保険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	**顧客保護等管理態勢の確認検査用チェックリスト**
Ⅰ．（略）	**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	**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）**	**【検証ポイント】** **（略）**
１．　～３．（略）	**１．　～３．（略）**
４．顧客情報管理態勢 **⑴（略）**	**４．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） （新設） （新設）	**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） （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。 （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

現行	改正後
（ⅲ）～（ⅳ）（略） ④～⑧（略）	より相互牽制を図っているか。 （ⅴ）～（ⅵ）（略） ④～⑧（略）
⑶　（略）	⑶　（略）
５．～６．（略）	５．～６．（略）
Ⅲ．（略）	Ⅲ．（略）

現行	改正後
オペレーショナル・リスク等管理態勢の確認検査用チェックリスト Ⅰ．経営陣によるオペレーショナル・リスク等管理態勢の整備・確立状況 【検証ポイント】 ・　（略） ・　（略） ・　（略） ・　検査官は、システムリスク管理態勢の確認検査を行うに当たっては、個別システムの重要度（当該システムの顧客取引又は経営判断への影響の大きさ）及び性格（コンピュータセンターにおける中央集中型の汎用機システム、クライアントサーバーシステム等の分散系システム、ユーザー部門設置の単体システム等のそれぞれの特性を表し、それぞれに適した管理手法がある。）に十分留意する必要がある。また、本チェックリストによる検証の結果、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、検査官は、「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）等に基づき行うものとする。さらに、検査官は、保険会社が保持する保護すべき情報が役職員又は部外者等により、改ざん、削除又は外部に漏洩するリスクについても本チェックリストに基づき行うこととする。 （新設）	オペレーショナル・リスク等管理態勢の確認検査用チェックリスト Ⅰ．経営陣によるオペレーショナル・リスク等管理態勢の整備・確立状況 【検証ポイント】 ・　（略） ・　（略） ・　（略） ・　検査官は、システムリスク管理態勢の確認検査を行うに当たっては、個別システムの重要度（当該システムの顧客取引又は経営判断への影響の大きさ）及び性格（コンピュータセンターにおける中央集中型の汎用機システム、クライアントサーバーシステム等の分散系システム、ユーザー部門設置の単体システム等のそれぞれの特性を表し、それぞれに適した管理手法がある。）に十分留意する必要がある。また、本チェックリストによる検証の結果、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、検査官は、「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」（公益財団法人金融情報システムセンター編）等に基づき行うものとする。さらに、検査官は、保険会社が保持する保護すべき情報が役職員又は部外者等により、改ざん、削除又は外部に漏洩するリスクについても本チェックリストに基づき行うこととする。 ・　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

現行	改正後
	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。 　また、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） ・　（略） ・　（略） ・　（略）
１.方針の策定 ①【取締役の役割・責任】 　取締役は、オペレーショナル・リスク等の管理を軽視することが、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、オペレーショナル・リスク等管理を重視しているか。特に担当取締役は、オペレーショナル・リスク等の所在、種類・特性及びオペレーショナル・リスク等の特定・評価・モニタリング・コントロール等の手法並びに管理の重要性を十分に理解し、この理解に基づき当該保険会社のオペレーショナル・リスク等の管理の状況を的確に認識し、適正なオペレーショナル・リスク等の管理態勢の整備・確立に向けて、方針及び具体的な方策を検討しているか。	１.方針の策定 ①【取締役の役割・責任】 （ｉ）取締役は、オペレーショナル・リスク等の管理を軽視することが、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、オペレーショナル・リスク等管理を重視しているか。特に担当取締役は、オペレーショナル・リスク等の所在、種類・特性及びオペレーショナル・リスク等の特定・評価・モニタリング・コントロール等の手法並びに管理の重要性を十分に理解し、この理解に基づき当該保険会社のオペレーショナル・リスク等の管理の状況を的確に認識し、適正なオペレーショナル・リスク等の管理態勢の整備・確立に向けて、方針及び具体的な方策を検討しているか。

現行	改正後
（新設）	（ⅱ）取締役は、システム障害等（システム障害やサイバーセキュリティ事案[1]をいう。以下同じ。）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。
（新設）	（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
（新設）	（ⅳ）取締役会は、システムリスク管理（システム障害等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。）の重要性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。
（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

現行	改正後
	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【戦略目標】 （ⅰ）取締役会は、情報技術革新を踏まえ、保険会社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。 ・　（略） ・　（略） ・　（略） （ⅱ）（略）	**②【戦略目標】** （ⅰ）取締役会は、情報技術革新を踏まえ、保険会社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。 ・　（略） ・　（略） ・　（略） （ⅱ）（略）
③【オペレーショナル・リスク等管理方針の整備・周知】 （ⅰ）～（ⅱ）（略） （ⅲ）システムリスク管理方針には、例えば、以下の項目が明確に記載される等、適切なものとなっているか。 ・　（略） ・　（略） ・　システムリスクの特定、評価、モニタリング及びコントロールに関する方針 ・　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	**③【オペレーショナル・リスク等管理方針の整備・周知】** （ⅰ）～（ⅱ）（略） （ⅲ）システムリスク管理方針には、例えば、以下の項目が明確に記載される等、適切なものとなっているか。 ・　（略） ・　（略） ・　システムリスクの特定、評価、モニタリング、コントロール及び削減に関する方針 ・　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

現行	改正後
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] （ⅳ）（略）	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] （ⅳ）（略）
脚注1　・（略） ・「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。	脚注2　・（略） ・「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」（公益財団法人金融情報システムセンター編）を参考。
④【方針策定のプロセスの見直し】 取締役会は、定期的に又は必要に応じて随時、オペレーショナル・リスク等の管理状況に関する報告・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。	**④【方針策定のプロセスの見直し】** 取締役会は、定期的に又は必要に応じて随時、オペレーショナル・リスク等の管理状況に関する報告・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 **⑴　事務リスク管理態勢の整備** **①（略）** **②【事務リスク管理部門の態勢整備】** （ⅰ）取締役会等は、事務リスク管理方針及び事務リスク管理規程に則り、事務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）	**２．内部規程・組織体制の整備** **⑴　事務リスク管理態勢の整備** **①（略）** **②【事務リスク管理部門の態勢整備】** （ⅰ）取締役会等は、事務リスク管理方針及び事務リスク管理規程に則り、事務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）

現行	改正後
（iii）取締役会等は、事務リスク管理部門に、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]	（iii）取締役会等は、事務リスク管理部門に、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）	（iv）（略）
脚注2　（略）	脚注3　（略）
脚注3　（略）	脚注4　（略）
③～④（略）	**③～④（略）**
⑤【監査役への報告態勢の整備】 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事務リスク管理部門の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]	**⑤【監査役への報告態勢の整備】** 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事務リスク管理部門の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、内部監査部門又は内部監査部門長に、事務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。	**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、内部監査部門又は内部監査部門長に、事務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。

現行	改正後
・　（略） ・　（略） ・　（略） ・　（略） 脚注5　（略） **⑦（略）** **⑵　システムリスク管理態勢の整備** **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。[6] （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。[7] （ⅳ）（略） 脚注6　（略） 脚注7　（略）	・　（略） ・　（略） ・　（略） ・　（略） 脚注6　（略） **⑦（略）** **⑵　システムリスク管理態勢の整備** **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。[7] （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。[8] （ⅳ）（略） 脚注7　（略） 脚注8　（略）

現行	改正後
③～④（略） **⑤【監査役への報告態勢の整備】** 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システムリスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[8] 脚注8　（略）	③～④（略） **⑤【監査役への報告態勢の整備】** 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システムリスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[9] 脚注9　（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、内部監査部門又は内部監査部門長に、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。[9]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9　（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、内部監査部門又は内部監査部門長に、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。[10]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10　（略）

現行	改正後
⑦（略）	⑦（略）
⑶　流動性リスク管理態勢の整備	⑶　流動性リスク管理態勢の整備
①～②（略）	①～②（略）
③【流動性リスク管理部門及び資金繰り管理部門の態勢整備】	③【流動性リスク管理部門及び資金繰り管理部門の態勢整備】
（ⅰ）取締役会等は、流動性リスク管理方針及び流動性リスク管理規程に則り、流動性リスク管理部門及び資金繰り管理部門を設置し、適切な役割を担わせる態勢を整備しているか。[10]	（ⅰ）取締役会等は、流動性リスク管理方針及び流動性リスク管理規程に則り、流動性リスク管理部門及び資金繰り管理部門を設置し、適切な役割を担わせる態勢を整備しているか。[11]
（ⅱ）（略）	（ⅱ）（略）
（ⅲ）取締役会等は、流動性リスク管理部門及び資金繰り管理部門に、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。[11]	（ⅲ）取締役会等は、流動性リスク管理部門及び資金繰り管理部門に、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。[12]
（ⅳ）（略）	（ⅳ）（略）
脚注10　（略）	脚注11　（略）
脚注11　（略）	脚注12　（略）
④～⑤（略）	④～⑤（略）
⑥【監査役への報告態勢の整備】	⑥【監査役への報告態勢の整備】
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流動性リスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[12]	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流動性リスク管理部門の管理者から直接報告を行わせる態勢を整備しているか。[13]

現行	改正後
脚注12　（略）	脚注13　（略）
⑦【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、内部監査部門又は内部監査部門長に、流動性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。[13]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） ・　流動性リスク管理システム[14]の適切性 ・　（略） ・　（略） ・　（略） ・　（略）	**⑦【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、内部監査部門又は内部監査部門長に、流動性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。[14]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） ・　流動性リスク管理システム[15]の適切性 ・　（略） ・　（略） ・　（略） ・　（略）
脚注13　（略） 脚注14　（略）	脚注14　（略） 脚注15　（略）
⑧（略）	**⑧（略）**
３．評価・改善活動	**３．評価・改善活動**

現行	改正後
⑴　分析・評価 **①【オペレーショナル・リスク等管理の分析・評価】** 取締役会等は、監査役監査、内部監査及び外部監査[15]の結果、各種調査結果並びに各部門からの報告等全てのオペレーショナル・リスク等管理の状況に関する情報に基づき、オペレーショナル・リスク等管理の状況を的確に分析し、オペレーショナル・リスク等管理の実効性の評価を行った上で、態勢上の弱点、問題点等改善すべき点の有無及びその内容を適切に検討するとともに、その原因を適切に検証しているか。また、必要な場合には、利害関係者以外の者によって構成された調査委員会等を設置する等、その原因究明について万全を期しているか。 脚注15　（略） **②（略）** **⑵　（略）** **Ⅱ．管理者によるオペレーショナル・リスク等管理態勢の整備・確立状況** **【検証ポイント】** **（略）**	**⑴　分析・評価** **①【オペレーショナル・リスク等管理の分析・評価】** 取締役会等は、監査役監査、内部監査及び外部監査[16]の結果、各種調査結果並びに各部門からの報告等全てのオペレーショナル・リスク等管理の状況に関する情報に基づき、オペレーショナル・リスク等管理の状況を的確に分析し、オペレーショナル・リスク等管理の実効性の評価を行った上で、態勢上の弱点、問題点等改善すべき点の有無及びその内容を適切に検討するとともに、その原因を適切に検証しているか。また、必要な場合には、利害関係者以外の者によって構成された調査委員会等を設置する等、その原因究明について万全を期しているか。 脚注16　（略） **②（略）** **⑵　（略）** **Ⅱ．管理者によるオペレーショナル・リスク等管理態勢の整備・確立状況** **【検証ポイント】** **（略）**

現行	改正後
１．事務リスク管理態勢 **⑴　事務リスク管理部門の管理者の役割・責任** **①～②（略）** **③【事務リスク管理部門の管理者による組織体制の整備】** （ⅰ）～（ⅵ）（略） （ⅶ）事務リスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在する事務リスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[16] 脚注16　（略） **④（略）** **⑵　事務リスク管理部門の役割・責任[17]** **①【事務統括部門の役割・責任】** （ⅰ）～（ⅶ）（略） （ⅷ）事務統括部門は、新規商品等の取扱い、新システムの導入、海外拠点・子会社での業務開始を行う場合には、事務リスクを特定しているか。リスクの特定に当たっては、例えば、商品開発等に関し、既存の各種規程等との整合性について検討を行っているか。これらの検討に当たっては、営業推進部門から不当な影響を受けることなく行っているか。[18]	**１．事務リスク管理態勢** **⑴　事務リスク管理部門の管理者の役割・責任** **①～②（略）** **③【事務リスク管理部門の管理者による組織体制の整備】** （ⅰ）～（ⅵ）（略） （ⅶ）事務リスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在する事務リスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[17] 脚注17　（略） **④（略）** **⑵　事務リスク管理部門の役割・責任[18]** **①【事務統括部門の役割・責任】** （ⅰ）～（ⅶ）（略） （ⅷ）事務統括部門は、新規商品等の取扱い、新システムの導入、海外拠点・子会社での業務開始を行う場合には、事務リスクを特定しているか。リスクの特定に当たっては、例えば、商品開発等に関し、既存の各種規程等との整合性について検討を行っているか。これらの検討に当たっては、営業推進部門から不当な影響を受けることなく行っているか。[19]

現行	改正後
（ix）（略）	（ix）（略）
脚注17　（略）	脚注18　（略）
脚注18　（略）	脚注19　（略）
②（略）	**②（略）**
２．システムリスク管理態勢	**２．システムリスク管理態勢**
⑴　システムリスク管理部門の管理者の役割・責任	**⑴　システムリスク管理部門の管理者の役割・責任**
①【システムリスク管理規程の整備・周知】 システムリスク管理部門の管理者は、システムリスクの所在、種類・特性及び管理手法を十分に理解し、システムリスク管理方針に沿って、リスクの特定、評価及びモニタリングの方法を決定し、これに基づいたリスクのコントロールに関する取決めを明確に定めたシステムリスク管理規程を策定しているか。システムリスク管理規程は、取締役会等の承認を受けた上で、組織内に周知されているか。	**①【システムリスク管理規程の整備・周知】** システムリスク管理部門の管理者は、システムリスクの所在、種類・特性及び管理手法を十分に理解し、システムリスク管理方針に沿って、リスクの特定、評価及びモニタリングの方法を決定し、これに基づいたリスクのコントロール及び削減に関する取決めを明確に定めたシステムリスク管理規程を策定しているか。システムリスク管理規程は、取締役会等の承認を受けた上で、組織内に周知されているか。
②（略）	**②（略）**
③【システムリスク管理部門の管理者による組織体制の整備】	**③【システムリスク管理部門の管理者による組織体制の整備】**
（ⅰ）～（ⅳ）（略）	（ⅰ）～（ⅳ）（略）
（ⅴ）システムリスク管理部門の管理者は、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。	（ⅴ）システムリスク管理部門の管理者は、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。

現行	改正後
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。	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。
（ⅵ）～（ⅶ）（略）	（ⅵ）～（ⅶ）（略）
（ⅷ）システムリスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在するシステムリスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[19]	（ⅷ）システムリスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在するシステムリスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[20]
脚注19　（略）	脚注20　（略）
④（略）	**④（略）**
⑵　システムリスク管理部門の役割・責任	**⑵　システムリスク管理部門の役割・責任**
①【システムリスクの認識・評価】	**①【システムリスクの認識・評価】**
（ⅰ）～（ⅱ）（略）	（ⅰ）～（ⅱ）（略）
（ⅲ）システムリスク管理部門は、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。	（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。
（新設）	（ⅳ）システムリスク管理部門は、例えば１日当たりの処理可能な契約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

現行	改正後
（新設）	するリスクを認識・評価しているか。 （ｖ）システムリスク管理部門は、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。
（ⅳ）（略） （ｖ）システムリスク管理部門は、新規商品等の取扱い、新システムの導入、海外拠点・子会社での業務開始を行う場合には、システムリスクを特定しているか。[20]	（ⅵ）（略） （ⅶ）システムリスク管理部門は、新システムの導入、海外拠点・子会社での業務開始を行う場合には、システムリスクを特定しているか。[21]
脚注20　（略）	脚注21　（略）
②【システムリスクの状況等のモニタリング】 （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、当該保険会社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。 （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評価・判断できる情報を、定期的に又は必要に応じて随時、報告しているか。	**②【システムリスクのモニタリング】** （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、当該保険会社の内部環境（リスク・プロファイル等）や外部環境の状況に照らし、当該保険会社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。 （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評価及び判断できる情報を、定期的に又は必要に応じて随時、報告しているか。
③【コントロール】 （ｉ）システムリスク管理部門は、重要なシステムリスクに係る対応策について、取締役会等が意思決定できる情報を報告しているか。	**③【システムリスクのコントロール及び削減】** （ｉ）システムリスクのコントロール 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

現行	改正後
	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。
（ⅱ）システムリスク管理部門は、システムリスクを削減する対応策を実施する場合、新たなリスクの発生に注意を払っているか。	（ⅱ）システムリスクの削減 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。
④【検証・見直し】 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。	**④【検証・見直し】** システムリスク管理部門は、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。
３．流動性リスク管理態勢	**３．流動性リスク管理態勢**
⑴　流動性リスク管理部門の管理者及び資金繰り管理部門の管理者の役割・責任	**⑴　流動性リスク管理部門の管理者及び資金繰り管理部門の管理者の役割・責任**
①～③（略）	**①～③（略）**
④【流動性リスク管理部門の管理者及び資金繰り管理部門の管理者による組織体制の整備】	**④【流動性リスク管理部門の管理者及び資金繰り管理部門の管理者による組織体制の整備】**
（ⅰ）～（ⅱ）（略）	（ⅰ）～（ⅱ）（略）
（ⅲ）流動性リスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在する流動性リスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[21]	（ⅲ）流動性リスク管理部門の管理者は、新規商品等に関し、統合的リスク管理部門の要請を受けた場合、新規商品等管理方針等に基づき、事前に内在する流動性リスクを特定し、統合的リスク管理部門に報告する態勢を整備しているか。[22]

現行	改正後
（ⅳ）～（ⅶ）（略）	（ⅳ）～（ⅶ）（略）
脚注21　（略）	脚注22　（略）
⑤（略）	**⑤（略）**
⑵　流動性リスク管理部門の役割・責任	**⑵　流動性リスク管理部門の役割・責任**
①【流動性リスクの特定・評価】	**①【流動性リスクの特定・評価】**
（ⅰ）流動性リスクに影響を与える要因の特定	**（ⅰ）流動性リスクに影響を与える要因の特定**
イ．（略）	イ．（略）
ロ．流動性リスク管理部門は、新規商品等の取扱い、新規の商品の購入、新システムの導入、海外拠点・子会社での業務開始を行う場合に、事前に流動性リスクの所在及びその影響を把握しているか。[22]	ロ．流動性リスク管理部門は、新規商品等の取扱い、新規の商品の購入、新システムの導入、海外拠点・子会社での業務開始を行う場合に、事前に流動性リスクの所在及びその影響を把握しているか。[23]
（ⅱ）～（ⅴ）（略）	**（ⅱ）～（ⅴ）（略）**
脚注22　（略）	脚注23　（略）
②～④（略）	**②～④（略）**
⑶　（略）	**⑶　（略）**
Ⅲ．個別の問題点	**Ⅲ．個別の問題点**

現行	改正後
【検証ポイント】 （略） １．（略） ２．システムリスク管理態勢 ⑴　情報セキュリティ管理 ①【セキュリティ管理者等の役割・責任】 （ⅰ）セキュリティ管理者の役割・責任 イ．～ニ．（略） （新設） （ⅱ）～（ⅳ）（略） （新設）	【検証ポイント】 （略） １．（略） ２．システムリスク管理態勢 ⑴　情報セキュリティ管理 ①【セキュリティ管理者等の役割・責任】 （ⅰ）セキュリティ管理者の役割・責任 イ．～ニ．（略） ホ．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。 （ⅱ）～（ⅳ）（略） ②【情報資産の保護】 （ⅰ）保険会社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

現行	改正後
	（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。
②～③（略）	③～④（略）
④【インターネットを利用した取引の管理】	⑤【インターネットを利用した取引の管理】
（新設）	（ⅰ）インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような取引のリスクに見合った適切な認証方式を導入しているか。[24] ・　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

現行	改正後
	・　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　等
（新設）	（ⅱ）インターネット等の通信手段を利用した非対面の取引を行う場合には、例えば、以下のような業務に応じた不正防止策を講じているか。 ・　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保険会社側で検知し、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）顧客からの相談・苦情等を受け付ける態勢を整備しているか。	（（ⅴ）へ変更）
（ⅱ）（略）	（（ⅳ）へ変更）
（ⅲ）（略）	（ⅲ）（略）
（ⅳ）当該保険会社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。

現行	改正後
（ⅴ）～（ⅷ）（略） （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。	（ⅵ）～（ix）（略） （削除）
（新設）	脚注 24　不正アクセスによる顧客口座からの不正出金を防止するための措置を講じている場合（例えば、保険金振り込み金融機関口座（出金先口座）の指定・変更手続きにおいて、顧客口座と名義が異なる出金先口座への指定・変更を認めないこととし、更に転送不要郵便により顧客の住所地に口座指定・変更手続きのための書面を送付するなどにより、顧客口座と名義が異なる出金先口座への振込みを防止する措置を講じている場合）は、取引のリスクに見合った対応がなされているものと考えられる。
（新設）	⑵　**サイバーセキュリティ管理** ①**【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

現行	改正後
	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、セキュリティ対策の向上を図っているか。 **②【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。 **③【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。
⑵　システム企画・開発・運用管理等 **①（略）**	**⑶　システム企画・開発・運用管理等** **①（略）**

現行	改正後
②【システム企画・開発態勢】	**②【システム企画・開発態勢】**
（ⅰ）企画・開発態勢	**（ⅰ）企画・開発態勢**
イ．～ハ．（略）	イ．～ハ．（略）
（新設）	ニ．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。また、システム開発・運用管理に当たっては、十分な予算や人的資源を配分しているか。
ニ．（略）	ホ．（略）
ホ．開発案件の検討・承認ルールが明確になっているか。	ヘ．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。
ヘ．～ト．（略）	ト．～チ．（略）
（ⅱ）～（ⅲ）（略）	**（ⅱ）～（ⅲ）（略）**
（ⅳ）テスト等	**（ⅳ）テスト等**
イ．～ロ．（略）	イ．～ロ．（略）
ハ．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。特に、保険料・配当金等の重要な事項に関するテストには、ユーザー部門が参加し、テスト結果の確認を行っているか。	ハ．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。特に、保険料・配当金等の重要な事項に関するテストには、ユーザー部門が参加し、テスト結果の確認を行っているか。
ニ．（略）	ニ．（略）
（ⅴ）～（ⅵ）（略）	**（ⅴ）～（ⅵ）（略）**
（ⅶ）人材の育成	**（ⅶ）人材の育成**
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。	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

現行	改正後
	術についても、精通した開発要員を養成しているか。
③【システム運用態勢】	**③【システム運用態勢】**
（ⅰ）～（ⅱ）（略）	**（ⅰ）～（ⅱ）（略）**
（ⅲ）本番データ管理	**（ⅲ）本番データ管理**
イ．システム障害対応やシステムテスト等において、本番データを使用する場合の当該データの貸与に係る方針、手続きを明確に定めているか。	イ．システム障害等対応やシステムテスト等において、本番データを使用する場合の当該データの貸与に係る方針、手続きを明確に定めているか。
ロ．～ハ．（略）	ロ．～ハ．（略）
（ⅳ）システム障害の管理	**（ⅳ）システム障害等の管理**
（新設・ロ．より）	イ．顧客や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
（新設）	ロ．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。
（新設）	ハ．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。
（新設）	ニ．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

現行	改正後
	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。
イ．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。また、システム障害の影響の調査や原因の究明を行い、再発防止策を講じているか。 （新設・ニ．より）	ホ．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。また、システム障害等の影響の調査や原因の究明を行い、再発防止策を講じているか。 ヘ．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。 （イ．～ヘ変更）
ロ．顧客や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。 ハ．システム障害の内容の定期的な分析（発生推移、発生原因の分類による傾向分析等）を行い、それに応じた対応策を講じることにより、システム障害の未然防止を図っているか。 ニ．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。 （新設）	ト．システム障害等の内容の定期的な分析（発生推移、発生原因の分類による傾向分析等）を行い、それに応じた対応策を講じることにより、システム障害等の未然防止を図っているか。） （ヘ．～ヘ変更） チ．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。
④【システム監査】 （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。また、必要に応じてシステム監査とシステム以外の監査を連携して行うことができる態勢となっているか。 （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。	**④【システム監査】** （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。また、必要に応じてシステム監査とシステム以外の監査を連携して行うことができる態勢となっているか。 （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

現行	改正後
	査人等による外部監査の活用を行っているか。
（iii）（略）	（iii）（略）
（iv）システムリスクについて、必要に応じ、会計監査人やシステム監査人等による外部監査を受けているか。	（（ii）へ統合）
⑶　防犯・防災・バックアップ・不正利用防止	⑷　防犯・防災・バックアップ・不正利用防止
①～③（略）	**①～③（略）**
④【バックアップ】	**④【バックアップ】**
（i）～（ii）（略）	（i）～（ii）（略）
（新設・（iv）より）	（iii）（略）
（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。	（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）バックアップ取得の周期を文書化しているか。	（（iii）へ変更）
（v）（略）	（v）（略）
⑤【コンティンジェンシー・プランの策定】	**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。	（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。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。
（ii）（略）	（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	（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

現行	改正後
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。	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はなく、保険会社の内部に起因するものや保険会社の外部に起因するものも想定しているか。	（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はなく、保険会社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。また、バッチ処理が大幅に遅延した場合など、十分なリスクシナリオを想定しているか。
（ⅴ）コンティンジェンシー・プランの整備に当たっては、顧客に与える被害等を分析しているか。	（ⅴ）コンティンジェンシー・プランの策定に当たっては、顧客に与える被害等を分析しているか。
(新設)	（ⅵ）コンティンジェンシー・プランは、他の金融機関等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・プランを使用した訓練を定期的に行っているか。また、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。	（ⅶ）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、外部委託先等と合同で、定期的に実施しているか。
⑷　外部委託管理[23]	**⑸　外部委託管理[25]**
①【外部委託業務の管理】	**①【外部委託業務の管理】**
（ⅰ）外部委託業務の計画・実行 システムに係る外部委託業務の計画・実行に当たっては、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、外部委託を行う範囲の決定及びリスク管理の具体策の策定を行っているか。	（ⅰ）外部委託業務の計画・実行 システムに係る外部委託業務（二段階以上の委託を含む。）の計画・実行に当たっては、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、外部委託を行う範囲の決定及びリスク管理の具体策の策定

現行	改正後
	を行っているか。
（ⅱ）外部委託先の選定	（ⅱ）外部委託先の選定
イ．外部委託先の選定に当たり、外部委託先の選定基準を定め、例えば、システムリスク管理の観点から、以下のような点について評価を行っているか。	イ．システムリスク管理部門は、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。
・（略）	・（略）
・（略）	・（略）
・保険会社のレピュテーション等の観点から問題ないか	・保険会社のレピュテーション等の観点[26]から問題ないか
ロ．外部委託した業務及び業者について定期的に評価を行っているか。 なお、外部委託した業務について、業務の内容等に応じ、第三者機関の評価を受けていることが望ましい。	ロ．外部委託した業務（二段階以上の委託を含む。）及び業者について定期的に評価を行っているか。 なお、外部委託した業務について、業務の内容等に応じ、第三者機関の評価を受けていることが望ましい。
（ⅲ）委託契約の内容	（ⅲ）委託契約の内容
イ．外部に委託している業務についてリスク管理が十分できるような態勢（リスクの認識・評価態勢、是正等）を契約等によって構築しているか。	イ．システムリスク管理部門は、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。

現行	改正後
ロ．～ハ．（略）	ロ．～ハ．（略）
（新設）	ニ．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。
（ⅳ）外部委託先のモニタリング	（ⅳ）外部委託先のモニタリング
イ．（略）	イ．（略）
（新設）	ロ．システムリスク管理部門は、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。また、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。
ロ．（略）	ハ．（略）
（新設）	（ⅴ）外部委託先への監査 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。
（ⅴ）問題点の是正 認識された問題点については、外部委託先と連携して速やかに是正しているか。	（ⅵ）問題点の是正 システムリスク管理部門は、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。
脚注23　（略）	脚注25　（略）
（新設）	脚注26　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。
②（略）	**②（略）**

現行	改正後
⑸　（略） ３．～４．（略）	⑸　（略） ３．～４．（略）