Global Conference on Multidisciplinary Research and Innovation
Hosted Online from Berlin, Germany
Date: 2nd September, 2026
Website: https://econferencia.com

CONTENT AND METHODOLOGICAL ANALYSIS OF INTERNAL AUDIT PROCEDURES FOR BANKING OPERATIONS

Yuldashev Xurshidbek Mamirjonovich
Independent researcher, Namangan State Technical University,
e-mail: x.yuldashev@hamkorbank.uz,
ORCID: 0009-0005-5512-8161

Abstract
The paper analyses the substantive content and methodological structure of internal audit procedures applied to the principal categories of banking operations — credit, deposit and settlement, treasury, payment cards, and information technology. Particular attention is devoted to the methodological transition from sample-based testing to full-population data analysis and to the organisational preconditions that this transition requires.

Keywords: audit procedures, credit operations, operational risk, data analytics, continuous auditing, sampling, IT audit, model risk, segregation of duties.

Introduction

Internal audit procedures in banks cannot be uniform, because the risk architecture of banking operations differs fundamentally across business lines. A procedure that is highly informative for the credit portfolio may be entirely inappropriate for high-volume payment processing. The Basel Committee's revised principles for the sound management of operational risk, published in March 2021 and comprising twelve principles, explicitly extend the supervisory focus to change management and information and communication technology [1] — areas historically underrepresented in traditional bank audit programmes.

Differentiation of procedures by operation type

Audit procedures concentrate on: completeness and integrity of borrower files; compliance of the credit decision with the approved authority matrix; independence of the credit risk assessment from the sales function; adequacy of collateral valuation and the frequency of revaluation; correctness of loan classification and provisioning; and the detection of restructuring or refinancing used to conceal deteriorating asset quality. The most informative procedures in this area are re-performance of the risk rating and analytical review of migration between classification categories over time.

The focus shifts to segregation of duties, handling of dormant accounts, unusual transaction patterns, reconciliation of internal and suspense accounts, and the timeliness of clearing. Given transaction volumes measured in millions, manual sampling is methodologically inadequate here; automated exception testing over the full population is the only defensible approach.

Audit attention concentrates on limit compliance, dealing authority, valuation of financial instruments, off-market rate detection, and — critically — the organisational independence of the back office from the front office. Model risk becomes a distinct audit object: the auditor must assess model governance, validation, and the appropriateness of assumptions, not merely the arithmetic.

Procedures cover card issuance controls, chargeback and dispute handling, transaction monitoring rules, fraud detection thresholds, and third-party processor oversight. The growth of remote onboarding has made identity verification controls a high-priority audit object.

Procedures cover logical access rights management (particularly privileged accounts), change management in the core banking system, integrity and retention of system logs, backup and disaster recovery testing, and vendor dependency. Weak

coverage of this domain is a recurring theme in supervisory findings across jurisdictions.

The methodological shift in sampling.

The central methodological question concerns sampling. Traditional attribute sampling and monetary-unit sampling remain necessary where audit evidence is documentary and not digitised — for example, physical loan files or signed board minutes. However, where transaction data are fully available in structured electronic form, testing the entire population removes sampling risk entirely and changes the auditor's role: the effort shifts from detecting exceptions to interpreting them.

This transition has three preconditions, only one of which is technical:

Data access — direct read-only access to the core banking database. In practice this is an organisational and political question rather than a technical one, and it is the most common point of failure.

Data quality — a documented data dictionary and stable field definitions; without these, analytical results are unreliable regardless of technique.

Competence — auditors capable of writing and validating queries, and, equally important, capable of recognising when an anomaly is a data artefact rather than a control failure.

Toward continuous auditing.

Continuous auditing represents the logical extension of the data-driven approach: predefined control tests are executed automatically at set intervals, and exceptions are escalated in near real time. Its introduction should be gradual, beginning with a limited set of high-value, well-defined tests (for example, transactions executed by an employee on their own account, or postings made outside business hours),

and expanding as the reliability of the rule set is confirmed. A methodological caution applies: continuous auditing does not replace judgement-based engagements, and a function that invests exclusively in automated testing will progressively lose the capacity to assess governance, culture and strategy — areas where no automated test exists.

Conclusion

1. The effectiveness of internal audit procedures depends less on their number than on their correspondence to the specific risk profile of each category of banking operation.
2. The systematic replacement of manual sample-based testing with full-population, data-driven procedures in high-volume operations is the principal direction for methodological development.
3. The binding constraint on this transition is organisational — data access and competence — rather than technological, and it must therefore be resolved at the level of the board and the audit committee.

References

1. Basel Committee on Banking Supervision. Revisions to the principles for the sound management of operational risk. — Basel: BIS, March 2021. URL: https://www.bis.org/bcbs/publ/d515.htm
2. Basel Committee on Banking Supervision. The internal audit function in banks. — Basel: BIS, June 2012. URL: https://www.bis.org/publ/bcbs223.pdf
3. The Institute of Internal Auditors. Global Internal Audit Standards. — IIA, 2024 (effective 9 January 2025). URL: https://www.theiia.org/en/standards/2024-standards/global-internal-audit-standards/

4. COSO. Internal Control — Integrated Framework. — COSO, 2013. URL: https://www.coso.org
5. Basel Committee on Banking Supervision. Corporate governance principles for banks. — Basel: BIS, July 2015. URL: https://www.bis.org/bcbs/publ/d328.pdf
6. Central Bank of the Republic of Uzbekistan. Regulation on requirements for the internal audit of commercial banks (registered No. 3302, 7 May 2021). URL: https://lex.uz/docs/5431666.