

(改定前)	(改定後)
<p>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</p> <p>I. ～II. (略)</p> <p>III. 個別の問題点</p> <p>【検証ポイント】 (略)</p> <p>1. ～2. (略)</p> <p>3. 外部委託業務のオペレーショナル・リスク管理</p> <p>①【外部委託先の選定】</p> <p>オペレーショナル・リスクの総合的な管理部門は、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オペレーショナル・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、オペレーショナル・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。</p> <p>(略)</p> <ul style="list-style-type: none"> 金融機関のレピュテーション等の観点から問題ないか。 	<p>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</p> <p>I. ～II. (略)</p> <p>III. 個別の問題点</p> <p>【検証ポイント】 (略)</p> <p>1. ～2. (略)</p> <p>3. 外部委託業務のオペレーショナル・リスク管理</p> <p>①【外部委託先の選定】</p> <p>オペレーショナル・リスクの総合的な管理部門は、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オペレーショナル・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、オペレーショナル・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。</p> <p>(略)</p> <ul style="list-style-type: none"> 金融機関のレピュテーション等の観点から問題ないか。 <p>脚注 11 <u>例えば、外部委託先と反社会的勢力との関係の有無などを含む。</u></p>

(改定前)	(改定後)
<p>②～④ (略)</p> <p>4. ～6. (略)</p> <p>(別紙2)</p> <p>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</p> <p>【検証ポイント】</p> <p>(略)</p> <ul style="list-style-type: none"> 検査官は、システムリスク管理態勢に問題が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、「金融機関等コンピュータシステムの安全対策基準・解説書」(財団法人金融情報システムセンター編)等に基づき確認する。 <p>(略)</p> <p>1. 方針の策定</p> <p>① 【取締役の役割・責任】</p> <p>取締役は、<u>システムリスク管理</u>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。</p> <p>(新設)</p>	<p>②～④ (略)</p> <p>4. ～6. (略)</p> <p>(別紙2)</p> <p>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</p> <p>【検証ポイント】</p> <p>(略)</p> <ul style="list-style-type: none"> 検査官は、システムリスク管理態勢に問題が見られ、さらに深く業務の具体的検証をすることが必要と認められる場合には、「金融機関等コンピュータシステムの安全対策基準・解説書」(<u>公益財団法人金融情報システムセンター</u>編)等に基づき確認する。 <p>(略)</p> <p>1. 方針の策定</p> <p>① 【取締役の役割・責任】</p> <p>(i) 取締役は、<u>システムリスク管理</u>(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。</p> <p>(ii) 取締役会は、<u>システムリスクの重要性</u>を十分に認識した上で、システムを統括管理する担当取締役(以下「システム担当取締役」という。)を定</p>

(改定前)	(改定後)
<p>特に担当取締役は、システムリスクの所在、システムリスクの種類・特性及びシステムリスクの特定・評価・モニタリング・コントロール等の手法並びにシステムリスク管理の重要性を十分に理解し、この理解に基づき当該金融機関のシステムリスク管理の状況を的確に認識し、適正なシステムリスク管理態勢の整備・確立に向けた方針及び具体的な方策を検討しているか。</p> <p>②【戦略目標の明確化】</p> <p>取締役会は、情報技術革新を踏まえ、金融機関全体の経営方針に沿った戦略目標の中に、経営戦略の一環としてシステムを捉えるシステム戦略方針を含んでいるか。例えば、以下の項目について、システム戦略方針に明確に記載しているか。</p> <p>(略)</p> <p>③【システムリスク管理方針の整備・周知】</p> <p>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。</p> <p>(略)</p> <ul style="list-style-type: none"> ・ 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 <p>④ (略)</p>	<p><u>めているか。なお、システム担当取締役は、システムに関する十分な知識・経験を有し業務を適切に遂行できる者であることが望ましい。</u></p> <p>(iii) システム担当取締役は、システムリスクの所在、システムリスクの種類・特性及びシステムリスクの特定・評価・モニタリング・コントロール等の手法並びにシステムリスク管理の重要性を十分に理解し、この理解に基づき当該金融機関のシステムリスク管理の状況を的確に認識し、適正なシステムリスク管理態勢の整備・確立に向けた方針及び具体的な方策を検討しているか。</p> <p>②【戦略目標の明確化】</p> <p>取締役会は、情報技術革新を踏まえ、金融機関全体の経営方針に沿った戦略目標の中に、経営戦略の一環としてシステムを捉えるシステム戦略方針を盛り込んでいるか。例えば、以下の項目について、システム戦略方針に明確に記載しているか。</p> <p>(略)</p> <p>③【システムリスク管理方針の整備・周知】</p> <p>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。</p> <p>(略)</p> <ul style="list-style-type: none"> ・ 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 <p>④ (略)</p>

(改定前)	(改定後)
<p>脚注1 ・ (略)</p> <p>・ 「金融機関等におけるセキュリティポリシー策定のための手引書」 (財団法人金融情報システムセンター編) を参考。</p> <p>2. 内部規程・組織体制の整備</p> <p>①【内部規程の整備】 (略)</p> <p>②～⑦ (略)</p> <p>3. (略)</p> <p>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</p> <p>【検証ポイント】 (略)</p> <p>1. 管理者の役割・責任</p> <p>①～② (略)</p> <p>③【管理者による組織体制の整備】 (i)～(iv) (略)</p> <p>(v) 管理者は、システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、適正に管理するシステム管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。</p> <p>また、EUC(エンドユーザーコンピューティング)等ユーザー部門等が独自にシステムの企画、開発、運用を行うシステムについても、システム管</p>	<p>脚注1 ・ (略)</p> <p>・ 「金融機関等におけるセキュリティポリシー策定のための手引書」 (<u>公益</u>財団法人金融情報システムセンター編) を参考。</p> <p>2. 内部規程・組織体制の整備</p> <p>①【内部規程の整備・周知】 (略)</p> <p>②～⑦ (略)</p> <p>3. (略)</p> <p>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</p> <p>【検証ポイント】 (略)</p> <p>1. 管理者の役割・責任</p> <p>①～② (略)</p> <p>③【管理者による組織体制の整備】 (i)～(iv) (略)</p> <p>(v) 管理者は、システムの安全かつ円滑な運用と不正防止のため、システムの管理手順を定め、適正に管理するシステム管理者を設置し、管理業務の遂行に必要な権限を与えて管理させているか。</p> <p>また、EUC(エンドユーザーコンピューティング)等ユーザー部門等が独自にシステムの企画、開発、運用を行うシステムについても、システム管</p>

(改定前)	(改定後)
<p>理者を設置しているか。なお、システム管理者をシステム単位あるいは業務単位で設置していることが望ましい。</p>	<p>理者を設置しているか。なお、システム管理者については、システム単位あるいは業務単位で設置していることが望ましい。</p>
<p>(vi) ~ (vii) (略)</p>	<p>(vi) ~ (vii) (略)</p>
<p>④ (略)</p>	<p>④ (略)</p>
<p>2. システムリスク管理部門の役割・責任</p>	<p>2. システムリスク管理部門の役割・責任</p>
<p>(1) 【システムリスクの認識・評価】</p>	<p>(1) 【システムリスクの認識・評価】</p>
<p>(i) ~ (ii) (略)</p>	<p>(i) ~ (ii) (略)</p>
<p>(iii) システムリスク管理部門は、<u>ネットワークの拡充や新技術の進展等によりリスクが多様化・増加していることを認識・評価しているか。</u></p>	<p>(iii) システムリスク管理部門は、<u>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。</u></p>
<p><u>(新設)</u></p>	<p>(iv) システムリスク管理部門は、<u>例えば1口座当たりの未記帳取引明細の保有可能件数などのシステムの制限値を把握するなど、システムの処理能力に関するリスクを認識・評価しているか。</u></p>
<p><u>(新設)</u></p>	<p>(v) システムリスク管理部門は、<u>新商品の導入時又は商品内容の変更時に、システム開発の有無にかかわらず、関連するシステムのリスクを認識・評価しているか。</u></p>
<p><u>(iv) (略)</u></p>	<p><u>(vi) (略)</u></p>
<p>(2) 【システムリスクの状況等のモニタリング】</p>	<p>(2) 【システムリスクのモニタリング】</p>
<p>(i) システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、当該金融機関のシステムリスクの状況を適切な頻</p>	<p>(i) システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、<u>当該金融機関の内部環境 (リスク・プロファイル</u></p>

(改定前)	(改定後)
<p>度でモニタリングしているか。</p> <p>(ii) システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、システムリスクの状況に関して、取締役会等が適切に<u>評価・判断</u>できる情報を、定期的に又は必要に応じて随時、報告しているか。</p> <p><u>(新設)</u></p> <p>(3) 【検証・見直し】</p> <p>システムリスク管理部門は、業務の規模・特性及びリスク・プロファイルに見合った適切なシステムリスク管理方法であるかを定期的に検証し、見直しているか。</p>	<p><u>等) や外部環境の状況に照らし、当該金融機関のシステムリスクの状況を適切な頻度でモニタリングしているか。</u></p> <p>(ii) システムリスク管理部門は、システムリスク管理方針及びシステムリスク管理規程等に基づき、システムリスクの状況に関して、取締役会等及び<u>オペレーショナル・リスクの総合的な管理部門</u>が適切に<u>評価及び判断</u>できる情報を、定期的に又は必要に応じて随時、報告しているか。</p> <p>(3) 【システムリスクのコントロール及び削減】</p> <p><u>(i) システムリスクのコントロール</u></p> <p><u>システムリスク管理部門は、システムの制限値を超えた場合のシステム面・事務面の対応策を検討しているか。また、評価された重要なシステムリスクに係るコントロール方法について、取締役会等が意思決定できる情報を報告しているか。</u></p> <p><u>(ii) システムリスクの削減</u></p> <p><u>システムリスク管理部門は、システムリスクを削減する方策を実施する場合、新たなリスクの発生に注意を払っているか。</u></p> <p>(4) 【検証・見直し】</p> <p>システムリスク管理部門は、<u>業務環境の変化、リスク・プロファイルの変化を把握し、業務の規模・特性及びリスク・プロファイルに見合った適切なシステムリスク管理方法であるかを定期的に検証し、見直しているか。</u></p>

(改定前)	(改定後)
<p>Ⅲ. 個別の問題点</p> <p>【検証ポイント】 (略)</p> <p>1. (略)</p> <p>2. システム企画・開発・運用管理等</p> <p>(1) (略)</p> <p>(2) システム企画・開発態勢</p> <p>① 【企画・開発態勢】</p> <p>(i) ~ (iii) (略)</p> <p><u>(新設)</u></p> <p><u>(iv) (略)</u></p> <p><u>(v) 開発案件の検討・承認ルールが明確になっているか。</u></p> <p><u>(vi) (略)</u></p> <p>② 【開発管理】</p> <p>(i) (略)</p> <p>(ii) 開発プロジェクトごとに責任者を定め、システムの重要度及び性格を踏まえ取締役会等が進捗状況をチェックしているか。</p> <p>③ (略)</p> <p>④ 【テスト等】</p> <p>(i) ~ (ii) (略)</p>	<p>Ⅲ. 個別の問題点</p> <p>【検証ポイント】 (略)</p> <p>1. (略)</p> <p>2. システム企画・開発・運用管理等</p> <p>(1) (略)</p> <p>(2) システム企画・開発態勢</p> <p>① 【企画・開発態勢】</p> <p>(i) ~ (iii) (略)</p> <p><u>(iv) 現行システムに内在するリスクを継続的に洗い出し、その維持・改善のための投資を計画的に行っているか。</u></p> <p><u>(v) (略)</u></p> <p><u>(vi) 開発案件の企画・開発・移行の承認ルールが明確になっているか。</u></p> <p><u>(vii) (略)</u></p> <p>② 【開発管理】</p> <p>(i) (略)</p> <p>(ii) 開発プロジェクトごとに責任者を定め、システムの重要度及び性格を踏まえ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が進捗状況をチェックしているか。</p> <p>③ (略)</p> <p>④ 【テスト等】</p> <p>(i) ~ (ii) (略)</p>

(改定前)	(改定後)
<p>(iii) <u>総合テストには、ユーザー部門も参加するなど適切に実施されているか。</u></p> <p>(iv) (略)</p> <p>⑤～⑥ (略)</p> <p>⑦【人材の育成】 <u>(新設)</u></p> <p>人材の育成に当たっては、開発技術の養成だけではなく、開発対象とする業務に精通した人材の養成を行っているか。例えば、デリバティブ業務、電子決済、電子取引等、専門性の高い業務分野や新技術についても、精通した開発要員を養成しているか。</p> <p>(3) システム運用態勢</p> <p>①～③ (略)</p> <p>④【システム障害の管理】</p> <p><u>(i) システム障害が発生した場合には、記録簿等に記入し、必要に応じ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。</u> <u>((v) へ変更)</u></p> <p><u>(ii) 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。</u> ((vii) へ変更)</p>	<p>(iii) <u>総合テストは、ユーザー部門も参加するなど適切に実施されているか。</u></p> <p>(iv) (略)</p> <p>⑤～⑥ (略)</p> <p>⑦【人材の育成】 <u>現行システムの仕組み及び開発技術の継承並びに専門性を持った人材の育成のための具体的な計画を策定し、実施しているか。また、人材の育成に当たっては、開発技術の養成だけではなく、開発対象とする業務に精通した人材の養成を行っているか。例えば、デリバティブ業務、電子決済、電子取引等、専門性の高い業務分野や新技術についても、精通した開発要員を養成しているか。</u></p> <p>(3) システム運用態勢</p> <p>①～③ (略)</p> <p>④【システム障害の管理】</p> <p><u>(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。</u></p> <p><u>(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。</u></p>

(改定前)	(改定後)
<p>(iii) 経営に重大な影響を与えるような重要なシステム障害の場合には、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に報告しているか。((i) へ変更)</p> <p>(iv) 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、報告される態勢となっているか。((vi) へ変更)</p> <p>(新設・ (i) より)</p> <p>(新設・ (iv) より)</p> <p>(新設・ (ii) より)</p> <p>(新設)</p>	<p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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。</p> <p>(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の仕組みを整備しているか。</p>
<p>(4) システム監査</p> <p>(i) システム部門から独立した内部監査部門が定期的にシステム監査を行っているか。</p> <p>(ii) 内部監査部門は、システム関係に精通した要員を確保しているか。また、システムリスクについて、必要に応じ、会計監査人等による外部監査を受けているか。</p>	<p>(4) システム監査</p> <p>(i) システム部門から独立した内部監査部門が、定期的にシステム監査を行っているか。</p> <p>(ii) システム関係に精通した要員による内部監査の実施や、システム監査人等による外部監査の活用を行っているか。</p>

(改定前)	(改定後)
<p>3. 防犯・防災・バックアップ・不正利用防止 (1)～(3) (略)</p> <p>(4) 【バックアップ】 (i)～(ii) (略) <u>(新設・(iv)より)</u> <u>(iii) 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を保有しているか。</u> <u>(iv) バックアップ取得の周期を文書化しているか。((iii)へ変更)</u></p> <p>(5) 【コンティンジェンシープランの策定】 (i) 災害等によりコンピュータシステムが正常に機能しなくなった場合に備えたコンティンジェンシープランを整備しているか。 (ii) (略) (iii) コンティンジェンシープランの整備に当たっては、「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（財団法人金融情報システムセンター編）を参照しているか。 (iv) コンティンジェンシープランの整備に当たっては、災害による緊急事態を想定するだけでなく、<u>金融機関の内部に起因するものや金融機関の外部に起因するものも想定しているか。</u></p>	<p>3. 防犯・防災・バックアップ・不正利用防止 (1)～(3) (略)</p> <p>(4) 【バックアップ】 (i)～(ii) (略) <u>(iii) バックアップ取得の周期を文書化しているか。</u> <u>(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。</u></p> <p>(5) 【コンティンジェンシープランの策定】 (i) 災害等によりコンピュータシステムが正常に機能しなくなった場合に備えたコンティンジェンシープランを整備しているか。<u>また、取締役の果たすべき役割・責任やとるべき対応について具体的に定めるとともに、取締役が自ら指揮を執る訓練を行い、その実効性を確保しているか。</u> (ii) (略) (iii) コンティンジェンシープランの策定に当たっては、「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」（公益財団法人金融情報システムセンター編）を参照しているか。 (iv) コンティンジェンシープランの策定に当たっては、災害による緊急事態を想定するだけでなく、<u>金融機関の内部又は外部に起因するシステム障害等も想定しているか。</u>また、バッチ処理が大幅に遅延した場合など、十</p>

(改定前)	(改定後)
<p>(v) <u>コンティンジェンシープランの整備</u>に当たっては、決済システムに及ぼす影響や、顧客に与える被害等を分析しているか。</p> <p><u>(新設)</u></p> <p>(vi) <u>コンティンジェンシープランを使用した訓練を定期的に行っているか。</u> また、<u>訓練は、全社レベルで行い、必要に応じて外部委託先等が参加しているか。</u></p> <p><u>(新設)</u></p>	<p><u>分なリスクシナリオを想定しているか。</u></p> <p>(v) <u>コンティンジェンシープランの策定</u>に当たっては、決済システムに及ぼす影響や、顧客に与える被害等を分析しているか。</p> <p>(vi) <u>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。</u></p> <p>(vii) <u>コンティンジェンシープランに基づく訓練は、全社レベルで行い、複数の金融機関の業務を受託するセンター等の外部委託先等と合同で、定期的</u> <u>に実施しているか。</u></p> <p>4. 外部委託管理⁶</p> <p>(1) 外部委託業務の管理</p> <p>①【外部委託先の選定】</p> <p><u>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。</u></p> <ul style="list-style-type: none"> <u>・ 金融機関の合理性の観点からみて十分なレベルのサービスの提供を行い得るか。</u> <u>・ 委託契約に沿ったサービス提供や損害負担が確保できる財務・経営内容か。</u>

(改定前)	(改定後)
	<p>・ <u>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。</u></p> <p>②【委託契約の内容】</p> <p><u>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。</u></p> <p>③【外部委託先のモニタリング】</p> <p><u>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。</u></p> <p><u>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。</u></p> <p>④【外部委託先への監査】</p> <p><u>複数の金融機関の業務を受託するセンター等の重要な外部委託先に対して、内部監査部門又はシステム監査人等による監査を実施しているか。</u></p> <p>⑤【問題点の是正】</p> <p><u>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。</u></p>

(改定前)	(改定後)
	<p>脚注 6 <u>外部委託の形態や委託される業務内容は多様であり、当該検証項目においては、外部委託された業務の内容及び当該金融機関における重要度等を踏まえた検証が必要である。</u></p> <p>脚注 7 <u>オペレーショナル・リスクの総合的な管理部門において行うことを妨げるものではない。</u></p> <p>脚注 8 <u>例えば、外部委託先と反社会的勢力との関係の有無などを含む。</u></p> <p>(2) システム関係の業務委託先の検証</p> <p>① 業務委託を受けたシステム全般について、システムリスクを認識・評価しているか。</p> <p>② 金融機関から受託したシステム業務について、委託者による監査又は外部監査を定期的に受けているか。また、外部監査を実施した場合は、委託者に対して監査結果を報告しているか。</p> <p>③ 金融機関等が求めるセキュリティレベルを設定し、その内容についてあらかじめ金融機関等と合意しているか。</p> <p>④ 企画段階、設計・開発段階、テスト段階において、金融機関等によるユーザーレビューやユーザーテストが実施されているか。</p> <p>⑤ 開発標準ルールの遵守状況や品質管理状況について、品質管理部署等により客観的に評価する態勢を整備しているか。</p> <p>⑥ システムの運用状況について、金融機関等に対して報告する事項を定め、定期的に報告しているか。</p> <p>⑦ システム障害等の発生時の連絡態勢を、あらかじめ定めているか。</p> <p>⑧ 複数の金融機関の業務を受託するセンターの場合、他の金融機関への影響</p>

(改定前)	(改定後)
<p>4. (略)</p> <p><u>5. システム関係の業務委託先の検証 (4.(2)へ変更)</u></p> <p>(1) 業務委託を受けたシステム全般について、システムリスクを認識・評価しているか。</p> <p>(2) 金融機関から受託したシステム業務について、委託者による監査又は外部監査を定期的に受けているか。また、外部監査を実施した場合は、委託者に対して監査結果を報告しているか。</p> <p>(3) 金融機関等が求めるセキュリティレベルを設定し、その内容についてあらかじめ金融機関等と合意しているか。</p> <p>(4) 企画段階、設計・開発段階、テスト段階において、金融機関等によるユーザーレビューやユーザーテストが実施されているか。</p> <p>(5) 開発標準ルールの遵守状況や品質管理状況について、品質管理部署等により客観的に評価する態勢を整備しているか。</p> <p>(6) システムの運用状況について、金融機関等に対して報告する事項を定め、定期的に報告しているか。</p> <p>(7) システム障害等の発生時の連絡態勢を、あらかじめ定めているか。</p> <p>(8) 複数の金融機関の業務を受託するセンターの場合、他の金融機関への影響等を速やかに判断し、対応する態勢を整備しているか。</p> <p>6. (略)</p>	<p>等を速やかに判断し、対応する態勢を整備しているか。</p> <p>5. (略)</p> <p>(削除)</p> <p>6. (略)</p>