運用態勢 ①～③（略） ④【システム障害の管理】 （ｉ）経営に重大な影響を与えるような重要なシステム障害が発生した場合には、速やかにシステムリスク管理部門及び関係業務部門と連携し、問題の解決を図るとともに、取締役会等及びオペレーショナル・リスクの総合的な管理部門に速やかに報告が行われる態勢を整備しているか。なお、報告に当たっては、最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で過小報	３．システム企画・開発・運用管理等 ⑴～⑵　（略） ⑶　システム運用態勢 ①～③（略） ④【システム障害等の管理】 （ｉ）経営に重大な影響を与えるような重要なシステム障害等が発生した場合には、速やかにシステムリスク管理部門及び関係業務部門と連携し、問題の解決を図るとともに、取締役会等及びオペレーショナル・リスクの総合的な管理部門に速やかに報告が行われる態勢を整備しているか。なお、報告に当たっては、最大リスク等を報告する態勢（例えば、顧客に重大な影響を及ぼす可能性がある場合、報告者の判断で

現行	改正後
告することなく、最大の可能性を速やかに報告すること）となっているか。 （ⅱ）システム障害の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢を整備しているか。 （ⅲ）システム障害の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。また、顧客に適切に対応する態勢を整備しているか。 （ⅳ）システム障害の発生に備え、外部委託先を含めた指揮・命令系統が明確になっているか。また、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。 （ⅴ）システム障害が発生した場合には、記録簿等に記入し、内部規程・業務細則等に基づき、システムリスク管理部門に報告が行われる態勢を整備しているか。 （ⅵ）システムの運用を外部委託している場合、委託先において発生したシステム障害について、報告が行われる態勢を整備しているか。 （ⅶ）システム障害の内容の定期的な分析を行い、それに応じた対応策をとっているか。 （ⅷ）システム障害の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。 **⑷ （略）**	過小報告することなく、最大の可能性を速やかに報告すること）となっているか。 （ⅱ）システム障害等の発生に備え、最悪のシナリオを想定した上で、必要な対応を行う態勢を整備しているか。 （ⅲ）システム障害等の発生に備え、関係業務部門への情報提供方法、内容が明確になっているか。また、顧客に適切に対応する態勢を整備しているか。 （ⅳ）システム障害等の発生に備え、外部委託先を含めた指揮・命令系統が明確になっているか。また、ノウハウ・経験を有する人材をシステム部門内、部門外及び外部委託先等から速やかに招集するために事前登録するなど、応援体制が明確になっているか。 （ⅴ）システム障害等が発生した場合には、記録簿等に記入し、内部規程・業務細則等に基づき、システムリスク管理部門に報告が行われる態勢を整備しているか。 （ⅵ）システムの運用を外部委託している場合、委託先において発生したシステム障害等について、報告が行われる態勢を整備しているか。 （ⅶ）システム障害等の内容の定期的な分析を行い、それに応じた対応策をとっているか。 （ⅷ）システム障害等の影響を極小化するために、例えば障害箇所を迂回するなどのシステム的な仕組みを整備しているか。 **⑷ （略）**

現行	改正後
３．防犯・防災・バックアップ・不正利用防止	４．防犯・防災・バックアップ・不正利用防止
⑴～⑶　（略）	⑴～⑶　（略）
⑷　【バックアップ】	⑷　【バックアップ】
（ⅰ）～（ⅲ）（略）	（ⅰ）～（ⅲ）（略）
（ⅳ）業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害が発生した場合等に、速やかに業務を継続できる態勢を整備しているか。	（ⅳ）業務への影響が大きい重要なシステムについては、オフサイトバックアップシステム等を事前に準備し、災害、システム障害等が発生した場合等に、速やかに業務を継続できる態勢を整備しているか。
⑸　【コンティンジェンシープランの策定】	⑸　【コンティンジェンシープランの策定】
（ⅰ）～（ⅴ）（略）	（ⅰ）～（ⅴ）（略）
（ⅵ）コンティンジェンシープランは、他の金融機関におけるシステム障害事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。	（ⅵ）コンティンジェンシープランは、他の金融機関におけるシステム障害等事例や中央防災会議等の検討結果を踏まえるなど、想定シナリオの見直しを適宜行っているか。
（ⅶ）（略）	（ⅶ）（略）
４．外部委託管理[6]	５．外部委託管理[7]
⑴　外部委託業務の管理	⑴　外部委託業務の管理
①【外部委託先の選定】	①【外部委託先の選定】
システムリスク管理部門[7]は、外部委託管理責任者と連携し、外部委託の実施前に当該外部委託業務に内在するシステムリスクを特定し、サービスの質や存続の確実性等のリスク管理上の問題点を認識した上で、外部委託業務を的確、公正かつ効率的に遂行することができる能	システムリスク管理部門[8]は、外部委託管理責任者と連携し、外部委託（二段階以上の委託を含む。）の実施前に当該外部委託業務に内在するシステムリスクを特定し、サービスの質や存続の確実性等のリスク管理上の問題点を認識した上で、外部委託業務を的確、公正かつ効率

現行	改正後
力を有する者に委託するための措置を講じているか。外部委託先の選定に当たり、例えば、システムリスク管理の観点から、以下のような点に留意しているか。 ・　（略） ・　（略） ・　金融機関のレピュテーション等の観点[8]から問題ないか。 脚注6　（略） 脚注7　（略） 脚注8　（略）	的に遂行することができる能力を有する者に委託するための措置を講じているか。外部委託先の選定に当たり、例えば、システムリスク管理の観点から、以下のような点に留意しているか。 ・　（略） ・　（略） ・　金融機関のレピュテーション等の観点[9]から問題ないか。 脚注7　（略） 脚注8　（略） 脚注9　（略）
②【委託契約の内容】 システムリスク管理部門[7]は、外部委託管理責任者と連携し、委託契約において、提供されるサービス水準、外部委託先との役割分担や責任分担（例えば、委託契約に沿ってサービスが提供されない場合における外部委託先の責務、又は委託に関連して発生するおそれのある損害の負担の関係）、監査権限及び再委託手続き等について定めていることを確認するための措置を講じているか。	**②【委託契約の内容】** システムリスク管理部門[8]は、外部委託管理責任者と連携し、委託契約において、提供されるサービス水準、外部委託先との役割分担や責任分担（例えば、委託契約に沿ってサービスが提供されない場合における外部委託先の責務、又は委託に関連して発生するおそれのある損害の負担の関係）、監査権限及び再委託手続き等について定めていることを確認するための措置を講じているか。 また、外部委託先が遵守すべきルールやセキュリティ要件を外部委託先へ提示し、契約書等に明記しているか。
③【外部委託先のモニタリング】 システムリスク管理部門[7]は、外部委託管理責任者と連携し、外部委託した業務について、委託元として委託業務が適切に行われているこ	**③【外部委託先のモニタリング】** システムリスク管理部門[8]は、外部委託管理責任者と連携し、外部委託した業務（二段階以上の委託を含む。）について、委託元として委託

現行	改正後
とを定期的にモニタリングするために、例えば要員を配置するなどの必要な措置を講じているか。特に複数の金融機関の業務を受託するセンターの内部管理、開発・運用管理の状況について、報告を受ける態勢を整備しているか。 　また、システムの共同化等が進展する中、外部委託先における顧客データの管理状況を、委託元が監視、追跡できる態勢を整備しているか。	業務が適切に行われていることを定期的にモニタリングするために、例えば要員を配置するなどの必要な措置を講じているか。特に複数の金融機関の業務を受託するセンターの内部管理、開発・運用管理の状況について、報告を受ける態勢を整備しているか。 　また、システムの共同化等が進展する中、外部委託先における顧客データの管理状況を、委託元が監視、追跡できる態勢を整備しているか。
④（略）	**④（略）**
⑤【問題点の是正】 　システムリスク管理部門[7]は、問題点等を発見した場合には、外部委託管理責任者と連携して速やかに是正する措置を講じているか。	**⑤【問題点の是正】** 　システムリスク管理部門[8]は、問題点等を発見した場合には、外部委託管理責任者と連携して速やかに是正する措置を講じているか。
⑵　（略）	**⑵　（略）**
５．付保預金の円滑な払戻しのための整備状況等	**６．付保預金の円滑な払戻しのための整備状況等**
⑴　預金保険法第 55 条の２第４項及び第 58 条の３第１項を遵守するための取組みがなされる態勢を整備しているか[9]。	⑴　預金保険法第 55 条の２第４項及び第 58 条の３第１項を遵守するための取組みがなされる態勢を整備しているか[10]。
脚注 9　（略）	脚注 10　（略）
⑵～⑷　（略）	⑵～⑷　（略）
⑸　以下の作業について、手順書・マニュアルを整備しているか[10]。	⑸　以下の作業について、手順書・マニュアルを整備しているか[11]。
①～⑤　（略）	①～⑤　（略）

現行	改正後
脚注10　（略） **６．（略）**	脚注11　（略） **７．（略）**