コメントの概要及びコメントに対する金融庁の考え方

No.	コメントの概要	金融庁の考え方
１．全般・BCP との違い		
1	規制当局も金融機関も国際的に協調してオペレーショナル・レジリエンス体制の確立に取り組むことにより、個社にとっても金融業界全体にとっても大きな利益になると考える。 日本においても、規制当局や金融機関が国際的に連携して標準的なオペレーショナル・レジリエンスに求められるスタンダードを整備していくべきだと考えるが、如何お考えか。	国際的な協調が重要であることはご指摘の通りであり、引き続き、様々な形で国際的に連携を図って参ります。
2	「チェックリストの適用といった形式的な手法は用いない。・・・サーベイの実施や経営陣等との対話を通して足もとの取組状況や問題意識を丁寧に把握し、国際的な議論の進展も見据えつつ更なる取組を進めていく上での課題を特定していく」とあるが、具体的にどのように調査・課題特定するのか。	DP に記載のとおり、サーベイや様々なレベルでの意見交換を通じた課題の特定を想定しており、その効果的な実施方法は今後検討を進めて参ります。
3	検査・監督において、「本文書の個々の論点を形式的に適用したり、チェックリストとして用いたりするものではない」とあるが、本文および参考事例をもとにオペレジの対応をしても不十分となるのか。	オペレジは、金融機関に対して画一的な基準を課す趣旨ではなく、金融機関の規模・リスク選好度・金融システムへの影響に応じた、比例原則に基づく対応を想定しております。 すなわち、各金融機関における対応が十分か否かは一定の幅を持って捉える必要があり、DP 本文や BOX の参考事例を全ての金融機関に形式的にあてはめることは想定しておりません。 なお、今後、好事例集の公表などを通じて、より良い実務の構築に向けた参考資料を提供することを検討しております。

4	オペレジに関して預取機関以外の金融機関においても重要であることに異論はないが、本ディスカッション・ペーパーの内容は、預取機関以外の金融機関と対話するには水準が高すぎると考える（決済機能を担う預取機関とそれ以外の金融機関ではIT投資の額等も異なることや、P.4に「主として銀行を対象としている」、「意見交換 を行うにあたっては、金融機関が提供しているサービスの金融システムにおける重要度・市場シェア・利用者への影響等、その規模・特性に応じて、オペレジ確保に必要な対応や経営資源（ヒト・モノ・カネ）は異なることを十分に踏まえた議論を行う」と書かれていることを考慮）。	各業態及び金融機関の提供するサービスが金融システムや国民生活に与える影響は様々であり、したがって、ステークホルダーに許容される耐性度や、オペレジ確保に必要な経営資源も異なります。こうした差異や比例原則を踏まえつつ、オペレジ確保に向けた対話を行って参ります。
5	「オールハザード型BCP」について、重要業務は「いかなる環境下でも遂行する」ことを前提としてBCP 態勢を組んでいる場合、これは「オールハザード」であると理解してよいか確認したい。「オールハザード」にその他の含意があれば、示していただきたい。	「従来型BCP」と「オールハザード型BCP」の相違点は、アプローチの方向性にあると考えられます。前者は、地震や感染症の蔓延といった特定の事象を想定したうえで、当該事象から生じる影響に着目して業務継続を考えます。出発点は原因となる特定の事象です。 一方、後者は特定の事象を想定せず、経営資源の毀損という結果を出発点に業務継続を考えるものです。オペレジは、想定外の事象により、業務が途絶することを前提としており、後者の考え方に近いことをDPでお示ししています。
6	ITBCPやサイバーBCPの考え方が多く取り入れられており、オペレジはその発展形と認識している。今後、具体的な取組み事例について、業界別にまとめて共有いただけると金融機関として取り組みやすくなると考える。	今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。

7	BCP とオペレジの関係性については BOX3 で解説いただいているが、事業継続マネジメントシステムとオペレジの関係性についても触れていただきたい。同システムとオペレーショナル・レジリエンスの関係性・対比が一覧で理解できる表が DP に掲載されると、金融機関にとって理解が進むと考える。	事業継続マネジメントシステム、あるいは、BCM は、BCP の策定や導入、運用、見直しを含む業務継続のための枠組みであり、監督指針においても、その構築を求めています。 オペレジの確保にあたっては、BCM を含めた既存の危機管理の枠組みを活用しつつ、その実効性を確保することが求められます。図表２に記載のとおり、BCP の見直しの際に、重要な業務の耐性度での提供に必要な経営資源が特定され、実際に投資されているか、といったリソース配分の実効性にまで踏み込む必要があります。また、経営資源は社外のサードパーティも含まれますので、サードパーティリスク管理も重要になります。 このほか、既存の BCM を補強する要素として DP で強調しているポイントとしては、図表２に記載のとおり、利用者目線で重要な業務や耐性度を設定すること、業務プロセス全体の合理化にもつながりうること、リソース配分の実効性を確保するためには経営陣のコミットメントが不可欠であること、適切性の検証と追加対応にあたっては、追加投資だけでなく、必要に応じて、IT 人材を採用・確保しやすくする人事制度や風通しの良い企業文化といった、長期的なガバナンスの改善に関する事項も含まれることが挙げられます。
8	サプライチェーン（海外子会社、外部委託先など）におけるサイバーリスクの具体例や、それに対する金融機関側の管理状況・好取組事例も詳しく取り上げていただきたい。	サプライチェーンにおけるサイバーリスクの具体例としては、外部委託先におけるランサムウェアの感染などが考えられます。 今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。

9	図表 2 の 6 つ目に「国際的なコンプライアンス認証の取得」を入れ、ISO/IEC27000 シリーズ、SOC 報告書などの内部統制書や、NIST SP 800 や FedRAMP、APRA 基準、FISC 基準等のサイバーセキュリティや金融に関わるコンプライアンス認証の取得や、取得や更新に係る人材の確保・トレーニング等に関する記述を追加願いたい。	貴重なご意見として承ります。ご指摘の図表は、金融機関が抱える諸課題がオペレジの確保に係る取組みを経て、どのように改善するかをお示ししているものです。「国際的なコンプライアンス認証の取得」は、レジリエンス確保の手段として有用である可能性があり、SOC 報告書などは後段の BOX にて言及しているところです。
10	図表 2 の 7 つ目に「最新事例へのキャッチアップとイノベーション」を入れ、常に最新の技術やビジネスケースについて学び続け（アップデートし続け）ることで、レジリエンスを強化するのみならず、新たなビジネスの創出にも寄与するものと考える。	貴重なご意見として承ります。 なお、「最新事例へのキャッチアップとイノベーション」は、オペレジに限らず、様々な分野で有用な視点であると考えられます。
11	サイバーセキュリティ事故やヒューマンエラーが起こる前提である「ゼロトラスト」の考え方を取り入れ、業務プロセス・オペレーション（何かが起きたときの対応を組織としてどう行うか）を組み直す旨記述すると良いかと思われる。	ゼロトラストはセキュリティ上重要な概念であり、金融庁としても、例えば以下の外部委託調査を実施し、報告書を公表しています。 「ゼロトラストの現状調査と事例分析に関する調査報告書」（金融庁ウェブサイト）： https://www.fsa.go.jp/common/about/research/20210630.html
12	「不測の事態」が起きた場合に、サービス提供途絶の影響を極力一定の範囲内に収めることは難しく、実際にはサービス復帰の早急化を図る「レジリエンス」や起きた場合の代替手段である「バックアップ計画」を準備しておくことが肝要であると思われる。	耐性度は、どれだけ早期に復旧するかという RTO（目標復旧時間）の形で設定することが一般的と考えられますが、業務中断の影響を軽減するためには、これに限ることなく、ご指摘のような代替手段も考慮することが重要です。
13	従前の BCP とオペレジ（包括的な枠組み）の「比較対象表」を作成し、その違いが何であるのか示した方が良いかと思われる。	従前の BCP やリスク管理の課題と、オペレジに期待される効果は図表２をご参照ください。とりわけ、サードパーティリスク管理を含めたリソース管理の実効性、経営陣のコミットメント、業務プロ

		セスの合理化、企業文化は、従前の BCP だけでは対応が不十分になりやすい項目であると考えられます。
14	本ペーパーにて特に新しいことの記載はない認識で、既にオペレーショナル・レジリエンス（＝危機管理）を実装できている金融機関では、2011 年東北の震災以後、従来までのシナリオベースに依存した原因事象型の BCM から結果事象型の BCM へ変更しているといった認識。その結果、事象型 BCM を危機管理へ応用し、想定外シナリオにも対応できるよう、”どの経営資源に影響があるのか”という観点で普段から準備と定期的な演習に取り組んでいる。原因事象型 BCM の時代に比べてより BIA（事業影響度分析）が重視されてきている環境下、なぜ BIA にきちんとふれないのか、違和感がある。	ご指摘を踏まえて、BIA（事業影響度分析）や結果事象型 BCM について追記致しました。
15	BIA 事業影響度分析の記載を明記すればよいが、結果事象の説明の際に明記していないのはおかしい。	
16	オールハザード型 BCP という経団連が最近用いた用語を使う必要はないのではないか。結果事象型で話は整理可能である。	
２．「重要な業務」の特定		
17	「外部環境（金融システムへの影響、市場シェア、利用者数、利用頻度）や自社の規模等の変化に応じて、重要な業務や耐性度も見直しの対象となる」とあるが、どの程度で「変化あり」と判断して見直しをしなければならないのか。	重要な業務や耐性度については、外部環境や自社の規模等の変化に応じて変わり得るものであることから、その十分性・適切性等については定期的に見直す必要があります。見直しを要する具体的な基準を示すことは想定しておらず、金融システムの安定と利用者保護の観点から、各金融機関において検討することが求められます。

18	金融業界における「重要な業務」の捉え方は、各々の業界毎に一定揃っていることが望ましいと考える。高い目線での定義は本 DP で示され、また、預取機関については具体的な事例も示されているが、預取機関以外の業界における「重要業務」について、具体的な内容を業界ごとにレベリングするために、追加情報を提供する予定はあるか確認したい。	オペレジ上の重要な業務の特定においては、各金融機関が自らの裁量で、その中断が金融システムの安定や利用者の日常生活に著しい悪影響を生じさせるおそれのある金融サービスを特定する必要があります。 そのため、金融庁から業態ごとに詳細な重要な業務の具体例を示す予定はありませんが、好事例集の公表などを通じて、金融機関による取組みを促進することを検討しております。
３．「耐性度」の設定		
19	耐性度というような新しい用語を持ち出す必要はなく、RTO（目標復旧時間）、RPO、最大許容停止時間 MTPD、最小事業継続水準 MBCO などを明記した方が良い。	耐性度は、バーゼル銀行監督委員会の策定する国際原則に規定された「Tolerance for Disruption」の概念を踏まえた表現です。 明確化のため、BCM（業務継続体制）の用語との関係性について追記致しました。 なお、耐性度は、典型的には BCP（業務継続計画）において設定する業務中断時の RTO（目標復旧時間）と重なりますが、それ以外にも、金融システムへの影響や利用者目線で生活への影響を一定の範囲内に収める観点から、業務中断が生じる範囲、影響を受ける取引数、取引額及び利用者数（例えば、業務中断時の利用者からの苦情数）なども考慮要素となり得るものであり、これらを踏まえ、各金融機関が柔軟に設定することを想定しております。

20	「・・・リスク選考度（リスクアペタイト）を設定した上で、・・・業務中断が必ず生じることを前提に最低限維持すべき水準を「耐性度」として設定する必要がある」とあるが、リスクアペタイトと耐性度について、具体的にどのような貌で整理することを想定しているのか例示頂きたい。	一般に、金融機関は、「どの程度の業務中断を受容し、業務中断を一定程度におさめるためにどの程度投資するか」といった方針を定めた上で、重要な業務の耐性度を設定しているものと理解しています。 例えば、コスト（例：物理施設の立地戦略・耐震性能の高い施設への移転、回線やデータセンタの冗長構成の確保、営業含めたオペレーションのデジタル化・省人化、コンプライアンスや企業文化に関する研修等）をかければかけるほど耐性度を強化することができ、業務中断時の早期復旧の可能性も高くなりますが、その分だけ高価格のサービスになってしまうというトレードオフがある中、利用者目線でみたより好ましいコストや利便性のバランスに関して自社の戦略を定めることは「リスク選好度の設定」の一例であると考えられます。 必ずしも、重要な業務ごとにリスク選好度を設定することが必要な訳ではありません。
21	「最低限維持すべき水準（耐性度）」は「業務中断が生じる範囲、影響を受ける取引数、取引額及び利用者数」から具体的にどう判断するのか。	例えば、「業務中断が生じる範囲、影響を受ける取引数、取引額及び利用者数」等を考慮したうえでRTO（目標復旧時間）を耐性度として設定するといった方法も考えられますが、これに限ることはなく、各金融機関が柔軟に耐性度を設定することを想定しております。オペレジ確保に向けては各金融機関の様々な取組みが考えられるため、今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。

22	Tolerance for disruption は「自社オペレーションの業務中断（disruption)」について、最低限維持すべき水準を各金融機関が自ら設定する（許容する）ものであることを踏まえると、「許容度」もしくは「許容水準」と和訳するのが適切ではないか。「耐性」という言葉を使うと、ビジネス環境や内部実態からして所与のものであるという印象があり、あえて英語に訳し戻す場合、「Tolerance to disruption （中断に対する耐性)」に近いニュアンスがあると考える。また、P.3 に示されている課題の一つであるゼロリスク志向からの意識改革を図るという意味でも、「許容」という言葉を使うことに一定の意味はあると考える。	Tolerance には、許容、寛容、耐性と様々なニュアンスがあり、金融機関の社内用語として、途絶許容度、許容水準、といった用語を使用していただくことも差し支えありません。また、ゼロリスク志向からの意識改革を図ることも、重要と考えられます。 その上で、DP において耐性度という訳語を用いた趣旨は、「どの程度の業務中断を受容し、業務中断を一定程度におさめるためにどの程度投資するか（どの程度の耐性を構築するか)」に関する金融機関の意思決定に着目しているためです。
23	「迅速な代替手段の案内や広報もまた重要」とあるが、耐性度の設定というのは、復旧目標時間の設定のように、案内や公表までの時間設定をすることなのか。	自社の提供する重要な業務が中断してしまった際、利用者のニーズを満たし得る別のサービス（他社のサービスも含む）に案内することで、利用者への影響を低減させることもオペレジの確保に係る取組みとして重要であり、こうした点も耐性度設定の考慮要素となると考えられます。 例えば、自社の ATM が障害により停止した際、ウェブサイト、SNS、モバイルアプリによる通知やコールセンターでの回答等の手段を通じ、自社のインターネットバンキングや他社の ATM へ案内することで、利用者の資金決済ニーズを一定程度充足できる可能性があります。自社サービスの目標復旧時間に加え、代替手段及びそれらが利用者への影響をどの程度低減するかを総合的に勘案し、耐性度を設定することが想定されます。
24	ここでいう、“迅速な代替手段”とは具体的に何が考えられるか。また、ここで必要なのは一般的な「広報」より、広くあまねく利用者に対して現状のアップデートと回復・復旧までの見通しを示す「通知・お知らせ」であると考える。	

25	「耐性度」について、各々の業界特性に照らして、各々の業界毎に一定の目線が揃っていることが望ましいと考える。預取機関以外の業界において、具体的な内容を業界ごとにレベリングするために、追加情報を提供する予定はあるか確認したい。予定がない場合、保険会社については業務の重要度に応じて柔軟に定めることでよいか確認したい。	重要な業務の耐性度は、一義的には各金融機関と利用者とのリスクコミュニケーションを通じて、各金融機関が自らの裁量で決定するものです。金融庁から業態ごとに詳細な耐性度の目線を示す予定はありませんが、好事例集の公表などを通して、金融機関による取組みを促進することを検討しております。 なお、重要な業務の耐性度の適切性は自ら検証する必要があり、経営陣はその適切性については監督当局含めたステークホルダーに対して説明責任を果たすことが必要となります。
26	「既存の BCP の復旧目標時間については、（～中略～）こうした既存の枠組を活用することは有益である。」について、銀行が対象であることを本文中に明示いただきたい。	脚注に、当該箇所の出典である「主要行等向けの総合的な監督指針」を掲載しており、本記載は銀行を対象としたものであることが明らかであると考えられます。
27	耐性度の設定や相互関連性のマッピングなど、最善策として非常に参考になるが、全域に適用を要求された場合、消化不良を起こして、却って取組みが遅れる懸念がある。相互関連性のマッピング手法は国際的にもベストプラクティスを探求している段階であり、適用において柔軟性が許容されていること、現時点では画一的な正解のない中長期的な取組みであることを確認したい。	オペレジは、金融機関に対して画一的な基準を課す趣旨ではなく、金融機関の規模・リスク選好度・金融システムへの影響に応じた、比例原則に基づく対応を想定しており、今後のスケジュールについても、実務的なフィージビリティも踏まえて検討して参ります。
４．相互連関性のマッピング・必要な経営資源の確保		
28	オペレジの基本動作１から４の内、「３ 社内外の業務プロセスの相互連関性をマッピングし、必要な経営資源(ヒト・モノ・カネ)を確保」とあるが、相互連関性のマッピングを通じて経営資源を把握することは可能である一方、特定・確保まで繋げることは難しいと考えられる。実務的な対応としては、シナリオテストを通じて重要	相互連関性のマッピングは、重要な業務を最低限維持すべき水準（耐性度）で遂行するにあたり必要な社内外の経営資源（ヒト・モノ・カネ）を特定できる粒度のものである必要があります。 したがって、ご指摘のように、マッピングのみでは不十分であり、

	業務に内在するリスク・脆弱性に係る検証を行い、その結果を踏まえ配分すべき経営資源を検討し、特定・確保するプロセスが考えられる。当該箇所における経営資源の特定・確保について、想定されている対応をご教示頂きたい。	その結果を踏まえ、人的資源の採用・育成・配置、施設やITシステムへの投資、そのための予算配分など、その確保のための具体的な行動が必要となります。更に、必要な経営資源の特定自体が適切だったか、十分な経営資源が確保されているかについて、特定のリスクシナリオを前提にした分析や訓練を通じて定期的に検証し、それを踏まえ、必要に応じて見直しや追加的措置を講じることが期待されます。 このように、マッピングを必要な経営資源の確保に繋げるには、経営陣がその十分性や適切性を監督当局含めたステークホルダーに対して説明責任を果たすなど、経営陣のコミットメントが重要と考えられます。 なお、マッピングの範囲・粒度は、金融庁が具体的な目線を示すのではなく、経営資源を特定するために必要な程度となるよう、各金融機関において判断するものとなります。
29	IT ベンダー等、サードパーティー・フォースパーティに関する経営資源について把握することは容易ではない。社内外の経営資源の相互関連性をどの程度までマッピングすべきかについては、業態ごとの特性や、費用対効果及び実効可能性の観点も考慮に入れて検討いただきたい。	
30	相互関連性のマッピングの手法およびその範囲や粒度について、現状は探求の段階とあるが、運営時には具体的に示していただくことが有益なマッピングの作成につながると思料。	今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。
31	「銀行の IT システムにおいては、（～中略～）こうした自社システム内のモジュール間の相互依存度を把握することは不可欠である」との記載があるが、できる限り具体的な好取組事例の提供を検討いただきたい。	

32	経営資源は「ヒト・モノ・カネ」以外にも、情報、時間、知的財産、技術力、イノベーション力、ブランド、信用、ネットワーク等も存在するほか、本稿では「レジリエンス」も入れたほうが良いと考える（ヒト・モノ・カネの伝統的な考え方に縛られない）。	貴重なご意見として承ります。ご指摘のとおり、重要な業務の提供に必要であれば、経営資源は「ヒト・モノ・カネ」以外も含まれ得る概念と考えられます。
33	金融機関のITシステムは複雑な要素や様々なサードパーティサービスの集合体から成り立っていることから、①頭取（社長）、役員、各部署の責任者を含めた経営陣が、各系統のシステム構成、利用中のサードパーティサービス、そのメリットとデメリット（リスク）、コスト、契約期間、社員のスキルレベル、コンプライアンス認証取得・更新の状況などを把握し、②「想定外」の事態が起きた際の組織としての対応を準備しておくと良いと考える。	オペレジの確保に係る取組みでは、お示し頂きました経営陣の関与は重要なポイントと考えております。オペレジの確保に係る取組みでは、トップを含めた経営陣が重要な業務を耐性度内で継続するために必要な経営資源を確保し、その十分性、適切性をステークホルダーに対して説明できることが、経営陣のコミットメントを実効的なものにするうえで重要です。また、危機時の対応について BCP 訓練を通じて習熟する際にも経営陣がどれだけ深く関与するかが肝要になると考えられます。
34	金融機関のオペレーションに係る内外（特に外部）の関係者の「ステークホルダーマップ」を作成し、彼らとどの様なコミュニケーションを平時及び緊急時に取るのか、常に議論・準備しておくことが肝要と考える。	ご指摘のとおり、関係者間の迅速な情報共有のために緊急時の連絡先一覧を作成し、コミュニケーション経路を整備することは重要であると考えられます。
35	自社の経営資源の欠如については、一般的に監査などの形で外部からの指摘からにより、初めて実感・理解すると考えられるところ（自ら「経営資源の欠如」について第三者的な目で判断することは困難であると考える）、例えば国際的なコンプライアンス認証の取得を金融機関に求めることで、これら認証を取得するのに現時点で何が足りないかを理解することに繋がるものと思われる。	金融機関が自社の経営資源の十分性や適切性を検証するにあたり、第三者による認証を判断材料の一つとすることも考えられます。もっとも、何を重要な業務として特定し、どこまでを耐性度として設定するかは、各金融機関より異なるため、必要な経営資源の質・量は様々であることが想定されます。このため、金融機関に一律の対応を求めるのではなく、各金融機関の実態に即し、必要な経営資源が実質的に確保されることが重要と考えられます。

36	人事体制をよりフラットなものにする、人事評価を明確なものにする、特定の要件や技術に対する専門家集団（例：Center of Excellence; COE）を立ち上げる、そして社員の働き方を柔軟にする（リモート環境の整備、柔軟な勤務時間等）などのIT人材内製化に向けた「基礎」を構築することが大事であるかと思われる。 また、デジタル・IT部門及び担当役員だけではなく経営陣がデジタル活用の有用性とこれに伴うリスク管理の重要性を把握、理解する上で外部団体等が提供しているトレーニングコンテンツの活用も一考に値するかと思われる。	各金融機関が、自社でIT人材を育成し、システム開発の内製化を推進する上では、ご紹介頂いた取組みやコンテンツは参考になると考えられます。 各金融機関におけるオペレジ確保に向けた取組みにおいては様々な実務が考えられますので、今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。
５．サードパーティリスク管理・サードパーティ集中リスクへの対応		
37	クラウドサービスに対する安全対策において、セキュリティ対策や脆弱性改善への対応等をクラウドサービス事業者に適時ヒアリングしているが、一部の事業者からは明確な回答を得られないケースもある。その場合、金融機関は、当該クラウドサービスが外部の評価制度で一定以上の評価を得ていることをもって、安全性を評価することが考えられる。利用し得る外部の評価制度の１つとして、「政府情報システムのためのセキュリティ評価制度（ISMAP）」がある。ISMAPに登録されたクラウドサービスであれば、政府が求める高いセキュリティ要求を満たしており、それが当行の基準とマッチしていれば、安全性が高いと考えられる。一方で、現状、ISMAPに登録されているクラウドサービスが限定的となっている。今後、政府がISMAPへの登録および利活用を促進することが、ク	ご指摘を踏まえて、文言を修正致しました。

	ラウドサービス事業者のセキュリティ対策の向上にも、金融機関のオペレジの強化にもつながると考えられる。上記を踏まえ、以下の修文案のとおり、ISMAP の利活用の記述を追記することも一案ではないか。 ＜BOX６修文案＞ 「なお 、 個別金融機関がそれぞれ監査する非効率性を解消するために、外部監査により一括してモニタリングする方法としては、クラウドを含む委託業務の内部統制を対象とした SOC（Service Organization Control）報告書の利用や、監査対象が SaaS である場合には「政府情報システムのためのセキュリティ評価制度（ISMAP)」への登録状況も参考情報として利用される例も聞かれる。」	
38	「金融機関が重要なサードパーティ等の利用状況について定期的に監督当局に報告・情報共有」について、業態に応じた必要性の検証を行ったうえで、業務負荷の軽減・事業者間の公平性の確保に努めていただきたい。	重要なサードパーティの利用状況に関する報告制度については検討中です。 また、重要なサードパーティへの監督については、国際的な議論も踏まえながら、検討を進めて参ります。
39	重要なサードパーティに関し、以下の点についてご検討いただきたい。 ・重要なサードパーティの定義について明確化していただきたい。 ・日銀、取引所、ほふり、清算機関などのインターバンクおよび証券インフラ機関のみならず、回線事業者（NTT コム、KDDI 等）や時価配信業者（Bloomberg、Reuters、Quick 等）など、事業者が利用	重要なサードパーティとは、重要な業務を最低限必要な水準（耐性度）で遂行するにあたり、必要不可欠なサードパーティをいいます。 その具体的な対象は、各金融機関の設定した重要業務及び耐性度により決せられることになり、一律に特定のサードパーティが含まれるか否かを示すことは困難です。

	する共通インフラ機関をどう取り扱うべきか、方針を示していただきたい。 ・例えば重要なサードパーティを含めた訓練の実施等について、金融機関が個別に対応することは限界があると考えられることから、重要なサードパーティの監督について海外で検討されている監督当局による直接監督なども含め、有効で実現可能な手法について検討いただきたい。	具体例としては、IT ベンダー、FinTech 企業、金融市場インフラ、警備保障、通信、電力などが挙げられますが、取引所や時価配信業者が該当する可能性もあります。 重要なサードパーティへの監督については、国際的な議論も踏まえながら、検討を進めて参ります。
40	「・・・監督当局が特定のサードパーティに対する集中リスクを把握した上で、・・・」とあるが、特定のサードパーティに焦点を当てた場合であっても、集中リスクを集計する為の切り口は複数考えられる（契約数・金額規模等）。当局として、足許検討している切り口や粒度等、具体的な対応や基準があればご教示頂きたい。	サードパーティに対する集中リスクへの対応については、国際的な議論も踏まえながら、検討を進めて参ります。
41	サードパーティについてのリスク管理について、多くの金融機関が特定のサードパーティにサービス提供を依頼している場合も存在する。 そのような場合に、金融機関が共同でリスク管理を導入することも許容されるのか。	金融機関が共同でサードパーティリスク管理を行うことは、既に監査の共同実施という形では実施されております。もっとも、金融機関においては「他社がチェックしているのだから自社のチェックは不要」と考えることなく、共同で行われるリスク管理の実効性について確認する必要があります。
42	クラウドサービスプロバイダー（CSP）に限らず、監督当局が金融機関の重要なサードパーティと日常的に様々なトピックに関して、対話・会話を行ったり、当該サードパーティが主催するイベント等に参加したりすることで、平常時からの関係構築や情報収集を行うことが、金融システム全体のレジリエンス向上に資すると思われる。	ご認識のとおりと考えられます。

43	ここでいう「不芳情報」とは、具体的に何を指すのかご教示頂ければ幸い。	「不芳情報」とは当該サードパーティに関するネガティブ・ニュースを指しております。例えば、「主要行等向けの総合的な監督指針」において、外部委託を行う際の着眼点として、委託先が情報の漏洩や滅失、毀損を防止するために必要な措置を講じていることを掲げておりますが、過去の情報漏洩は不芳情報に該当し得ます。
44	「大手クラウド事業者に対しては・・・業務中断時に適時・詳細な情報開示に応じてもらうことが・・・難しい」とあり、続けて「声も聞かれている」と記述されているが、イメージ・印象ではなく、具体的な事例についてご教示頂ければ幸い。	左記の記載は金融機関から聴取した情報を踏まえたものであり、日本だけでなく海外の法域からも同様の問題意識を聴取しております。 具体的には、クラウド事業者との契約は、システム開発や保守をシステムインテグレーターに委託する際の請負契約や準委任契約と比較すると、業務中断時の適時・詳細な情報共有に課題があると聴取しております。
45	現状、勘定系のインフラにクラウドを利用している金融機関は数えるほどしかなく、一つのクラウドに利用が集中するリスクは存在していないと考える。また、仮にその様なリスクが存在するとしたら、それを避けるために「マルチクラウド」の導入を監督当局は薦める（進める）べきと考える。	IT システムの利用においては、様々なレイヤーの冗長性を考慮することが重要であり、クラウド事業者（クラウドサービスプロバイダ）単位の冗長性を考慮すると、「マルチクラウド」の採用も選択肢となり得ると考えられます。 一方で、「マルチクラウド」の採用については、各クラウド事業者が提供するクラウドサービスが一律のものでないこと、それぞれのサービスに精通した専門人材が必要であること、それぞれのサービスに適したシステム（あるいは可搬性の高いシステム）を構築する必要があること等、コスト面での課題もあると承知しており、これら両側面を踏まえた上で、各金融機関において検討するもの
46	危機時に IT システムが止まった場合、とありますが、例えばクラウドサービスの利用においては、一つの CSP に依存するのではなく、利便性と効率性、BCP の観点も含め、「マルチクラウド」（複数のクラウドサービスを同時に利用する）の導入を考慮すると良いと考える（当然スキルやコストメリット等を考慮する必要があると思われる）。	

47	「マルチクラウド」が困難である旨“聞かれている”とのことですが、クラウドサービス利用に係る技術的トレーニングや支援体制を規制当局として CSP と協力しながら作成・実施することが肝要と考える。	と考えられます。
48	監査の効率性という観点では、海外金融機関ではクラウド上で実行されているシステムの自動監査、リアルタイム監査への取り組みが行われており、国内金融機関でも検討する余地があると考える。このような取り組みを行うためには、監査人のクラウドや自動化に対応するスキルが重要になってくると思われる。	貴重なご意見として承ります。
49	日本国内の一定地域に IT システムのリソースが集中するリスクを避けるために、日本と基本的な価値観を共有する海外の国にその一部を置くという考え方もあるかと思われる。	貴重なご意見として承ります。
50	金融機関の冗長構成について記述されているが、クラウドを利用する場合、「マルチリージョン」及び「マルチクラウド」の採用、また足回り回線も冗長化を図る必要があると考える。	貴重なご意見として承ります。
51	第三者機関が日常的な「牽制」を図る事例、と記述されているが、より重要なのは「平時からのコミュニケーション」であると考える。また当該「第三者機関」が銀行 OB・研究者・セキュリティコンサルタントで構成されている旨記述されているが、それら「専門家」の専門性を担保する資格や業務経験を明確化すべき、とも考える。	貴重なご意見として承ります。
52	「第三者機関」について、当該組織の能力・経験・ビジネス志向等を踏まえながら、一定の資格（第三者機関適合）を与えるような予	現時点では、金融庁がこれら「第三者機関」に何らかの資格を付与することは想定しておりません。

	定はあるか確認したい（各金融機関は、適合した組織に対して監査を委託することになるのではと思料）。	
53	まさに貴庁が仰っている、対話を通じて民間のステークホルダーと共にベストプラクティスを探求する、というアプローチが“正解が見えない回答を探す”のに最適な方法であると思われる。また、技術の進展やビジネスモデルの変化は常に起きていることから、「ベストプラクティス」は常に変化しているものと理解している。	貴重なご意見として承ります。
６．適切性の検証・追加対応		
54	「極端だが起こり得る想定外の事象の発生を想定して機能度を検証することが求められる」との記載があるが、検証は必要だと思う一方で、極端な事例を出せばキリがないため、ある程度の蓋然性の設定は必要ではないかと考える。	適切性の検証においては、従来型の BCP と同様に特定の事象を想定したリスクシナリオを策定の上、影響を評価することを想定しております。リスクシナリオとしては、自然災害、システム障害、サイバー攻撃、地政学リスクなど様々なものが考えられますが、それぞれのリスクシナリオにおいて、ヒト、モノ（施設、システム）及びその両方にどの程度極端な被害を見積もるかは、その蓋然性を含め、各金融機関において柔軟に設定することを想定しております。
55	ここでいう“想定外の事象”とは具体的に何を想定しているかご教示願いたい。	ご指摘頂いた箇所は、特定のリスク事象を前提としたリスク対応策では、想定外のリスク事象が発生した際に業務の継続性を確保できない、ということを述べているものです。例えば、従来型の BCP の枠組みに基づく地震や新型インフルエンザが発生した場合を想定した対応計画では、それ以外の事象（例えばサイバー攻撃）による業務中断が生じた場合に対応が困難となる可能性があるということを指しています。

56	BCP で想定されるリスクシナリオにおいて、システム障害、テロやサイバー攻撃、感染症、自然災害に加え、「戦争」、「システム従事者による内部からの攻撃」等を加えるのも一案と思われる。	貴重なご意見として承ります。ご指摘の箇所は、リスク事象として代表的なものを列挙しており、その他の事象を排除するものではありません。
57	BCP で想定されるリスクシナリオにおいて、サイバー攻撃によるシステム停止を入れるべきほか、「コンピューター事故」については「システム障害」という用語の方が適切ではないかと思われる。	ご指摘の箇所は、金融庁「主要行等向けの総合的な監督指針」からの引用となりますので、該当箇所をご参照ください。一般に、サイバー攻撃は対企業犯罪や外部不正の一類型であり、システム障害はコンピュータ事故と同義であると考えられます。 用語については修正致しました。
58	BCP で想定されるリスクシナリオにおいて、営業上、人事上、労務上のトラブルにおいてもオペレジでの対応が必要か。	ご指摘頂いた箇所は、金融庁「主要行等向けの総合的な監督指針」からの引用となりますので、該当箇所をご参照ください。 オペレジ上の重要な業務等の検討を進める上で、BCP 等の既存の枠組みを活用することは有益であると考えられます。
59	PDCA サイクルは 1950 年代にその起源を遡る伝統的なアプローチであり、21 世紀のデジタル化のニーズに合致しているかは不明（Plan と Do で終わってしまう旨も指摘されている）。 各金融機関の特性や展開しているビジネスラインの違いにより、OODA（Observe, Orient, Decide, and Action）、STPD（See, Think, Plan, Do）、DCAP（Do, Check, Action, Plan；PDCA の順番を変更）の個別採用や他との組合せを行うほか、シリコンバレーで目標設定とその実行アイテムを結果として測る OKR （Objective, Key Results）などの採用等を考慮しても良いかと思われる。	貴重なご意見として承ります。ご指摘の通り、定期的にプロセスを検証する枠組みとしては様々なものがある中、PDCA サイクルが最も浸透している概念と考え、DP では PDCA サイクルによる検証を要請しているところです。ただし、PDCA 以外の手法についても、オペレジ確保にあたり有益な枠組みがあれば、好事例集などの形で各金融機関へ還元して参ります。
60	人事制度や企業文化の見直しについてもオペレジで対応が求められることとなるのか。	オペレジの実効性確保には、必要な人的資源確保のための人事制度の構築やリスク管理文化の醸成も重要な要素の１つと考えられ

		ます。これらについても、今後、好事例集をより良い実務の構築に向けた参考資料として公表することを検討しております。
61	異なる価値観・専門性・バックグラウンドを持つ人員・組織同士がぶつかり合い・・・、との記述があるが、「ぶつかる」のではなく、互いの違い（多様性）を「認め合い」、「協業（コラボレーション）」することが出来る環境を意識的に作り上げることが重要であると考える。理由として、技術の著しい発展やビジネス環境の急激な変化が起き続ける環境下では、様々なバックグラウンドや考え方を持った多様な人材が自由に意見交換を行い、新たなサービスを立ち上げたり、現状の問題を解決したりすることが、「正解のない回答」を導くための最適な方法と思料。	ご指摘のとおり、多様性の「認め合い」や「協業」の姿勢は、心理的安全性の観点でも重要と考えております。ご指摘を踏まえ、文言を修正致しました。
62	インシデントや懸念、内部不正の疑いに関しては、報告・検証・解決を行う組織体制を平時から構築することが重要で、特定の個人にその責任を帰着させること自体が誤っていると考える。	貴重なご意見として承ります。
63	1:1 ミーティングはあくまでもマネージメントの 1 手法に過ぎず、またマネージャー自身のコミュニケーションスキルが一定レベルに達している必要がある。よって、社員に対するトレーニングやワークショップを継続的に行い、「心理的安全性」が担保される組織を作り上げることが重要であると思われる。	貴重なご意見として承ります。DP にも記載のとおり、心理的安全性の確保するための手法は様々あり、一例として「1on1 ミーティング」を例示しましたが、マネージャー自身のコミュニケーションスキル不足によって形骸化するおそれもあります。このほか、DP では「2on2 ミーティング」や「トライアローグ」といったコミュニケーション手法も例示しておりますが、いずれの手法であっても形式的に導入するのみでは十分な効果を発揮するものではなく、役職員に対する継続的なトレーニングやワークショップなどにより、実質的に心理的安全性が担保される組織作りが重要です。

７．その他		
64	外国銀行支店に対するオペレジの適用について、英国当局は、母国当局の監督レジームの同等性評価により代替する方針とあるが、本邦においても同様の方針をグローバルなシステム上重要な外国銀行の日本における支店または子会社に対して採用するのか、ご教示頂きたい。	オペレジはベストプラクティスを探求している段階にある論点も多いことから、本意見募集期間後も、国際的な議論や実務等の進展も踏まえながら、金融機関や利用者をはじめとした幅広い関係者との間で継続的に議論・対話を行うことを予定しております。ご指摘の点についても、幅広い関係者との議論・対話の状況を踏まえ、具体的な対応の検討を進めて参ります。
65	オペリスク管理において、オペレーションの実行部門（1 線）、リスク管理部門（2 線）、内部監査部門（3 線）とあるが、優先順位や重要性の違いはあるか。また「4 線」として、“オペレーション立案・修正（レビュー）・更新部門”があっても良いと考えますが、如何お考えか。	重要な業務を最低限維持すべき水準（耐性度）で遂行するにあたり、必要な経営資源を確保する中で、各金融機関において、それぞれの重要性を判断していくものと考えられます。例えば、重要な業務の中断時には、現場でオペレーションを実行する 1 線にリソースを配分し、それ以外の部門を一時的に縮退させることも考えられます。 他方で、平時のオペレジ確保に向けた取組では、1 線から 3 線に至るまで連携して取り組む必要があり、重要性に差異はないとも考えられます。 なお、DP でお示ししている「3 線防衛体制」は、BCBS「健全なオペレーショナル・リスク管理のための諸原則（改訂版）」や COSO「内部統制の統合的フレームワーク」で示されている概念であり、これらの枠組みにおいて 4 線は存在していませんが、各金融機関において、オペレジの実効性確保のため、ご指摘のような手法も含めた創意工夫を妨げるものではありません。

66	オペリスク管理において、「フォワードルッキング」、「バックワードルッキング」の具体的な内容を例示頂けると幸い。	金融機関のオペレーショナル・リスク管理における「バックワードルッキング」なリスク計測とは、過去 10 年間で財務諸表に影響したオペレーショナル・リスク損失を収集し、当該データを基に将来も起こり得る損失を推計し、当該損失を吸収できるだけの自己資本を予め維持することを指します。 他方で、「フォワードルッキング」な対応とは、例えば暗号資産などの過去のデータ蓄積が十分ではないエマージング・リスクについて、過去データを基に将来起こり得る損失を推計すると所要自己資本が過少になりかねないとの懸念を踏まえて、保守的に過去データ対比で大きめの損失も見積もって、自己資本を多めに維持することなどを指します。