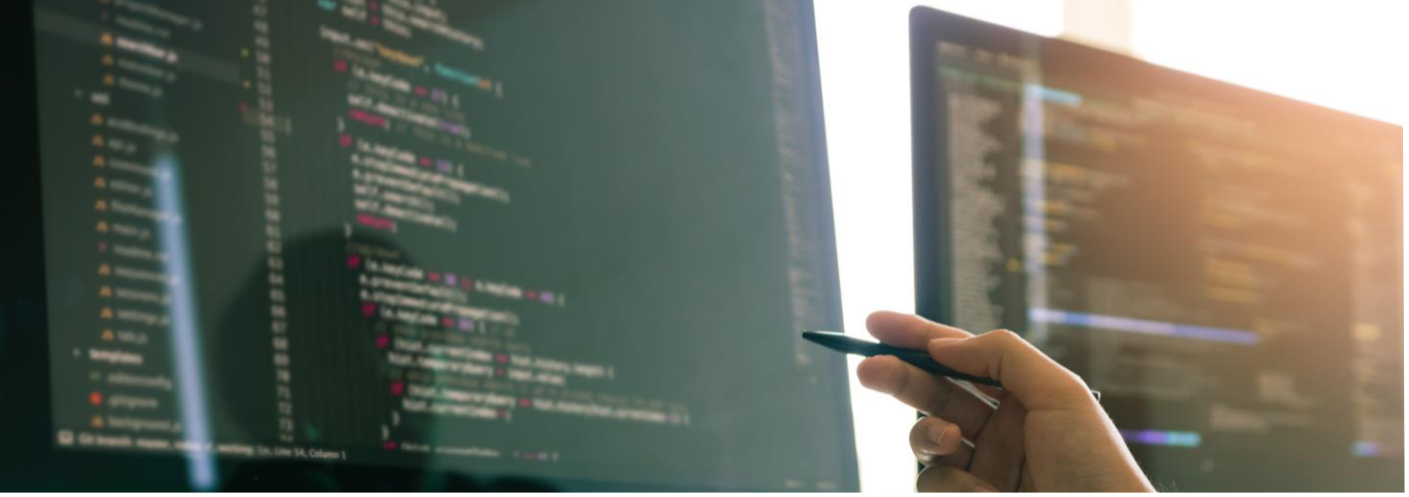

Digital Trust NewsFlash

PwC Digital Services / 2022 年 9 月 / 第 4 号

インドネシア金融庁規則 No.11/POJK.03/2022 商業銀行による情報技術の導入について

銀行業界における金融サービス提供のための情報技術（IT）の導入が進んでいる状況に対応し、インドネシア金融庁（OJK）は 2022 年 7 月 7 日に商業銀行による IT の導入に関する規則 No.11/POJK.03/2022（Peyelenggaraan Teknologi Informasi Oleh Bank Umum、以下「POJK PTI」）を発表しました。POJK PTI は 2022 年 10 月 7 日に発効し、商業銀行による IT 利用時のリスク管理の適用に関する OJK 規則 No.38/POJK.03/2016 に代わるものとなります。

POJK PTI は、銀行が満たすべき IT に関するガイドラインを提供し、銀行の事業において優れた IT ガバナンスを実施することで、デジタルバンキングの成熟度を高めることを目的としています。

POJK PTI のポイント

サイバーセキュリティと強靭性

銀行はサイバーセキュリティの強靭性を確保しなければなりません。銀行は少なくとも以下のことを実行しなければなりません。

a. 資産、脅威、および脆弱性の特定
b. 資産の保護
c. サイバーインシデントの検出
d. サイバーインシデントへの対応と復旧

上記を実行するために、銀行は IT 管理機能から**独立した強靭化されたサイバーセキュリティ機能**を設置する必要があります。
さらに、以下のような定期的な評価を実施することが求められます。

a. **サイバーセキュリティ成熟度評価**を毎年実施すること。当該評価は自己評価の形で行うことができるが、12 月末までの期間を対象としなければならない。また、評価結果は、銀行の IT 運用に関する定期報告書の一部として OJK に提出しなければならない。
b. 以下の方法で**サイバーセキュリティテスト**を実施する。
    1) **脆弱性評価と侵入テスト（VAPT）**

- 定期的にテストを実施する必要がある。
- テスト結果は、銀行の IT 運用に関する定期報告書で報告される必要がある。

2) **シナリオベースの評価**（例：サイバーインシデント対応、机上演習、レッドチーム演習など）
   - 評価は少なくとも年 1 回実施しなければならない
   - 評価結果は、評価の完了後 10 営業日以内に OJK に報告しなければならない。
   - 作業範囲には、少なくとも、目的、範囲、シナリオ、評価の実行、サイバーインシデントの緩和、対応、回復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。

各銀行のサイバーセキュリティ成熟度評価には、サイバーテストの結果分析を含む包括的な分析が含まれていなければなりません(第 21 条～第 27 条)。

データガバナンス
銀行は、少なくとも、データの所有権とガバナンス、データの品質、データ管理システムといった効果的なデータガバナンスが実施されており、データガバナンスをサポートするリソースがあることを確認しなければなりません(第 43 条)

個人情報の保護
銀行は、個人情報処理活動において、個人情報保護の原則を順守するものとします。情報対象者のリスクを高める可能性がある場合、銀行は情報保護影響評価（DPIA）を実施することが要求されます。

情報の転送における個人情報保護を実施するにあたり、銀行は少なくとも以下の事項を決定する必要があります。
a. 個人情報の識別と分類
b. 個人情報の移転に関わる当事者の権利と義務
c. 個人情報の移転に関する合意
d. 個人情報の移転方法
e. 個人情報の安全性

情報の移転は、法律で規定された顧客・潜在的な顧客の同意に基づいて行わなければなりません(第 44 条～第 45 条)。

IT アーキテクチャ
IT アーキテクチャの構築において、銀行は少なくともいくつかの要因、例えば情報、アプリケーション、技術管理の原則、および情報・電子取引法などの関連法を考慮しなければなりません(第 11 条)

IT 戦略
銀行は、長期的な IT 導入、銀行の経営計画をサポートする IT 戦略計画を整備することが要請されます。
IT 戦略計画は、計画が開始される前年の 11 月末までに OJK に提出されなければなりません。IT 戦略計画の変更は、期間中であればいつでも提出することができます。

銀行は、進行中の IT 戦略計画に関して、銀行の目標および戦略に重大な影響を与える事態が発生した場合、IT 戦略計画を修正することができます(第 12 条～第 13 条)

外部 IT サービスの利用
銀行は、データセンター（DC）や災害復旧センター（DRC）としてクラウドコンピューティングサービスの利用など、外部の IT サービスプロバイダーを利用して IT 業務を実施することができます。また、銀行は少なくとも以下の条項に対応した業務契約を作成することが求められています。

a. IT サービスプロバイダーが、銀行と顧客のデータ及び情報のプライバシーを保護すること
b. IT サービスプロバイダーが、銀行に提供された IT サービスについて、独立監査人が実施する定期的な IT 監査の結果を提出すること
c. IT サービスプロバイダーによる銀行への重大インシデントの報告体制が西部されていること

d. IT サービスプロバイダーが、OJK 及び・またはその他の権限ある関係者が、法律と規則に従って提供された IT サービスの検査のためにアクセス権を提供する準備があること(第 29 条～第 30 条)

電子システムおよび IT ベースの決済処理の設置

銀行は、インドネシア国内の DC および DRC に電子システムを設置することが義務付けられています。オフショア（インドネシア国外）にシステムの設置を希望する銀行は、OJK の許可を得る必要があるとともに、以下のシステム基準を満たしている必要があります。

a. 統合的な分析
b. 統合的なリスク管理
c. マネーロンダリング防止、テロ資金調達防止の導入
d. グローバルに顧客サービスを提供するための、顧客サービスの統合

e. 銀行本部と支店間のコミュニケーション管理
f. 銀行の内部管理（第 35 条）

その他の規定

その他にも、以下のような注目すべき規定がいくつかあります。

a. **IT 内部監査機能**は、少なくとも 3 年に一度、独立した外部の第三者によってレビューされる必要があります。OJK に提出する必要のある書類には、以下のものが含まれます。
   1) 独立した外部当事者によるレビュー報告書の一部としてのレビュー結果
   2) 商業銀行の内部監査機能の実施に関する OJK 規則に従った、実施および内部監査結果報告書の一部としての IT 内部監査結果(第 55 条)
b. **IT リスク管理の実施**。銀行は災害復旧計画（DRP）を持ち、ビジネス影響分析に従って、すべての重要なアプリケーションとインフラについて、IT ユーザーを巻き込んで少なくとも年 1 回の DRP のテストを実施することが要求されます (第 18 条)。
c. **銀行のデジタルバンク成熟度を決定するための自己評価**は、POJK PTI で規定されているすべての IT 管理面を見直すことにより、少なくとも年 1 回実施されます。その結果は、銀行の IT 運用の現状に関する報告書の一部として、OJK に提出されなければなりません(第 66 条)。
d. IT 導入のための**方針、基準、手続き、リスク管理ガイドライン**を、OJK 規制の有効性が確認されてから最大 6 か月以内に調整する (第 67 条)。

罰則規定

本規則の要件に違反した場合、書面による警告、罰金、事業活動の一時停止などの行政処分を受ける可能性があります。

重要なポイント

多くの銀行が、POJK PTI の順守の見直しが必要になると考えられます。有効性を高め、コストを削減するだけでなく、少ない労力でより多くのことができるよう、コンプライアンスの再定義が必要になります。その結果、これまでにない変化と機会がもたらされ、テクノロジーを駆使した効率的なコンプライアンス機能は、任意ではなく、競争力の維持のみならず、将来の事業運営とその成功のための要件となります。

a. 2023 年 4 月までに銀行が内部方針と手続を調整することが要請される、大きな変更があります。
    1) 独立したサイバーセキュリティ機能の確立と定期的なサイバーセキュリティテストの実施
    2) データガバナンスとデータプライバシーの仕組みを確立すること。これには、以下のような方法が含まれます。
        - 機密性の高いデータ/情報の特定
        - データの作成/取得から廃棄に至るまでのデータライフサイクルを管理するための手続きを規定する
        - 適切なデータ保護のためのプロセスやテクノロジーを定義する
    3) 包括的な IT アーキテクチャの構築
    4) デジタル成熟度評価を毎年実施すること
b. 銀行は、データセンターの設備がインドネシア国内にある場合、システムをクラウドでホストすることを許可されます。
c. 銀行は、2022 年 11 月までに POJK PTI に準拠した IT 戦略計画を策定または更新する必要があります。

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

Hengky Antony
Risk Assurance Director
hengky.antony@pwc.com

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

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

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

www.pwc.com/id

PwC Indonesia

@PwC_Indonesia

If you would like to be removed from this mailing list, please reply and write UNSUBSCRIBE in the subject line, or send an email to **id_contactus@pwc.com**.