profyt.ai

BANKING COMPLIANCE BRIEFING · JUNE 2026

Documented Is Not Defensible

Why BSP, AMLC, and FATF Now Judge Philippine Banks on What They Can Demonstrate, Not What They Document.

The post-FATF, AFASA-era supervisory regime rewards what an institution can demonstrate, not what it has documented. This briefing explains the shift, why traditional programs are buckling under it, and how a growing number of banks are re-engineering compliance around structured obligations and retrievable evidence.

Prepared for Chief Compliance Officers, Chief Risk Officers, Heads of AML, Internal Audit leaders, and Regulatory Affairs teams at BSP-supervised institutions, including universal, commercial, thrift, rural, and digital banks.

Published by **ProfytAI**

profyt.ai

EXECUTIVE SUMMARY

The Burden of Proof Has Moved

Three forces are converging on Philippine banking compliance in 2026, and together they redefine what "compliant" means. The change is not another rule to absorb. It is a change in how every rule is examined.

First, the supervisory question has changed. The Philippines exited the FATF grey list on 21 February 2025, after more than three and a half years of increased monitoring.[12] Exit moved the country into the effectiveness phase of the cycle, with technical-compliance documentation scheduled by 31 March 2027 under the APG's published fifth-round schedule (subject to APG/FATF process changes).[13] The Anti-Money Laundering Council's third National Risk Assessment, released in December 2025, still rates the inherent money-laundering threat as high.[11] In ProfytAI's reading, the practical test of compliance is shifting from "is it written down" toward "does it work, obligation by obligation, with the evidence the rules already require."

Second, new BSP instruments attach consequences to evidence rather than to paperwork. The Anti-Financial Account Scams Act (Republic Act No. 12010) makes an inadequate fraud programme a restitution liability, not merely a supervisory finding, with the operational controls detailed in its implementing circulars.[9] Circular 1232 introduces a Cybersecurity Maturity Framework with an annual cybersecurity control self-assessment for BSFIs notified by BSP as moderate- or complex-IT-profile and others specifically identified by BSP.[8] Circular 1203 requires operational resilience that is scenario-tested and signed off by the board.[2] Each requires specific artifacts the institution must hold and be able to produce: annual self-assessments, scenario-test results, transaction logs, and control records.

Third, the clock is immediate. The Act's deadline for upgraded fraud-management systems and the phase-down of interceptable one-time passwords falls in **June 2026**, one year after the implementing rules took effect,[3] and BSP publicly signalled in January 2026 that it would not extend it. It lands within weeks of this briefing.

> THE POINT MOST INSTITUTIONS ARE UNDERESTIMATING
>
> **The unit of compliance has changed from the document to the obligation backed by evidence. A program organized as a library of policy PDFs cannot answer an obligation-level, evidence-level examination at speed.**

A growing number of institutions have stopped treating regulation as a shelf of documents and started treating it as structured data. This briefing sets out the regulatory reality driving the shift (Section 1), why manual, document-centric programs break under it (Section 2), the operating concept that replaces them (Sections 3 and 4), and a practical readiness checklist (Section 5).

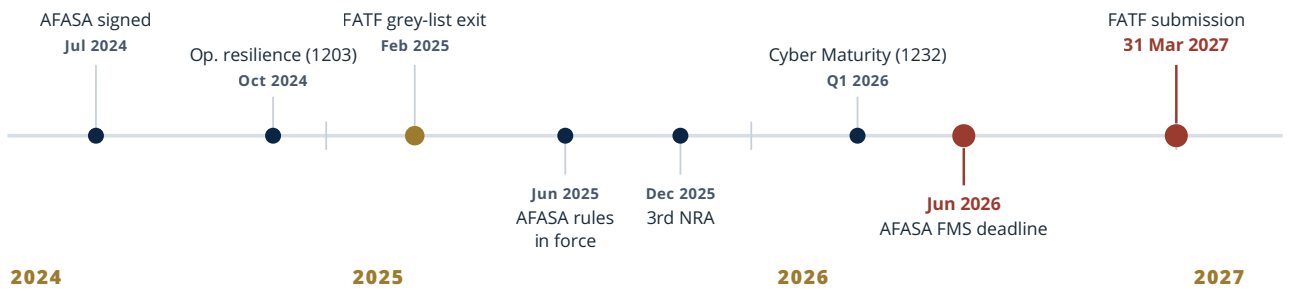

Figure 1. The Compliance Clock. A dense eighteen-month wave of mandates, two of them with near-term, examiner-tested deadlines.

SECTION 1

01 The New Compliance Reality in Philippine Banking

A short window has produced an unusually dense run of regulation. Read together, the issuances point in one direction: away from documented intent and toward demonstrated effect.

From Technical Compliance to Effectiveness

The FATF grey-list exit reset the test rather than ending it. The next mutual evaluation, with technical-compliance documentation scheduled by 31 March 2027 under the APG's published fifth-round schedule (subject to APG/FATF process changes), assesses something harder: effectiveness. AMLC's third National Risk Assessment (December 2025) keeps the inherent money-laundering threat at high. The practical translation: it is no longer enough to hold a customer due diligence policy. You must show it operated, on a named customer, with a retrievable record.

A Regulator Raising the Evidentiary Bar across Every Risk Domain

The same shift now runs through prudential and conduct supervision, not only AML. Each instrument below requires the institution to hold a specific record and stand ready to produce it when supervisors look: a scenario test, a control self-assessment, a fraud-rule calibration record, a disputed-funds hold log.

TABLE 1 · SELECTED BSP AND AMLC INSTRUMENTS RESHAPING EXAMINATIONS, 2024 TO 2026

Instrument	Subject	What it requires institutions to evidence
RA 12010 Circulars 1213 / 1214 / 1215 (2025)	Anti-Financial Account Scams Act and implementing rules	A fraud-management system with five mandated fraud-rule classes (velocity, device and account-change, geolocation, blacklist, and behavioural anomaly), multi-factor authentication, a transaction pause period after key account changes, customer kill-switch and money-lock controls, disputed-funds holding, and transaction logs retained at least five years. Inadequate controls can expose an institution to restitution liability; institutions BSP determines compliant with adequate-control requirements are non-liable under the statute.
Circular 1232 (2026)	Cybersecurity Maturity Framework	An annual Cybersecurity Control Self-Assessment for BSFIs notified by BSP as having a moderate or complex IT profile and others specifically identified by BSP, placed on a maturity ladder (Foundational, Established, Managed, Optimized) proportionate to its IT-risk profile.
Circular 1203 (2024)	Operational Resilience	Mapped critical operations, defined tolerances for disruption, severe-but-plausible scenario testing, third-party dependency mapping, board-approved framework, 24-hour notification on activating the incident-response plan, and Annual Report disclosure.
Circulars 1218 / 1230 (2025 / 2026)	Large-value cash transactions and EDD threshold	A non-cash-channel requirement for large-value payouts above PHP 500,000 (Circular 1218), and a customer-level EDD trigger once cash activity exceeds PHP 1,000,000 (Circular 1230), with documented risk rationale.
GoTRACS AMLC Reg. Issuance No. 2 (2024)	Transaction reporting and compliance submissions	Standardized electronic submission of covered-transaction reports (five working days) and suspicious-transaction reports (next working day from occurrence or determination of suspicion, as applicable under GoTRACS), with a beneficial-owner template for juridical persons.
Circular 1019 (2018, in force)	Cyber-incident reporting	Notification to BSP within two hours of discovery of a major incident, and a structured follow-up report within 24 hours.

TONE FROM THE TOP

BSP convened its first Corporate Governance Summit for bank directors in May 2026 and framed sound governance as the safeguard that matters most under stress. The Financial Services Cyber Resilience Plan 2025 to 2029 institutionalizes industry threat-intelligence sharing. Supervision is shifting from periodic form-checking toward continuous, evidence-led assurance.

The Operational Consequence

The volume and velocity of obligations now exceed what a manually maintained register can hold. A single circular can touch dozens of discrete requirements spread across fraud operations, IT, AML, customer experience, and the board reporting calendar. When the rule changes, as Circular 1230 changed the cash-EDD trigger within months of Circular 1218, the real question is "which of our obligations, controls, procedures, and training materials must change, and who owns each." Few programs can answer quickly because the answer lives in documents and people's heads, not in data.

SECTION 2

02 Why Traditional Compliance Programs Are Breaking Down

The failure is not effort or competence. It is architecture. Programs built on documents and spreadsheets were designed for an era that asked "is it written down," and that era has ended.

1. Spreadsheet-Driven Obligation Tracking Loses the Thread

A workbook can list requirements, but it carries no stable obligation identifiers, no version lineage, and no link from a requirement to the proof it was met. Cells drift, tabs multiply, and ownership blurs.

IN PRACTICE When Circular 1230 raised the cash-EDD trigger to PHP 1,000,000, a spreadsheet cannot tell you which monitoring rules, branch procedures, and training decks reference the old PHP 500,000 logic, or who must change each. The work becomes a manual hunt, repeated by hand every time a rule moves.

2. Regulatory Change Management Is a Manual Re-reading Exercise

A new issuance lands and someone reads it, then guesses which internal obligations and controls it affects. The mapping is slow, lossy, and dependent on the individual who happens to do it.

IN PRACTICE Circular 1232 replaces a familiar IT-rating approach with maturity tiers and a self-assessment. Translating that into the specific controls a bank must now evidence, and the new annual self-assessment filing cadence, is precisely the kind of cross-walk that manual processes perform inconsistently.

3. Evidence Is Collected as One-Off Artifacts, Then Lost

Screenshots and exports assembled for the last examination are scattered across shared drives and inboxes by the next. Each cycle re-requests, re-formats, and re-files the same proof. Nothing that was proven stays proven.

IN PRACTICE The Act's disputed-funds regime allows a temporary hold of up to thirty days and ties weak controls to restitution. The defense is contemporaneous, retrievable evidence that the fraud system and the hold process operated as designed. A folder of ad hoc captures is not that.

4. Audit Preparation Is a Recurring Fire Drill

Because evidence is not maintained as a standing asset, every examination triggers weeks of reactive assembly. Senior compliance and audit staff are pulled off forward work to reconstruct a trail that should already exist.

IN PRACTICE Operational-resilience supervision under Circular 1203 expects mapped critical operations, tolerance settings, and scenario-test results on request. Reconstructing these after the request arrives is slow and rarely convincing.

5. Documentation Exists, but Cannot Be Produced as Proof

The most expensive failure is the quiet one: a control that genuinely works but cannot be evidenced on demand. Examiners increasingly treat poorly documented enhanced due diligence the same as no due diligence at all.

IN PRACTICE A bank may run effective source-of-wealth review, yet if it cannot retrieve the specific record, the senior approval, and the monitoring trail for a named high-risk customer, the control fails the examination regardless of whether it worked in reality.

> **THE COMMON ROOT CAUSE**
>
> Each failure traces to the same source: the program is organized around **documents**, but the regulator examines **obligations**. A policy PDF answers "what is our position." An examiner asks "show me, for this specific requirement, the control and the evidence." The mismatch between the two is where modern compliance programs are breaking.

SECTION 3

03 The Shift from Documents to Regulatory Data

The fix is conceptual before it is technological. Stop treating a regulation as a document to be read and start treating it as a set of structured obligations to be operated on.

A regulation, viewed correctly, is not prose. It is a collection of atomic, individually testable requirements. A document-centric program stores the prose and re-derives the requirements by hand whenever it needs them. An obligation-centric program extracts the requirements once, as structured records, and builds everything else on top of that layer. A connected chain follows naturally once obligations are data.

- **An obligation registry.** Every requirement becomes a discrete record with a stable identifier, its legal citation, severity, and the verbatim source text it derives from. The registry, not a policy binder, is the source of truth.
- **Policy mapping.** Each obligation is linked to the bank policy that implements it, so the institution's own program, not the regulator's prose, is what carries the requirement forward.
- **Control mapping.** Each policy is linked to the control that implements it, so coverage and gaps are visible at the level the regulator actually examines.
- **Evidence traceability.** Each control, and any procedures or added steps an audit requires, links to retrievable proof, traceable back through policy and obligation to the source clause, captured once and reused across every cycle.
- **Regulatory intelligence.** Each new issuance is triaged against the registry to surface exactly which obligations, policies, and controls it creates, amends, or supersedes, within days rather than after the fact.
- **Audit readiness.** Because obligation, policy, control, and evidence are already joined, an examination package is assembled by query, not by project.

TABLE 2 · TWO WAYS TO RUN A COMPLIANCE PROGRAM

Dimension	Document-centric (legacy)	Obligation-centric (data)
Unit of work	The policy document	The individual obligation
Source of truth	A library of PDFs and workbooks	A structured obligation registry tied to source text
Handling a new circular	Re-read and manually guess what it touches	Triage against the registry to surface affected obligations
Evidence	Collected ad hoc, scattered, re-gathered each cycle	Captured once, anchored through control and policy to the obligation, reused
Examiner request	Reconstructed reactively over weeks	Retrieved by obligation, reproducible on demand
Knowledge retention	Lives in individuals; walks out the door	Lives in the data layer; compounds each cycle
The examiner's question	"Where is your policy?"	**"Prove this obligation, now."**

This is the insight beneath the entire briefing. The shift to obligations as data is not a tooling preference. It aligns with how the regulator now examines, by obligation, control, and evidence, and it is what turns each examination cycle into a compounding asset rather than a reset to zero.

SECTION 4

04 A Modern Operating Model for AML and Regulatory Compliance

A growing number of institutions are building a layered operating model in which proof is an ordinary by-product of running the program, not an emergency rescue before an exam.

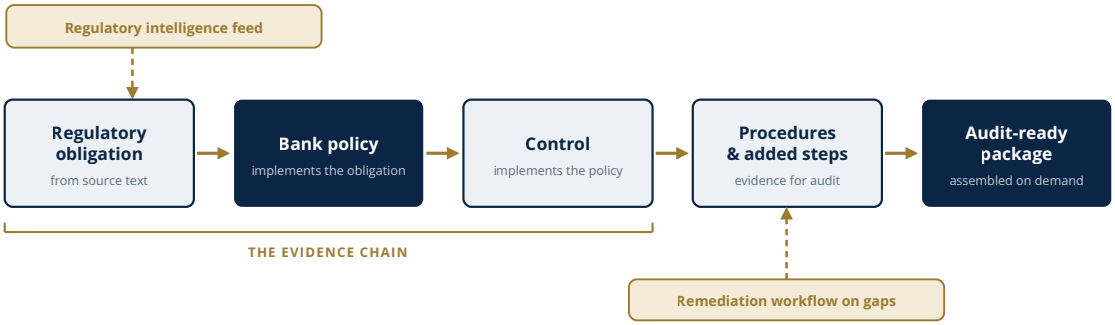

Figure 2. The Evidence Chain. Each obligation maps to the bank policy that implements it, then to the control that implements the policy. Teams extend the chain with the procedures and evidence an audit needs, then assemble an audit-ready package on demand. A regulatory-intelligence feed keeps obligations current; gaps flow into remediation.

Six Building Blocks

- **A living obligation inventory.** One authoritative registry, sourced from the regulator's own text and versioned as rules change, replacing scattered workbooks as the single source of truth.
- **A traceable policy-to-control chain.** Each obligation maps to the bank policy that implements it and the control that implements the policy, extensible with the procedures and added steps an audit requires.
- **An evidence system, not an evidence folder.** Proof is captured against the control or procedure it serves, traceable back through policy to the obligation and its source clause, stored once and retrievable on demand across every future cycle.
- **Remediation workflows.** Every identified gap becomes a tracked action with a named owner, a deadline, and a closure record, routed to the accountable business unit.
- **Continuous regulatory monitoring.** A triaged feed of issuances mapped to affected obligations, so a material change is understood in days and never discovered during an exam.
- **Audit readiness as a standing state.** Readiness is scored continuously and the examiner package is one assembly step away, because the underlying joins already exist.

WHERE TO START, NEXT TWO QUARTERS

1. Build a structured obligation registry for your priority frameworks (MORB Part IX, the AFASA circulars, Circular 1232), anchored to the regulator's source text.
2. Map each obligation to the bank policy that implements it, then to the control that implements the policy, each with a named owner.
3. Convert ad hoc evidence collection into an evidence system that links each proof item through control and policy back to its obligation.
4. Close the AFASA items first: fraud rules, MFA, kill switch and money lock, disputed-funds holding, and five-year logs, with the policy, control, and evidence for each, ahead of June 2026.
5. Make audit readiness a board-visible standing dashboard, scored by obligation coverage and evidence completeness.

SECTION 5

05 The 2026 Readiness Checklist

A practical, examiner-oriented checklist. Each item is phrased as proof a bank should be able to produce on demand, not merely a policy it should hold.

GOVERNANCE

- ☐ Board has **approved** the operational-resilience and fraud-prevention frameworks, with minutes evidencing oversight.
- ☐ Compliance reports coverage and gaps to the board **in obligation terms**, not document counts.
- ☐ Director fitness and disqualification screening is documented and current.

AML / CFT

- ☐ Institutional risk assessment refreshed against the December 2025 NRA findings.
- ☐ Enhanced due diligence is **retrievable per customer**: source of wealth, senior approval, monitoring trail.
- ☐ Cash-EDD logic updated for the **PHP 1,000,000** customer-level trigger (Circular 1230) and the non-cash-channel requirement for large-value payouts above PHP 500,000 (Circular 1218).
- ☐ Covered- and suspicious-transaction reports are submitted on the statutory deadlines through GoTRACS, including its beneficial-owner template.
- ☐ Sanctions screening freezes without delay and covers beneficial owners and related parties.

FRAUD AND AFASA (BY JUNE 2026)

- ☐ Fraud-management system covers all **five mandated rule classes**, with calibration and test records.
- ☐ Multi-factor authentication deployed and interceptable OTPs phased down.
- ☐ **Kill switch**, money lock, payee verification, and the post-change transaction pause are live.
- ☐ Disputed-funds holding process operates within the statutory window, with logs.
- ☐ Transaction logs retained at least **five years** with the prescribed fields.

REGULATORY CHANGE MANAGEMENT

- ☐ Every new issuance is triaged to the **specific obligations** it creates or amends within days.
- ☐ Change history is versioned, so superseded requirements remain traceable.
- ☐ Owners are notified automatically when an obligation they hold changes.

EVIDENCE MANAGEMENT

- ☐ Each obligation maps to the **bank policy** that implements it and the control that implements the policy.
- ☐ Each control and procedure links to **retrievable proof**, traceable back to the obligation and source clause.
- ☐ Evidence is captured once and reused across cycles, not re-gathered each exam.
- ☐ Any obligation can be produced with its **full chain of proof** on demand, reproducibly.

INTERNAL AUDIT

- ☐ Assurance plan covers cybersecurity, third-party risk, and operational resilience as discrete topics, in step with the 2024 IIA Standards.
- ☐ Independent review of the fraud-management system is scheduled and evidenced.
- ☐ Audit works from the obligation registry, not a separate manual list.

RISK MANAGEMENT AND RESILIENCE

- ☐ Critical operations and **tolerances for disruption** are mapped and approved.
- ☐ Severe-but-plausible **scenario tests** are run, with results retained (Circular 1203).
- ☐ Third-party and cloud dependencies are mapped to the critical operations they support.
- ☐ Incident-response activation triggers 24-hour BSP notification, with a tested workflow.

EXAMINATION READINESS

- ☐ If notified by BSP as moderate- or complex-IT-profile (or otherwise specifically identified), the annual **CCSA** is maintained as data and submitted on or before 31 March following the reference year (Circular 1232).
- ☐ Cyber-incident reporting meets the **two-hour** and 24-hour windows (Circular 1019).
- ☐ An examiner package can be assembled **by obligation** without a multi-week scramble.
- ☐ Readiness is scored continuously and visible to the board.

CLOSING PERSPECTIVE

Compliance Infrastructure Is Becoming a Regional Discipline

The Philippine shift is part of a wider Southeast Asian pattern. Singapore's MAS, Indonesia's OJK, Malaysia's Bank Negara, Thailand's central bank, and their peers are all raising the evidentiary bar at once, each demanding that regulated institutions demonstrate effectiveness rather than merely assert it. For banks that operate across borders, or aspire to, the consequence is structural: several effectiveness regimes must be satisfied in parallel, each with its own obligations, its own evidence expectations, and its own examination cadence. Maintained by hand, in documents, that burden compounds until it becomes unmanageable.

The institutions that will spend the next cycle answering questions rather than assembling binders are the ones that treat regulation as what it has become: structured data. An obligation registry tied to source text, controls mapped to obligations, evidence captured once and retrievable on demand, and a feed that keeps the whole picture current. This is no longer a back-office convenience. It is the operating substrate of a credible compliance program, and it is starting to look less like software a bank buys and more like infrastructure the sector runs on.

THE TAKEAWAY

Our read of 2026: the question is shifting from "Is it written down?" to "Can you prove this obligation works?" The programs that answer yes have rebuilt compliance on data, not documents.

A NOTE ON THE EMERGING CATEGORY

Structured Regulatory Infrastructure, in Practice

A small group of platforms is forming around exactly this idea: turning a regulator's source documents into a structured, examination-ready data layer. **ProfytAI** is one example, positioning itself as the connective tissue between regulation, policy, and proof. It compiles a regulator's text into obligation registers anchored verbatim to the source clause and page, links each obligation to the bank policy that implements it and the control that implements the policy, lets teams extend that chain with the procedures and evidence an audit needs, triages new issuances into a regulatory feed, surfaces gaps, and assembles examiner-ready packages. It is in active use on BSP frameworks (MORB, MORB Part IX for AML/CFT, and AMLC GoTRACS) and MAS Technology Risk Management, with a Philippine digital bank among its early adopters. We include it not as a recommendation but as a marker of where the category is heading: compliance built on obligations, policy, and proof, rather than on documents and effort.

Sources. Every regulatory statement in this briefing is mapped to its primary issuance, with verified links and verification status, in the *Primary Sources and Verification* appendix that follows.

This is the same source-anchored discipline ProfytAI applies in product: every obligation, and every claim made about it, traces back to verbatim regulator source text.

APPENDIX

Primary Sources and Verification

Every regulatory claim in this briefing was verified by ProfytAI against the primary issuance, not secondary reporting. The table maps each claim to its source and the type of authority it represents. The body's broader framing, that the regime rewards demonstrable evidence over documented intent, is ProfytAI's analytical reading, not a quoted regulatory standard.

#	Regulatory statement in this guide	Primary source	Verified against
1	The Philippines exited the FATF grey list on 21 February 2025.	AMLC (2025)	**AMLC issuance**
2	Technical-compliance documentation for the next country evaluation is scheduled under the APG's published fifth-round schedule for 31 March 2027 (Philippines in the 2028 assessment cohort; subject to APG/FATF process changes).	APG schedule	**APG / FATF**
3	The AMLC third National Risk Assessment (December 2025) rates the inherent money-laundering threat as high.	AMLC 3rd NRA	**AMLC issuance**
4	AFASA (RA 12010) creates fault-based restitution liability for inadequate controls, with statutory non-liability where BSP determines compliance with adequate-control requirements.	RA 12010	**Statute**
5	Circular 1232 (2026): Cybersecurity Maturity Framework; annual CCSA for BSFIs notified by BSP as moderate/complex IT profile and others specifically identified by BSP; tiers Foundational, Established, Managed, Optimized.	BSP Circ. 1232	**BSP issuance**
6	Circular 1203 (2024): operational resilience; impact tolerances, scenario testing, 24-hour notice on activating the incident-response plan, Annual Report disclosure.	BSP Circ. 1203	**BSP issuance**
7	The AFASA fraud-management and OTP-phase-down deadline falls in June 2026 (one year after the implementing rules took effect).	BSP Circ. 1213	**BSP issuance**
8	Circular 1213: five fraud-rule classes, multi-factor authentication, 24-hour transaction pause, kill switch, money lock, five-year log retention.	BSP Circ. 1213	**BSP issuance**
9	Circular 1218 (2025): non-cash-channel requirement for large-value payouts above PHP 500,000.	BSP Circ. 1218	**BSP issuance**
10	Circular 1230 (2026): enhanced-due-diligence trigger recalibrated to PHP 1,000,000, applied per customer.	BSP Circ. 1230	**BSP issuance**
11	GoTRACS (AMLC Regulatory Issuance No. 2, 2024): standardized electronic CTR/STR reporting (STR within the next working day from occurrence or determination of suspicion, as applicable under GoTRACS); beneficial-owner template for juridical persons.	AMLC RI No. 2	**AMLC issuance**
12	Circular 1019 (2018): cyber-incident notification within two hours; structured follow-up within 24 hours.	BSP Circ. 1019	**BSP issuance**

PRIMARY REGULATORY REFERENCES

1. BSP Circular No. 1019, s. 2018, Technology and Cyber-Risk Reporting. bsp.gov.ph/Regulations/Issuances/2018/c1019.pdf	**2.** BSP Circular No. 1203, s. 2024, Operational Resilience. bsp.gov.ph/Regulations/Issuances/2024/1203.pdf
3. BSP Circular No. 1213, s. 2025, AFASA fraud-management. bsp.gov.ph/Regulations/Issuances/2025/1213.pdf	**4.** BSP Circular No. 1214, s. 2025, AFASA account inquiry. bsp.gov.ph/Regulations/Issuances/2025/1214.pdf
5. BSP Circular No. 1215, s. 2025, AFASA disputed-funds holding. bsp.gov.ph/Regulations/Issuances/2025/1215.pdf	**6.** BSP Circular No. 1218, s. 2025, Large-Value Cash Transactions. bsp.gov.ph/Regulations/Issuances/2025/1218.pdf
7. BSP Circular No. 1230, s. 2026, EDD-threshold recalibration. bsp.gov.ph/Regulations/Issuances/2026/1230.pdf Reported: pna.gov.ph/articles/1270247	**8.** BSP Circular No. 1232, s. 2026, Cybersecurity Maturity Framework. bsp.gov.ph/Regulations/Issuances/2026/1232.pdf
9. Republic Act No. 12010 (AFASA). lawphil.net/statutes/repacts/ra2024/ra_12010_2024.html Senate: ldr.senate.gov.ph/legislative-issuance/republic-act-no-12010	**10.** BSP AFASA Booklet with implementing rules. bsp.gov.ph/Regulations/Banking Laws/AFASA-Booklet-with-IRRs.pdf
11. AMLC Regulatory Issuance No. 2, s. 2024 (GoTRACS). amlc.gov.ph/images/PDFs/Main/Guidelines_on_Transaction_Reporting_and_Compliance_Submissions.pdf	**12.** AMLC Third National Risk Assessment, December 2025. amlc.gov.ph/images/PDFs/Main/Press Release - 3rd NRA.pdf
13. Philippines FATF grey-list exit, 21 February 2025. amlc.gov.ph/images/PDFs/Main/PR_PH Exits FATF GREYLIST.pdf	**14.** APG Global Fifth Round Mutual Evaluation Schedule; FATF Mutual Evaluation of the Philippines (2019). apgml.org Global Fifth Round schedule apgml.org/about-us/members/members/philippines fatf-gafi.org Mer-philippines-2019

profyt.ai

ABOUT PROFYTAI

ProfytAI builds structured regulatory infrastructure for banks. It compiles a regulator's source documents into an examination-ready data layer, linking every obligation to the bank policy and control that implement it, and to the evidence that proves it. It is live today across BSP and MAS frameworks.

Written by **Chris Burkhardt**

Co-Founder & CTO, ProfytAI

Researched and verified by ProfytAI's regulatory intelligence team. Every regulatory claim in this briefing is traced to its primary issuance in the Primary Sources and Verification appendix.