Digital Trust NewsFlash

PwC Digital Services / 2023 年 1 月 / 第 6 号

商業銀行のためのサイバーセキュリティとレジリエンスに関するOJK通達No. 29/SEOJK.03/2022

銀行業界における金融サービス提供のためのITの高度化・革新化に伴うサイバーセキュリティリスクの高まりを受け、インドネシア金融庁（Otoritas Jasa Keuangan：OJK）は2022年12月27日に商業銀行のサイバーセキュリティとレジリエンスに関する通達No29/SEOJK.03/2022（(Ketahanan dan Keamanan Siber bagi Bank Umum、以下「SEOJK Siber」）を発行しています。**従来の銀行とシャリア銀行を含むすべての商業銀行**に対して直ちに適用されます。この通達は、2022年10月7日から有効なPOJK PTI No. 11/POJK.03/2022の一部分となります。。

SEOJK Siberは、銀行が満たすべきサイバーセキュリティとレジリエンスに関する最低限の要件を規定し、効果的な**サイバーセキュリティリスク管理**および銀行の事業目標をサポートする**サイバーレジリエンスプロセス**（識別、保護、検出、対応、回復）のエンドツーエンドの実装を組み込むことによって、全体のサイバーセキュリティとレジリエンスを高めることを目指しています。

SEOJK Siberの新着情報

サイバーセキュリティリスク評価

SEOJK Siberは、主に以下のようないくつかの重要な要素から構成され、**総合的なサイバーセキュリティリスク評価**を定義しています。

銀行は、**サイバーセキュリティリスク評価**を実施し、以下の結果に基づいて総合的なサイバーセキュリティリスクのレーティングを決定することが求められています。

a. **サイバーセキュリティの固有リスク評価**：銀行の事業、複雑性、テクノロジーの採用から生じるリスクを測定する。

   1) これは、テクノロジー、銀行の商品、組織の特性、サイバーインシデントの実績の4つの側面に関して評価される
   2) 固有リスク評価は、レベル1（低）、レベル2（低～中）、レベル3（中）、レベル4（中～高）、レベル5（高）に分類される

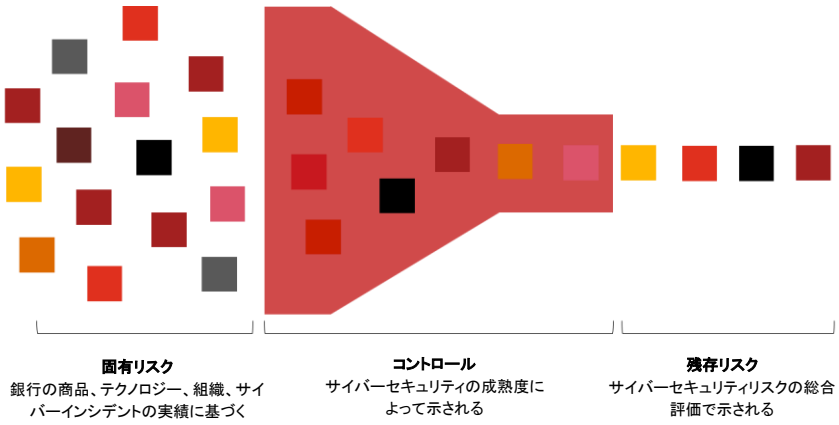
b. **サイバーセキュリティ成熟度評価**：現在のサイバーセキュリティの状況を反映した形で、サイバーセキュリティの成熟度を測定すること。サイバーセキュリティ成熟度は、以下の実装品質に基づいて評価される。

   1) **サイバーセキュリティリスク管理は**、4つのドメインと11のサブドメインに分かれた56のコントロールで構成され、以下をカバーしている。
      a) サイバーセキュリティリスクガバナンス。これには、取締役会及び監査役会の積極的な監督、サイバーセキュリティリスクの選好、リスク許容度、社風及び社員の意識を含む。
      b) サイバーセキュリティリスクの枠組み。サイバーセキュリティリスク管理戦略、組織の適切性、方針・手続き・リスク制限の適切性を含む。
      c) サイバーセキュリティリスクのプロセス、資源、及び情報システム
      d) サイバーセキュリティリスクの管理体制。内部統制システム、レビューの適切性を含む。

   2) **サイバーレジリエンスプロセスの実施は**、4つのドメインに分かれた24のコントロールで構成され、以下をカバーしている。
      a) 資産、脅威、脆弱性の特定
         i) 資産およびその構成のインベントリ作成と評価
         ii) 脆弱性評価の実施と新たな脅威の監視
         iii) 定期的なサイバーセキュリティテスト（VAPTまたはシナリオベースのテスト）の実施
      b) 資産の保護
         i) IT資産に対する包括的なセキュリティ管理を実施、管理、維持し、継続的に改善
         ii) リスクベースの情報、データセキュリティ管理の実施
         iii) コンピュータネットワーク、ハードウェア、ソフトウェアに対する保護の実施
         iv) システム開発中のアクセスコントロールの管理、セキュリティパッチ管理、第三者サービスの保護、セキュアコーディングの実施
      c) サイバーインシデントの検知
         i) ベースラインパフォーマンスとサイバー検知プロセスの確立
         ii) 異常な活動に対する継続的な監視と検知の実施
         iii) サイバー検知プロセスのテストと継続的な改善
         iv) サイバーインシデントの脅威と脆弱性の分析の実施
      d) サイバーインシデントへの対応と復旧
         i) エスカレーションパスとコミュニケーション計画を含む、サイバーインシデント対応と復旧計画の策定と実行
         ii) サイバーインシデント対応チームの役割と責任の決定
         iii) 封じ込め、根絶、復旧手順の実行
         iv) インシデント後の分析を行い、教訓と改善の機会を特定

   （参考：セクションIII - V）

サイバーセキュリティの固有リスク評価、サイバーセキュリティ成熟度評価、サイバーセキュリティリスク評価の関係は、下図のように銀行全体のサイバーセキュリティ管理の現在の状況を示しています。



リスク評価プロセスの終了までに、銀行は総合的なサイバーセキュリティリスクのレーティングを決定することができ、銀行の予想されるリスク選好度およびリスク許容度に対して追跡および監視する必要がある残存リスクを示すことができるようになります。リスク評価は、レベル1（低）、レベル2（低～中）、レベル3（中）、レベル4（中～高）、レベル5（高）に分類されます。
（参考：セクションVI）

サイバーセキュリティテスト

サイバーレジリエンスプロセスの実施における資産、脅威、脆弱性の特定プロセスの一環として、銀行は以下のようなサイバーセキュリティテストを実施しなければなりません。

a. **脆弱性評価と侵入テスト（VAPT）**
    1) 銀行の内部評価と必要性に基づいて定期的に実施されなければならない。例えば、システムの重要度や、銀行のシステムやITアーキテクチャの変更に基づく
    2) 銀行のIT運用の現状報告の一部として、OJKに報告される
b. **シナリオベースのテスト**（机上演習、サイバーレンジ演習、ソーシャルエンジニアリング演習、レッドチーミング、敵対的攻撃シミュレーション演習など）
    1) 少なくとも年1回実施しなければならない
    2) 評価が完了後、10営業日以内にOJKに報告される
    3) 作業範囲には、少なくとも、目的、範囲、シナリオ、テストの実行、テストの評価、サイバーインシデントの緩和、対応、復旧プロセスの有効性の評価などが含まれていなければならない

（参考：セクションVII）

サイバーインシデント報告

サイバーインシデント（例：マルウェア、ウェブ改ざん、DoS、DDoS）とは、電子システム障害を引き起こす可能性のある活動、及び行動です。サイバーインシデントが発生した場合、銀行は以下のことを行う必要があります。

a. サイバーインシデントの監視と関係者への伝達
b. OJKに以下の形式で報告する:
    1) 初回通知
        - サイバーインシデントが検出された後、24時間以内に報告しなければならない
        - インシデントのタイムライン、種類、影響を受けたシステム、サイバーインシデントの初期対応と分析などの一般的なインシデント情報を含み、規定のフォーマットを使用して報告

2) サイバーインシデント報告
- サイバーインシデントが検出されてから5営業日以内に報告しなければならない
- 一般的なインシデント情報、影響評価、時系列分析、根本原因分析、結論、修復作業を含み、規定のフォーマットを使用して報告

(参考：セクションIX)

サイバーセキュリティ組織

銀行は、IT管理機能から**独立したサイバーセキュリティ機能**を設置し、以下のことを調整および・または実行する必要があります。

a. サイバーレジリエンスプロセスの実施
b. サイバーリスク評価、固有のサイバーリスク評価、サイバー成熟度評価
c. サイバーセキュリティのテスト
d. サイバーインシデント対応チーム

(参考：セクションVIII)

罰則規定

SEOJK Siber には、制裁措置について明示的に説明するセクションはありません。しかし、SEOJK Siber は、OJK 規制 No.11/POJK.03/2022 または POJK PTI の第 15 条および第 21 条で要求されているサイバーリスク管理およびサイバーレジリエンスを実施するためのガイドラインを提供しているため、この通達に従わない場合、POJK PTI の不遵守となり、書面による警告、罰金、活動の一時停止、健全性の評価におけるガバナン ス要素のスコア減少などの行政罰が課せられる可能性があります。

重要なポイント

SEOJK Siberは、銀行業界におけるサイバーセキュリティの状況に新たな基準と期待値を設定するものです。多くの銀行がサイバーセキュリティの実践を見直す必要があり、SEOJK Siberへの準拠を管理するために、現在のサイバーセキュリティの実践を確立または調整する必要がある可能性があります。重要なのは、SEOJKがインドネシアの銀行業界全体のサイバーセキュリティ成熟度を向上させ、銀行とその主要な利害関係者がサイバーセキュリティの状態を確認できるようにするのに役立ちます。

a. 銀行は、IT管理機能から独立したサイバーセキュリティとレジリエンスの機能を設置する必要がある
b. 銀行は、サイバーセキュリティインシデント管理及びサイバーセキュリティインシデント発生時のOJKへの報告を含む、サイバーセキュリティリスク管理及びサイバーレジリエンスプロセスを実施する必要がある
c. このSEOJK Siberから期待される報告は以下の通り

	サイバーセキュリティ固有のリスクレベル評価	サイバーセキュリティ成熟度リスク評価	サイバーセキュリティリスク評価	サイバーセキュリティテスト		サイバーインシデント	
				脆弱性評価と侵入テスト	シナリオベーステスト	初期通知	サイバーインシデント報告
タイプ	通常	通常	通常	通常	通常	アドホック	アドホック
頻度	年次	年次	年次	年次	年次	-	-
最終提出	報告年度終了後15営業日以内	報告年度終了後15営業日以内	報告年度終了後15営業日以内	報告年度終了後15営業日以内	テスト実施後10営業日以内	サイバーインシデントが発生してから1x24時間以内	サイバーインシデントが発生してから5営業日以内
初回報告	2023年6月末日まで	2023年6月末日まで	2023年6月末日まで	2022年銀行のIT運用の現状報告書の一部として	2023年に実施されたシナリオベースのテスト後直ちに	-	-

Your PwC Indonesia Contacts:

Subianto
Broader Assurance Services Leader
subianto.subianto@pwc.com

Andrew Tirtadjaja
Risk Assurance Director
andrew.tirtadjaja@pwc.com

Melissa Gunarto
Risk Assurance Director
melissa.g.gunarto@pwc.com

Benny Setyadi
Risk Assurance Senior Manager
benny.setyadi@pwc.com

Salman Alfarisy
Risk Assurance Senior Manager
salman.alfarisy@pwc.com

Beatrix Ariane
Risk Assurance Senior Manager
beatrix.b.ariane@pwc.com

Ade Triangga
Risk Assurance Manager
ade.triangga@pwc.com

Ledwin Ewaldo
Risk Assurance Manager
ledwin.ewaldo@pwc.com

Yudhi Ariyanto
Risk Assurance Manager
yudhi.ariyanto@pwc.com

Mila Ichwanto
Risk Assurance Manager
mila.ichwanto@pwc.com

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

pwc