Republic of the Philippines
SOCIAL SECURITY SYSTEM
INTERNAL AUDIT SERVICE GROUP
10th Floor, SSS Building, East Avenue, Diliman, Quezon City

INTERIM REPORT

as of March 31, 2025

I. Executive Summary:

A. Overview

The Baseline Assessment of Internal Controls (BAICs) Report provides a comprehensive evaluation of the current internal control components of the organization.
The assessment aims to identify strengths, weaknesses, and potential areas for improvement. By establishing a clear baseline, we can ensure that our financial reporting, compliance, and operational objectives are being met efficiently and effectively.
This report outlines key findings, significant risks, and recommendations requiring immediate action, which are designed to enhance the effectiveness and reliability of our internal control framework, thereby supporting the organization's strategic goals and safeguarding its resources.

B. BAICS Highlights

Control Environment
1. Finding Statement: The organization has not implemented a process to periodically review and update user access permissions in the financial management system.

Recommendations: The absence of a dedicated IT policy development team and oversight for routine review and update of procedures.

2. Finding Statement: The financial statements contain material misstatements that could affect the accuracy of reported earnings.

Recommendations: Lack of understanding and appreciation of internal controls can lead to ineffectiveness, inefficiencies, and potential financial losses and reputational damage.

II. Objectives, Scope and Methodology:

Objective:

The assessment aimed to:
• Assess the internal control system and proper implementation of controls.
• Check compliance with statutory requirements and internal policies, rules, and procedures.
• Evaluate the efficiency and effectiveness of operations.

Scope:

The assessment of internal controls covers the following process/es:
Processes: Contributions
Key Processes: Collection of contribution payments - Self-employed
Sub Processes: Collection of contribution payments - Self-employed

Methodology:

The audit aims to:
• Administration of Internal Control Checklist (ICC).
• Validation of processes to determine existing design of internal controls which seeks to mitigate identified risks.
• Evaluation of control design to ensure that, at a point in time, internal controls are put in place and executed at the proper timing to mitigate risks which could hinder the achievement of the organization's strategic goals.
• Testing of control effectiveness to determine if internal control procedures are being carried out consistently over a period of time.

III. Findings and Recommendations:

Control Environment

1. Finding Statement:
The organization has not implemented a process to periodically review and update user access permissions in the financial management system.

Condition:
The absence of a formal procedure for regular access reviews and a lack of accountability assigned to a specific team or individual.

Criteria:
As per ISO 27001:2013 (Clause A.9.2.1), "User access management should be regularly reviewed to ensure appropriate levels of access are maintained."

Cause:
The absence of a formal procedure for regular access reviews and a lack of accountability assigned to a specific team or individual.

Consequences:
The absence of a dedicated IT policy development team and oversight for routine review and update of procedures.

Recommendations:
Unauthorized access to sensitive financial data, increasing the risk of data breaches.Non-compliance with regulatory requirements, potentially leading to penalties or reputational damage.

2. Finding Statement:
The financial statements contain material misstatements that could affect the accuracy of reported earnings.

Condition:
Inadequate Documentation: Missing or incomplete documentation supporting transactions or decisions.

Criteria:
Conformance with industry best practices and standards.

Cause:
Overburdened Employees: Employees are overloaded with responsibilities, leading to mistakes or neglect of critical tasks.

Consequences:
Lack of understanding and appreciation of internal controls can lead to ineffectiveness, inefficiencies, and potential financial losses and reputational damage.

Recommendations:
Regularly Review and Update Policies: Conduct periodic reviews and updates of policies to ensure they remain relevant and in compliance with regulations.

IV. Overall Findings:

Lack of clear policies and procedures: Several departments operate without standardized procedures, leading to inefficiencies and confusion.
Inadequate internal controls: Weaknesses in the internal control structure expose the organization to errors, fraud, and operational inefficiencies.
Insufficient employee training: Employees lack sufficient training on critical systems, leading to mistakes and inefficiencies.
Lack of accountability: Inadequate assignment of responsibilities leads to tasks being overlooked or improperly executed.
Failure to document key processes: Key business processes lack adequate documentation, making them difficult to track and improve.
Inconsistent application of procedures: Procedures are applied inconsistently across departments, leading to discrepancies in outputs and results.
Weak monitoring of business performance: The organization lacks consistent monitoring of business performance indicators, leading to missed opportunities for improvements.
Lack of clear communication channels: There are insufficient communication channels, resulting in confusion and misunderstandings between departments.
Insufficient follow-up on audit recommendations: Previous audit recommendations have not been adequately addressed or implemented.
Absence of an effective risk management framework: There is no formalized process to identify, assess, and mitigate risks across the organization.
Inaccurate financial reporting: Financial reports contain errors or inconsistencies that undermine their reliability.

Lack of proper reconciliation: Accounts are not reconciled on time, leading to discrepancies in financial records.
Unapproved expenses: Some expenses are incurred without proper approval, violating organizational policies.
Weak cash flow management: Cash flow is poorly managed, leading to liquidity issues or missed opportunities for investment.
Inadequate inventory controls: Inventory records are not accurate, leading to overstocking or stockouts.
Failure to adhere to accounting standards: Financial reporting does not align with generally accepted accounting principles (GAAP) or other relevant accounting standards.
Poor asset management: Assets are not tracked properly, leading to potential mismanagement or loss.
Inadequate financial oversight: Financial management lacks sufficient oversight, making it difficult to identify inefficiencies or potential fraud.
Failure to segregate duties: Key financial duties are not adequately segregated, increasing the risk of fraud or error.
Delayed financial audits: Financial audits are not conducted in a timely manner, delaying key decision-making processes.
Non-compliance with legal regulations: The organization is not adhering to relevant laws and regulations, exposing itself to legal and financial risks.
Lack of a formal compliance program: There is no structured program in place to ensure the organization is in compliance with applicable regulations.
Failure to update compliance policies: Compliance policies are outdated and do not reflect current legal or regulatory requirements.
Weak monitoring of compliance risks: The organization does not adequately monitor or assess compliance risks across all areas.
Inadequate documentation of compliance efforts: There is insufficient documentation of compliance-related activities, making it difficult to prove adherence to laws and regulations.
Failure to conduct regular compliance audits: Regular compliance audits are not conducted, allowing potential violations to go undetected.
Inconsistent enforcement of compliance policies: Compliance policies are not consistently enforced, creating gaps in organizational adherence.
Failure to maintain regulatory reporting: The organization does not consistently meet its regulatory reporting requirements, risking penalties or fines.
Lack of compliance training for employees: Employees have not received adequate training on compliance requirements, leading to inadvertent violations.
Inadequate vendor compliance monitoring: Third-party vendors are not regularly audited for compliance with relevant legal or contractual obligations.
Weak cybersecurity measures: The organization’s IT infrastructure is vulnerable to cyber threats due to inadequate security measures.
Inadequate access controls: Sensitive systems or data are accessible to employees without proper authorization, posing a security risk.
Failure to back up critical data: Key business data is not regularly backed up, increasing the risk of data loss in case of disaster.
Unpatched software vulnerabilities: Outdated or unpatched software creates vulnerabilities that expose the organization to potential cyberattacks.
Poorly defined IT policies: IT policies and procedures are not adequately defined or enforced, leading to inefficiencies and security risks.
Lack of disaster recovery planning: The organization lacks a comprehensive disaster recovery plan to quickly recover from system failures or data loss.
Inadequate user training on IT security: Employees are not trained to recognize or prevent common IT security threats like phishing or malware attacks.
Failure to monitor IT system performance: There is no monitoring of IT systems to detect performance issues or system failures before they impact operations.
Failure to secure third-party access: Third-party vendors or contractors have access to sensitive systems without adequate oversight or controls.
Weak IT governance framework: The organization does not have a well-defined IT governance framework to ensure that IT decisions align with business objectives.
Inconsistent application of HR policies: HR policies are not consistently applied, leading to employee dissatisfaction and potential legal risks.
Lack of employee performance evaluations: There is no regular performance review process in place, leaving employees without feedback on their performance.
Failure to address employee grievances: Employee grievances or complaints are not being addressed in a timely or consistent manner.
Inadequate employee training and development: Training programs are insufficient, preventing employees from developing necessary skills for their roles.
Non-compliance with labor laws: The organization is not fully compliant with labor laws, risking penalties or legal action.
Inadequate recruitment processes: The organization does not have a structured or effective recruitment process in place, leading to inconsistent hiring practices.
Lack of succession planning: There is no formal succession planning process in place to prepare for future leadership transitions.
Failure to offer competitive compensation packages: Employee compensation and benefits are not competitive within

the industry, resulting in potential talent retention issues.
Inconsistent application of disciplinary actions: Disciplinary actions are applied inconsistently, which can lead to perceptions of unfairness and potential legal risks.
Failure to maintain accurate employee records: Employee records are not updated regularly or maintained accurately, leading to potential compliance issues.
Inefficient business processes: Business processes are not optimized, leading to inefficiencies and wasted resources.
Poorly managed inventory: Inventory management practices are inadequate, resulting in excess stock or stockouts.
Lack of quality control mechanisms: There are no formalized processes to ensure product or service quality, leading to inconsistencies and customer dissatisfaction.
Inadequate resource allocation: Resources (human or financial) are not being allocated effectively, resulting in underperformance or missed opportunities.
Failure to meet customer expectations: Customer service practices are inadequate, leading to dissatisfaction or loss of customers.
Lack of performance monitoring: Key performance indicators (KPIs) are not tracked, hindering the ability to measure and improve operational performance.
Unclear organizational structure: The organization's structure is unclear, leading to confusion about roles, responsibilities, and reporting relationships.
Poor communication between departments: Communication between departments is inadequate, causing delays and misunderstandings.
Failure to optimize supply chain operations: Supply chain inefficiencies lead to higher costs or delays in delivering products or services.
Lack of continuous improvement efforts: There is no structured approach to identifying and implementing process improvements within the organization.
Lack of competitive bidding: The organization does not consistently use competitive bidding to select suppliers, potentially resulting in overpaying for goods and services.
Poor vendor management: Vendor relationships are not effectively managed, leading to performance issues or unmet expectations.
Failure to negotiate favorable contract terms: Procurement contracts are not adequately negotiated, potentially resulting in unfavorable terms for the organization.
Weak supplier performance monitoring: Supplier performance is not regularly reviewed, leading to the continuation of underperforming relationships.
Failure to monitor procurement compliance: Procurement activities are not consistently monitored for compliance with internal policies or legal requirements.
Inadequate inventory controls: Inventory management systems are inefficient, leading to potential overstocking or stockouts.
Failure to align procurement with strategic goals: Procurement decisions are not aligned with the organization's long-term goals or strategies.
Weak contract enforcement: Contracts with suppliers are not properly enforced, leading to missed deliverables or service failures.
Failure to track supplier payments: Supplier payments are not properly tracked, leading to late payments or disputes.
Lack of contingency planning in supply chain: The organization does not have contingency plans in place for potential disruptions in the supply chain.
Unclear project goals: Project objectives are not clearly defined, leading to confusion and misalignment with business priorities.
Unrealistic project timelines: Project timelines are overly ambitious and not aligned with available resources, leading to delays.
Inadequate project resource allocation: Resources are not allocated appropriately, leading to underperformance or project failure.
Lack of proper risk management: Project risks are not identified or managed proactively, leading to unforeseen challenges.
Poor project communication: Communication between project teams, stakeholders, and sponsors is inadequate, leading to misunderstandings and delays.
Failure to monitor project progress: Projects are not tracked against key performance metrics, making it difficult to identify problems early.
Inconsistent project documentation: Project documentation is not maintained properly, making it difficult to track decisions or progress.
Failure to adhere to project budgets: Projects frequently exceed budget, due to poor cost estimation or uncontrolled spending.
Scope creep in projects: Projects experience uncontrolled changes in scope, leading to delays, cost overruns, or misalignment with original goals.
Inadequate project closure processes: Projects are not properly closed out, leaving critical tasks unfinished or overlooked.
Weak fraud prevention controls: The organization's fraud prevention measures are inadequate, leaving it vulnerable to fraudulent activities.
Failure to segregate duties: Critical financial duties are not properly segregated, increasing the risk of fraudulent activities.
Inadequate fraud monitoring systems: Fraud detection systems are not in place or not functioning effectively, allowing fraudulent transactions to go unnoticed.

Failure to implement anti-fraud training: Employees are not trained on fraud detection and prevention, increasing the likelihood of fraud going undetected.
Lack of a whistleblower program: The organization does not have a formal system for reporting suspected fraud, reducing the chances of early detection.
Inadequate background checks: Employees, vendors, or contractors are not adequately vetted, increasing the risk of fraud or misconduct.
Failure to monitor high-risk areas: High-risk areas for fraud, such as cash handling or procurement, are not monitored regularly.
Lack of fraud risk assessments: The organization does not regularly assess fraud risks, missing opportunities to mitigate potential vulnerabilities.
Weak audit trails: Financial transactions lack adequate documentation, making it difficult to detect or investigate fraudulent activities.
Failure to enforce anti-fraud policies: Anti-fraud policies are not consistently enforced, reducing their effectiveness.
Unclear contract terms: Contracts are vague or lack specific terms, leading to confusion or disputes.
Failure to monitor contract performance: Contracts are not actively monitored, leading to missed obligations or subpar performance by vendors.
Weak contract enforcement: Contracts are not enforced properly, resulting in breaches or delays without consequences.
Lack of formal contract review processes: Contracts are not regularly reviewed to ensure they remain relevant and compliant with regulations.
Non-compliance with contract terms: Both the organization and its vendors fail to fully comply with contract terms, resulting in disputes or legal risks.
Failure to track contract renewals: Contracts are allowed to expire without timely renewals or renegotiation, creating service gaps.
Inadequate contract documentation: Contracts and related documents are not properly maintained or stored, leading to difficulties in reference or enforcement.
Failure to conduct contract audits: Contracts are not audited regularly to ensure compliance and to identify potential savings opportunities.
Lack of contingency plans in contracts: Contracts lack clear provisions for managing unforeseen changes or disruptions in service.
Failure to standardize contracts: The organization uses inconsistent contracts across different departments, leading to confusion and inefficiencies.

V. Appendices / Attachments:

Note: All supporting evidence provided by auditees has been appropriately cataloged using standardized naming conventions to ensure consistency and ease of reference.

Prepared by	Designation	Signature	Date Signed
Nicole Aquino	Department Head		

Reviewed by:	Approved by:
Nicole Aquino **Team Leader**	Nicole Aquino **Head of Internal Audit**
Reviewed Date:	**Approved Date:**
03/31/2025	03/31/2025