**REVISION HISTORY**

|  |  |  |  |
| --- | --- | --- | --- |
| **Rev. No.** | **Rev. Date** | **Description of Change** | **Author / Originator** |
| 00 | December 31, 2021 | Initial release | Zheena Ocampo,  HoldCo Internal Audit |
|  |  |  |  |
|  |  |  |  |

**DOCUMENT CONFIDENTIALITY ACCESS LIST**

|  |  |  |  |
| --- | --- | --- | --- |
| **List of Users** | **Access Type**  (View, Edit) | **Type of Media**  (Electronic / Hard Copy) | **Retention Period** |
| HoldCo Management  (CEO to AVP) | Edit, view | Electronic | Until superseded |
| Document Author | Edit, view | Electronic | Until superseded |
| HoldCo Employees | View  *(Download restricted)* | Electronic | N/A |
| Other Users | View, as needed | Electronic | N/A |

**DOCUMENT AUTHOR, REVIEWER, AND APPROVER**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Prepared by:** | **Name** | **Position** | **Signature** | **Date** |
| Zheena Ocampo | IA Manager |  |  |
| **Reviewed by:** | Celso Vivas | ACC |  |  |
| Ramon Diaz | CFO |  |  |
| **Approved by:** | Edgar Saavedra | Chairman |  |  |

**Table of Contents**

[1.0 OVERVIEW 5](#_Toc88231697)

[2.0 CORE FUNCTIONS 5](#_Toc88231698)

[3.0 ROLES AND RESPONSIBILITIES 8](#_Toc88231699)

[4.0 RISK MANAGEMENT 11](#_Toc88231700)

[5.0 RISk-BASED INTERNAL AUDIT (RBIA) FRAMEWORK 12](#_Toc88231701)

[5.1 RBIA OVERVIEW 12](#_Toc88231704)

[5.2 AUDIT PRE-PLANNING AND SCOPING 14](#_Toc88231705)

[5.3 RISK ASSESSMENT AND CONTROLS 14](#_Toc88231706)

[5.4 AUDIT EXECUTION 20](#_Toc88231707)

[5.5 REPORTING 22](#_Toc88231708)

[5.6 FOLLOW-UP AUDIT 24](#_Toc88231709)

[5.7 FRAUD AUDITING 24](#_Toc88231710)

[6.0 FORMS & TEMPLATES 30](#_Toc88231711)

[1.0 7.0 REFERENCES 31](#_Toc88231712)

[5.8 7.1 Megawide EPC: 5PLMC Process 31](#_Toc88231713)

[5.9 7.2 HoldCo Corporate Finance and Planning Business Process 31](#_Toc88231714)

[8.1 ANNEXES 32](#_Toc88231715)

[8.1 Glossary of Terms 32](#_Toc88231716)

**INTERNAL AUDIT**

**Department Manual**

# [OVERVIEW](#TOC)

The **Internal Audit Department (IAD)** of **Megawide Construction Corporation** shallaim to provide independent and objective assurance that the governance and control system of the Strategic Business Units (SBU), is effective, and advisory services related to risk management and systems improvements. IAD shall help the Company accomplish its strategic objectives by bringing a systematic and disciplined approach in evaluating and improving the efficiency and effectiveness of risk management, internal controls, and governance processes.

[**About the Manual**](#TOC)

The Manual shall outline the department’s business framework and processes. It shall serve as a reference for all CHII, MCC, and SBU employees on the services and support offered by the department.

The Manual shall contain the links to forms, reporting templates, and references indicated by underlined characters in dark red font. For easier navigation, headers of each section shall link the user back to the Table of Contents.

[**Key Objectives of the Manual**](#TOC)

The Manual shall be used by the Internal Auditors for the following purposes:

* Provide the standard policies and guidelines to ensure effective, efficient, and consistent execution of CHII IAD processes
* Train the Internal Auditors and orient the auditees (i.e., the departments, business units, and projects), thereby enabling them to understand their respective roles and responsibilities while an internal audit is being conducted
* Provide guidelines in setting up the fraud investigations as the need arise

# CORE FUNCTIONS

The Company shall have a strong and effective Enterprise Risk Management (ERM) framework and Internal Control System (ICS) that ensure integrity, transparency, and proper governance are observed in the conduct of its affairs. The Company shall have an independent and non-operation internal auditing function that provides impartial and objective assurance and consulting services designed to add value and improve operations. In compliance with IIA’s International Professional Practices Framework, IAD shall be under the control of the Board of the Directors (BOD) and Audit and Compliance Committee (ACC).

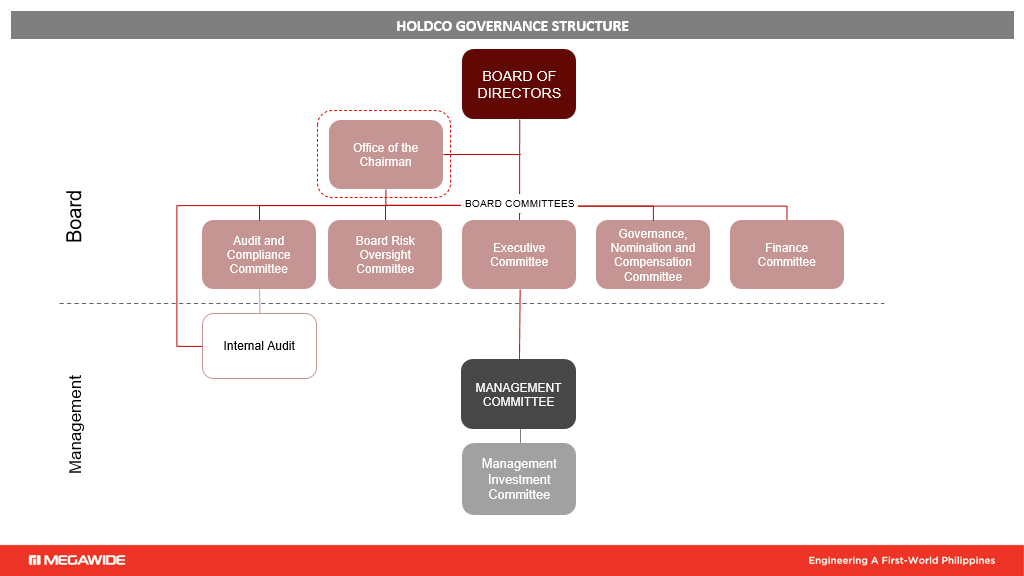


Figure 1 HoldCo Governance Structure

Risk-Based Internal Auditing (RBIA) shall be applied by IAD in performing the Board-mandated functions. These can be summarized into three main categories and corresponding risk coverage:

1. ERM Program (strategic, financial, operational, and human resources)
2. ICS (fraud and other irregularities, possible misstatement of financial and management reports)
3. Governance and compliance (misrepresentations in the governance compliance reporting, compliance in governance reporting, regulatory, environmental, sustainability)

Other IAD services shall be provided as arises:

1. Advisory services
2. Other activities requested by the ACC, BOD, and Chairman

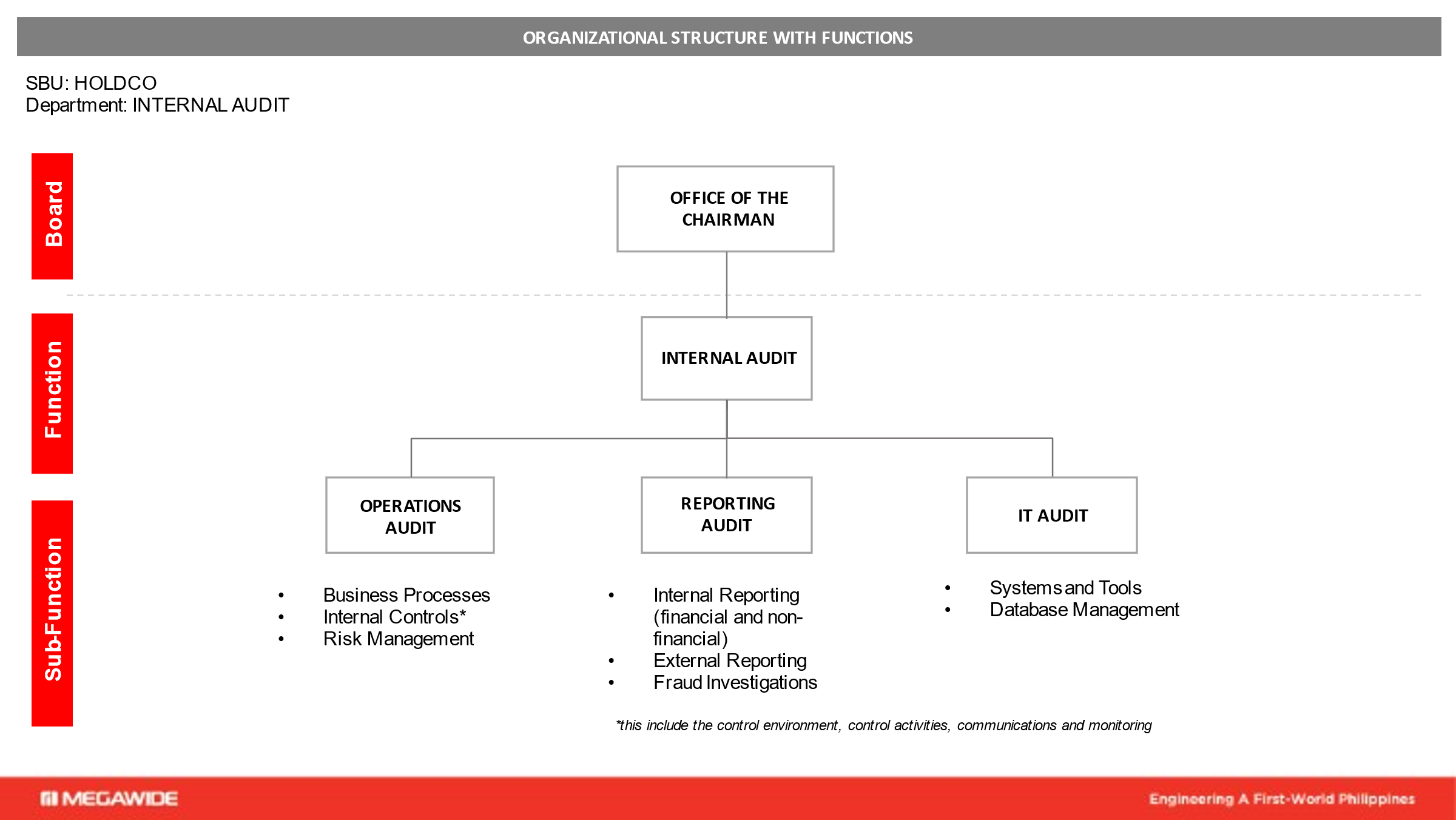


Figure 2 Organizational Structure with Functions

IAD’s organizational structure shall organize the internal auditors into sub-functional units based on their specialized knowledge and competencies to maximize operational efficiency and productivity. IAD subfunctions shall not be designed to operate exclusively but to work collaboratively for greater audit coverage. This structure shall empower IAD to find support within, instead of having to outsource work when specific skills and knowledge are required for an audit engagement, as well as build the skills of everyone in IAD through cross-functional on-the-job training.

[**KEY RESULT AREA (KRA)**](#TOC)

The following KRAs and Key Performance Indicators (KPIs) shall be reported to ACC periodically:

|  |  |
| --- | --- |
| **KRAs** | **KPIs** |
| Support management strategic initiatives by auditing key risk areas | * Percentage of key risk areas covered * Percentage of audits delivered against planned |
| Conducts internal audit transparently and professionally; results are duly supported by material evidence and communicated clearly to the auditees | * Percentage of audit findings accepted by auditees * Percentage of satisfactory ratings provided by auditee |
| Provide relevant and credible results and quality recommendations; helps Management identify serious issues | * Percentage of audit findings open, closed, and past due * Percentage of audit recommendations implemented |
| Identify systemic weakness/root cause of issues facing the business units | * Count of recurring nonconformities / repeated findings |

KPIs to measure the department’s productivity and efficiency shall be monitored internally and shall be reported as needed.

# ROLES AND RESPONSIBILITIES

* 1. **IAD** shall:
* Provide an independent risk-based assurance to the ACC, and BOD, focusing on reviewing the effectiveness of the governance and control processes by conducting risk assessment and performing planned and special audits on key risk areas
* Review, audit and evaluate the efficiency and effectiveness of the existing ICS
* Check the operations and management initiatives/programs to ascertain whether the results are consistent with the established objectives and goals and are being carried out as planned/schedule
* Evaluate specific operations at the request of the BOD and Chairman
  1. **Chief Internal Auditor (CIA)** shall:
* Manage all internal audit activities of the Company, including portions that are outsourced to third-party service providers
* Periodically review the IA Charter and present it to the ACC for approval
* Develop and implement the Annual RBIA Plan outlining the high-risk areas and priority activities that are consistent with the Strategic Plans of CHII, MCC, and SBUs
* Present findings and recommendations to the Management, ACC, BOD, and Chairman on how to improve the policies, procedures, reports, and enterprise resource planning systems in terms of internal controls, process alignments, reporting tools, and system designs
* Coordinate activities and information among the external auditors, Management, ACC, BOD, and Chairman
* Be primarily responsible for implementing the Whistleblower Policy (SD-FIN001)
* Coordinate with HRD for campaigning of the Whistleblower Policy among employees of CHII, MCC, and SBUs on regular basis.
* Evaluate all leads received from whistleblowers, and either endorse these to Industrial Relations or initiate fraud investigations
* Maintain the confidentiality of the whistleblowers
* Conduct, assign internal auditors or hire external auditors to conduct investigations of whistleblowing concerns, other investigations performed/managed by ACC
* Directly report valid whistleblowing concerns involving MCC Officers to the CEO, and those involving the CEO and other directors to the ACC
* Consolidate, file, and retain all records related to the status/results of internal audits and fraud investigations conducted
  1. **ACC** shall:
* Ensure that the Company establishes an effective thorough risk management process (i.e., ERM framework) and effective ICS by finalizing the manuals and risk templates
* Oversee IAD during the development and implementation of the IA Charter and Annual RBIA Plan
* Provide adequate protection and mechanism to ensure that the financial reports released by the Company and SBUs are reliable and trustworthy
* Review critical policies, particularly in the areas of financial reporting and prevention of fraud and conflicts of interest
* Support the development of the end-to-end accounting system, including the design of the financial reporting structure and templates
* Promote the right values and ethics by reviewing critical policies particularly in the areas of financial reporting, conflict of interests, and fraud
* Provide an avenue of communication among the independent auditors, BOD and Chairman
* Approve and sign contracts for hiring external auditors (including audit of annual financial statements, and fraud investigations)
* Provide oversights on the Whistleblowing Policy
* Be primarily responsible for investigating whistleblowing concerns involving the CEO and BD of the CHII, MCC, and SBUs
  1. **BOD** shall:
* Oversee and monitor the business in terms of operation, financial, risk, and people, to be aligned with the Company’s vision & mission, as well as long-term business strategies and objectives
* Perform fiduciary duty to protect the company assets and stakeholder investments
* Approve high-value transactions and contracts on behalf of the Company, appointments of authorized signatories for the ordinary course of business, and quarterly reports to the BOD such contracts and transactions
* ​Resolve urgent issues and problems particularly affecting the company assets, stakeholder investments, and appointments of Executives
  1. **Chairman** shall:
* Provide strategic directions across the CHII, MCC, and SBUs
* Decide on matters related to the confidentiality of company information and records excluded for internal auditing
  1. **CHII Legal Department** shall:
* Assist IAD during the identification and substantiation of required evidence related to fraud investigations and employee-related audit investigations that may result in employee terminations
* Provide legal advisory related to audit engagements that may result to contract disputes between MCC and third-party vendors/subcontractors
  1. **CHII, MCC, and SBU Human Resources Department (HRD)** shall:
* Assist the IAD related to audit engagements and fraud investigation involving employees of the Company
* Conduct administrative hearing related to findings involving CHII, MCC, and SBU employees
* Ensure that the Code of Business Conducts & Ethics, and Whistleblowing Policy are communicated to all CHII, MCC, and SBU employees
  1. **MCC Employee** shall:
* Perform duties and responsibilities with integrity, transparency, and honesty
* Cooperate with the IAD by providing all information relevant to the audit scope and schedule
* Perform their duties and responsibilities following the Organization’s policies, procedures, Code of Business Conducts & Ethics
* **Report and email any wrongdoing or concerns to** [**sumbongkayed@megawide.com.ph**](mailto:sumbongkayed@megawide.com.ph)**, including those relative to financial reporting, suspected fraudulent activities, breaches of the Company policies and procedures**

# RISK MANAGEMENT

|  |  |  |
| --- | --- | --- |
| **Risk Area** | **Risk** | **Possible Causes** |
| Planning and scoping | * Key risk areas are excluded from RBIA | * Misalignment between the strategic plans and audit objectives * Insufficient manpower to cover key risk areas |
| Reporting | * Improper calibration of findings | * Audit nomenclatures are nonstandard or prone to misinterpretation * Not truly understanding the business unit/area of the Company that they are auditing * Lack or no materiality/impact assessment |
| Reporting | * Findings are not appreciated nor understood by auditees and Management | * Insufficient or disorganized evidence * Findings are not clear, concise nor catered to the audience (e.g., too wordy, materiality not considered) |
| Follow-up audit | * Audit findings are past due * Recommendations are not adopted by the auditee * Recurring findings | * Lapses in the monitoring and escalation of past-due NCRs * The root cause was not properly identified |
| Fraud investigations | * Evidence gathered are incomplete/insufficient for administrative hearing or legal proceedings | * Lack of coordination with CHII Legal |

# RISk-BASED INTERNAL AUDIT (RBIA) FRAMEWORK

## RBIA [OVERVIEW](#TOC)

The RBIA methodology shall be applied to comply with the above fiduciary responsibilities and the individual business units based on their complexity, size, and risk profile and as agreed with the BOD and Chairman of CHII. This risk-based approach allows IAD to be more effective and cost-efficient as IAD focuses its efforts on applying risk management techniques on and auditing areas/processes that are more significant contributors towards achieving the strategic goals of the business units.

Table, calendar

Description automatically generated

Figure 3 RBIA Framework

## AUDIT PRE-PLANNING AND SCOPING

|  |  |
| --- | --- |
| * + 1. **Understanding of Business Goals, Supporting Objectives and Controls**   **TAT: *2 Days***  **Timeframe: *Upon approval of the StratPlan during Annual Planning*** | *Responsibility:* ***CAE*** |
| * Shall obtain the following for CHII, MCC, and all SBUs from the Office of the CEO:   + Approved StratPlan & Tracker and current Governance Structure   + Approved Table of Organization (TOO)   + Latest Total Quality Management (TQM) Manuals * Shall review the documents to gain an understanding of the priority objectives and high-risk areas identified by the Department Heads and Group Heads and confirmed by the CEO |
| * + 1. **Define Scope and Objectives**   **TAT: *2 Days***  **Timeframe: *Upon approval of the StratPlan during Annual Planning*** | *Responsibility:* ***CAE*** |
| * Shall prepare the Audit Scoping Memo defining IAD’s overall directions and targets across CHII, MCC, and SBUs, and shall present these to ACC for approval. * Once approved, shall release the Audit Scoping Memo to the CEO, BOD, Department Heads, and Group Heads as reference for future audits. * Shall also instruct the Internal Auditors to use the Audit Scoping Memo as the basis in identifying high-risk areas/processes for their assigned SBUs. |

## RISK ASSESSMENT AND CONTROLS

RBIA means that audit planning is driven by the business units’ risk register and its need for objective assurance. This shall require IAD to perform a risk assessment in developing the Annual RBIA Plan. The risk assessment shall be performed to identify, measure, and prioritize risks that are critical to the StratPlan, vision, and core operations and to focus on the areas threatened by a higher degree of risks.

|  |  |
| --- | --- |
| * + 1. **Enterprise Risk Assessment**   **TAT: x *Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***Internal Auditor*** |
| * Shall interview the Department Heads and Group Heads to obtain additional information for identifying high-risk areas that are needed in developing the audit plans and work programs:   + Core business processes (e.g., 5-PMLC for EPC)   + Line items in the Risk Registers that are adversely affecting the achievement of the business unit’s vision, strategies, and objectives   + Implementation status and effectiveness of corresponding risk responses * Shall also review the critical and recurring audit findings on the Audit Findings Dashboards |
| **TAT: x *Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***Internal Auditor*** |
| * Shall consolidate and rank the risks according to the Senior Management’s perceptions using the pre-defined criteria (Refer to Annex A for the risk assessment criteria):   + Inherent/gross risk – Significant risks that shall be managed well by the Risk Champion to support the achievement of the business units’ objectives, regardless of the effectiveness of the actual risk responses/controls implemented to address those risks   + Residual risk – The remaining level of risks once the effects of the existing risks responses are implemented * Then, shall identify the significant business processes that are associated with these high-risk areas and shall include those in the initial audit plan. * For more complex processes, shall perform a process-level risk analysis to gain a better understanding of the significant activities and critical paths within the high-risk processes and to further pinpoint the audit scope. Documentation to be reviewed shall include TQM manuals, flowcharts, reporting templates, etc.   + For example, the financial reporting process was identified as a high-risk area. Further risk analysis at the process level may be necessary to identify if the process for billing and revenue recognition shall be the focus area for the audit engagement.   + When performing process-level risk analysis, the internal auditors shall analyze how the processes are managed against leading practices (e.g., industry standards and guidelines, regulator’s expectations, and other publicized leading practices). However, the appropriate practices to be adopted by MCC shall be the ones that best support the organization achieve its strategic objectives within the context of its processes and structure.   **This activity shall not replace the risk assessment performed by the business units and individual departments/projects as this will be detrimental to MCC’s risk maturity.** IAD shall audit the existing Risk Registers to provide third-party and objective assurance and recommendations for improving the organization’s risk management. |

|  |  |
| --- | --- |
| * + 1. **Assess Design Adequacy of Controls**   **TAT: *1-2 Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***Internal Audit*** |
| * Shall understand the controls embedded in high-risk areas/processes by considering the past year’s auditing ratings, recommendations, and status of committed action plans (see [Annex 4: Risk Assessment Factors](#Annex_4) for details). |

Audit planning is important for conducting audit work and for managing the engagements as RBIA is known for its “rapid-fire” execution.

|  |  |
| --- | --- |
| * + 1. **Development and Approval of Audit Plan**   **TAT: *1-2 Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***Internal Auditor*** |
| * Shall prepare the Individual Audit Engagement Plans by specifying, but not limited to, the following details:   + Audit objectives - What the audit aims to achieve   + Scope of work - The magnitude and boundaries of activities, objectives, and exposures to be reviewed.   + Approach - The nature of the audit to be performed   + Risks to be reviewed   + Limitation of scope   + Work program and rating model to be used - Standard work programs with predefined objectives and test procedures to be performed for high-risk areas shall be established by the CIA as necessary   + Audit team – Assigned Internal Auditors, and distribution of tasks   + Auditee team – The Department/Group Head and their subject-matter-experts   + Duration - The estimated timeline for the completion of the audit. It is expected that the actual engagement shall not exceed more than 2 weeks per project/department due to the thorough audit pre-work performed.   + Analysis of relevant information - Brief on activity/business or process to be audited, previous audit results, and external reviews   + Audit deliverables - Describe the type of reporting to be provided   Planning audit engagements shall help the Internal Auditors become familiar with the high-risk areas for their assigned audits and help them identify the risks that it exposes to and existing controls for mitigating these risks (in line with IPPF’s Standard 2021). The risks and controls associated with the high-risk areas/processes shall be evaluated during the annual audit planning. Specific instructions on how to analyze risks and associated controls in the individual audit engagement planning shall be provided by the CIA as there may be jobs or tasks warranted by the ACC, BOD, and/or CEO.   * After which, shall consolidate the individual plans for review and finalization of the CIA. |
| **TAT: *1-2 Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***CIA*** |
| * After which, shall consolidate, review and finalize the individual plans to:   + Ensure alignment with the Audit Scoping Memo   + Ensure proper calibration of the risk assessments performed so that only high-risk areas/processes across CHI, MCC, and SBU shall be audited   + Optimize workload assignments, which can be done through consolidation of similar engagements and subsequent scheduling of interrelated processes among the business units   + Incorporate special instructions from the ACC, BOD, and Chairman (if any) |
| **TAT: *1-2 Days***  **Timeframe: *Upon approval of the Audit Scoping*** | *Responsibility:* ***CIA*** |
| * Shall present the Annual RBIA Plan to the ACC for approval.   The Annual RBIA Plan shall be inherently dynamic and modified over time to reflect evolving MCC’s risk profile as various factors associated with the internal operations and external environment change and impact the business over time. **At the discretion of the CIA, individual audit engagement shall be deferred to the following year to prioritize fraud investigations and special audit requests from the ACC, BOD, and CEO.**  Significant changes to the approved Annual RBIA Plan shall be discussed with the ACC quarterly. |

The Audit Work Program shall include the test procedures that will guide the Internal Auditors on how to validate the effectiveness of the design and implementation of the ICS in mitigating inherent and residual risks. However, the Internal Auditors should still use their professional judgment to modify the test programs as the need arise.

|  |  |
| --- | --- |
| **Development Approval of Audit Work Program**  **TAT: *1-2 Days***  **Timeframe:** Upon ***approval of the Audit Scoping*** | *Responsibility:* ***Internal Auditor*** |
| * Shall prepare the Audit Work Programs for their specific audit engagements using the risks and controls previously evaluated during the enterprise risk assessment stage. The Internal Auditor shall ensure there is a specific test for each risk included in the Annual RBIA Plan and that sufficient evidence can be obtained with the least man-hours. There are generally two (2) types of internal audit procedures:   + Test of design shall be performed to evaluate if the ICS was designed to effectively address the high risk and its impact on the business units   + Test of effectiveness shall confirm whether ICS is being implemented as designed. However, if the test of design is already found weak or not yet implemented, testing may be skipped |

The table below shall show the simplified examples of how test procedures of a work program can be determined based on the process-risk analysis.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Risk ID** | **Process Risk - Inherent** | **Control** | **Strength of Control Design** | **Process Risk - Residual** | **Considerations for Test Procedures** |
| 1 | High | A | Strong | Low | Test if control is operating and effective as designed |
| 2 | High | B | Weak | High | Control inadequacy issues are noted. Re-evaluated of control design is recommended |
| 3 | Medium | C | Strong | Low | Test if control is operating and effective as designed. Consider a cost-benefit analysis |
| 4 | Low | D | Strong | Low | Not a focus |

|  |  |
| --- | --- |
| **Approval of Audit Work Program**  **TAT: *1-2 Days***  **Timeframe:** Upon ***approval of the Audit Scoping*** | *Responsibility:* ***CIA*** |
| * Shall review and approve the Audit Work Program * After which, shall issue the following to the various stakeholders as reference:   + Accomplished Risk and Control Matrix   + Annual RBIA Plan to the CEO, Department Heads, and Group Heads across the CHII, MCC, and SBUs   + Audit Work Programs to the affected department heads, and group heads. |

## AUDIT EXECUTION

Once the Annual RBIA Plan is approved, the audit engagement shall be carried out (including the execution of the work program and test procedures). During this audit cycle, the internal auditors shall focus on providing recommendations for improvement opportunities to the business units.

|  |  |
| --- | --- |
| * + 1. **Execution of the Audit Work Program for scoped-in accounts/projects**   **TAT: *1 week before***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Shall prepare an audit engagement letter with the following details:   + Audit objectives   + Scope of work – Specifies the high-risk areas/projects and sample projects for test programs   + Audit engagement schedule – dates for the kick-off meeting, walkthroughs, test programs, sprint meetings,   + Audit request list – Documentary requirements for the test programs   + Assigned auditors * Shall have the audit engagement letter approved and signed by the CIA, then release it to the involved department heads and group heads at least 1 week before the kick-off meeting to provide sufficient time to gather the requested requirements. |
| **Kick-off meeting**  **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Shall conduct the kick-off meeting to provide a venue for the IAD and the auditees in:   + Signifying the official start of the audit engagement   + Discussing why the audit is occurring and what audit will be covering   + Clarifying challenges/issues in the past   + Bringing together the right people and resources to effectively and consistently respond to internal audit requests |
| **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Shall perform process-level risk analysis before performing the test procedures. The analysis shall be more general in nature and focus more on the gross risks at the strategic level.   + If already performed during the planning stage, then risk analysis shall be at the operational level. |
| **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * After which shall perform test procedures in the work program. Data for the test programs shall come, but not limited to, the following sources:   + Interviews and process walkthroughs from the process owners   + Spot audits and ocular inspections   + Uploaded files in MSTeams and other shared/online repositories   + Transactional records and system-generated reports from the ERP system   + User and client survey results * Shall record issues with the supporting evidence as Work Papers. |
| **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Shall discuss the detect issues with the audited departments/projects and provide opportunity them:   + Clarify and express their points of view on the finding   + Corroborate the accuracy of information used and findings obtained as well as analyze the need to perform additional tests * Shall objectively assess the received comments. The comments obtained in this manner shall be included in the work papers, if appropriate. |
| **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Shall end of the audit engagement once the work papers are considered sufficient by meeting the following criteria:   + Information sources used are listed (e.g., names of people providing information, names of documents reviewed)   + Scope of work carried out   + Audit tests performed   + Results of audit tests are discussed   + Comments and additional evidence are obtained |

## REPORTING

|  |  |
| --- | --- |
| * + 1. **Summarize audit findings and communicate to Management**   **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***Internal Auditor*** |
| * Perform the audit ratings using the rating model identified in the Audit Engagement Plan. |
| **Communicate to management**  **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***CIA*** |
| * Shall prepare and present to Management the audit findings * Shall secure and document their recommendations, agreements, and commitments to resolve the issues. This shall also be incorporated into the audit finding dashboard. Documentation of Management Responses and Action Plans with Timelines and Resources Needed are already incorporated in Detailed Audit. Significant audit issues, as well as the status of the agreed action plans by management, will be reported during regular AC meetings to ensure related risk/s are managed within acceptable levels.   For ease of preparing the final report, the final report shall be an excerpt from the audit findings dashboards. |
| **Present audit findings dashboard and management response to the Audit Committee**  **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | *Responsibility:* ***CIA*** |
| * Present the audit findings from the dashboards to the ACC and secure management responses. |

The communication of audit findings for MCC is structured as follows:

|  |  |  |  |
| --- | --- | --- | --- |
| **Level** | **Committee Meeting** | **Timing** | **Discussion** |
| Board | BROC Meeting | Six times in a year | Policies and procedures |
| Departmental / Functional | ManCom Meeting | Once a month | Risk Priorities per SBU |
|  | EPC Subcommittees  BU Subcommittees | Once a month per committee | Risk Register per SBU (all risks) |
| On-going Projects | Project Operations Committee Meeting | Once a month per project | Risk Register per Project |
| Projects for Bid | Management Investment Committee Meeting  Bid Management Review | Twice a month  As the need arises, per bid | Potential Risks  Potential Risks |

## FOLLOW-UP AUDIT

|  |  |
| --- | --- |
| * + 1. **Track the status and monitor milestones**   **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | Responsibility: **Internal Auditor** |
| * Shall track status and monitor milestones established in the management action plan. Status monitoring of observations and recommendations performed every quarter to:   + Monitor the disposition of the results communicated to the management; and   + Ensure agreed management actions have been effectively implemented or that senior management has accepted the risk of not taking action.   Post-audit procedures will be conducted to validate actions taken and the results will be reported to the Chairman of the Board & President and the Audit Committee. |

## FRAUD AUDITING

Diagnosing vulnerabilities to fraud and detecting gaps in anti-fraud controls shall form part of the enterprise risk assessment performed by the Internal Auditors during audit planning. The Internal Auditor shall evaluate, but not limited to, the following:

* Effectiveness of the design and implementation of anti-fraud controls (including monitoring of financial ratios for detecting suspicious activities)
* Culture, attitude, and awareness among employees regarding about their knowledge and response to any fraud or misconduct, including Whistleblowing Policy
* HRD’s policies and practices in terms of hiring (background investigation), promotions and exit interviews
* Preventive Controls on the process-level controls that are designed to mitigate the opportunity for an individual to perpetrate fraud and limit the extend or fraud, and other actions that will serve as deterrent by creating an additional obstacle to carrying out a fraud. This includes check-and-balance, limit of computer access, signing approval matrix. Implementing processes and control improvements enterprise-wide to gain efficiencies and prevent recurrences
* Feedback or reporting mechanisms for customers, suppliers, external parties with copies of your ethics guidelines (e.g., survey), whistleblower hotline

The following shall warrant the ACC and IAD to initiate a fraud investigation:

|  |  |
| --- | --- |
| **Possible Fraud Concern** | **Examples** |
| 1. Financial reporting | * Falsification or destruction of business/financial records * Misrepresentation or suppression of financial information * Non-adherence to internal financial reporting policy/controls * Management overrides * Auditor independence concerns |
| 1. Suspected Fraudulent Activity | * Theft * Misappropriation of assets * Defalcation (e.g., misappropriation of money) * Unlawful or improper payment |
| 1. Breaches of the Guidelines and Other Compliance Policies | * Insider trading and market manipulation * Corrupt practices including giving or receiving bribes or other improper benefits * Conflict of interest concerns * Deliberate cover-up of the inappropriate activity or disruption of investigation * Illegal, deceptive, or anti-competitive sales practices * Other violations of governing regulations * Non-adherence to internal compliance policies. |
| 1. Retaliation or Retribution against an Individual who reports a concerns | * statements, * conduct, or actions involving discharging, demoting, suspending, harassing, or d * discriminating against an individual reporting a concern in good faith and in accordance with this Policy |
| 1. Harmful to the Company | * Any other acts or omissions which are harmful to the public or the Company, or are in violation of the law, the Company’s rules and regulations, and its Code of Business Conduct and Ethics |

|  |  |
| --- | --- |
| * + 1. **Receive fraud complaint**   **TAT: *1-2 Days***  **Timeframe: *Based on Approved Schedule*** | Responsibility: **CIA** |
| * Receive a suspected fraud reporting * Evaluate the validity if it warrants fraud investigation or endorsement to other department or hr   The report log should include information on the following items: · How the organization became aware of the suspected fraud, including the name of any complaining party · The date the issue was raised or reported · The nature of the suspected fraud · Department or divisions involved · Suspect employees or parties · Actions take |
|  | Responsibility: **CIA** |
|  | * he Head of Internal Audit (except in any case involving his or her division) will take the lead when fraud investigations are being conducted   A fraud response plan outlines the actions that members of an organization will take when suspicions of fraud have arisen. Because every fraud is different, the response plan should not outline how a fraud examination should be conducted. Instead, response plans should help organizations manage their responses and create environments to minimize risk and maximize the potential for success. a response plan will allow management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner, and by having a response plan in place, management will send a message that it takes fraud seriously.   * Evaluate persons who can cover up, obstruct, or fail to report (monitor) or any persons that an accessories. Great care shall be taken to ensure that employees in dealing with suspected dishonesty will not be alerted nor treated unfairly/discriminated. Persons who cover up, obstruct, or fail to report (or monitor) a fraud that they become aware of, or ought to have been aware of, may be considered to be an accessory after the fact and may be subject to the Bank’s disciplinary code which could involve action up to and including dismissal. * Identify the details of the incidents facts, suspicions or allegations ad where to obtained them in the most discrete manner. * Identify who will be part of the audit team (do we have capability to join or hire an external documents)   In circumstances where the investigation requires the use of technical expertise, which Internal Audit may not possess, external specialists (subject to the approval of the Governor or Deputy Governors) may be appointed to lead (if the case involves Internal Audit) or to contribute to the investigation   * What are the documents required or evidence - scrutiny from the media, regulators, investors, and law enforcement * • Establishing and documenting fraud investigation protocols * • Identifying fraud investigation resources, especially global response teams, before the occurrence of a crisis * Preventing measures to stop   In general, litigation hold policies should be developed so the organization can: · Promptly notify employees who might possess relevant documents. · Issue a preliminary hold order to all individuals and employees who might possess relevant information. · Promptly notify information technology (IT) personnel and get their involvement if electronic data is at issue. · Notify employees and IT personnel of their duty to preserve. · Suspend any deletion protocols. · Prohibit the destruction, loss, or alteration of any potentially relevant documents. · Prohibit employees from destroying, hiding, or manipulating documents. · Alert employees as to the risk to the company and the employees if they fail to heed the litigation hold request |
|  | * a response plan will allow management to respond to suspected and detected incidents of fraud in a consistent and comprehensive manner, and by having a response plan in place, management will send a message that it takes fraud seriously. |
|  | * Where the Head of Internal Audit report provides reasonable grounds for suspecting an employee or employees of fraud or a dishonest activity, the Governor in consultation with the Human Resources Director, the Head of Internal Audit, and other relevant Bank officers, will decide if any actions are necessary to deal with the situation and/or prevent further loss. This may require the suspension with or without pay of the employee(s) (which will take place in accordance with Disciplinary Procedures) and/or a decision as to whether further investigation is required. |
|  | * Discuss with ACC the plan and audit team |
|  | * Where further investigation is required the Governor and the Chair of the Audit Committee in consultation with the Head of Internal Audit and other relevant Bank officers will determine the format and nature of the investigation |
|  | * Initial investigation Once fraud or corruption has been reported it must be handled confidentially, treated seriously and investigated competently. The department will explore all reports of fraud or corruption. All reports received by management will be submitted to the Fraud Control Officer and Public Interest Disclosure Coordinator. Within the department, the Fraud Control Officer and Public Interest Disclosure Coordinator is the Deputy Director General, Finance Strategy and Operations. The Fraud Control Officer and Public Interest Disclosure Coordinator will: § record all reports received § maintain confidentiality throughout the assessment and review § make an initial assessment of each report and determine the appropriate action to be taken § coordinate the initial investigation by nominating an appropriate investigator in a timely manner to conduct an investigation to establish whether there is a reasonable basis for believing that fraud may have occurred § ensure the investigating officer produces an investigation plan and is provided with full access and cooperation § keep all parties involved in the matter informed of status and process § report to the Director General on the results of each investigation and recommendation |
|  | * ensure that approved recommendations are implemented. Where actual or suspected corruption has been identified and reported to management, the Director General must notify ICAC as required under the ICAC Act 1988. In the case of fraud, during the initial investigation phase the aim is to impartially gather, assess and report facts rather than act as a prosecutor or advocate. The department aims to complete all initial investigations within 3 months. If, following the initial investigation, a reasonable basis appears to have been established for believing that fraud may indeed have occurred, the Director General must report the matter to the Police and likewise advise the ICAC. In this regard, the Personnel Handbook (Chapter 9, Section 9.9.2) states: “… the Department should advise the Police if the matter is also subject to an internal investigation. Unless there will be an impact on the Police investigation, there is usually no need to suspend the internal investigation. If appropriate all stages of dealing with the matter as a disciplinary matter may be taken. If all stages are not completed and the officer is charged criminally it is usually appropriate to await the outcome of the court proceedings. If the Police indicate that an internal investigation should be suspended, the grounds and reasons should be noted. Contact should be maintained with the Police, to ensure internal issues can be dealt with as quickly as possible.” 3. Further investigations |
|  | * Further investigations If the matter is reported to the Police and ICAC, the issue of further investigation of the alleged offence will be discussed with all parties involved in the matter in order to establish a satisfactory approach. If the department needs to conduct further investigations, it is most likely that the services of an independent investigator will be utilised. Investigation actions should be consistent with commonly used best practice investigation standards, such as the ICAC Investigation handbook - A guide to conducting internal investigations, Fact Finder, March 2012. Ensuring the quality of outsourced investigations remains a departmental responsibility. Where it has been discussed and agreed with the external authorities that further investigation of a suspected fraud situation should be undertaken by the department (using an independent investigator), the next step in the process is the development of an investigation plan. Departmental management will not become directly involved in an external investigation process or attempt to unduly influence the final report. Inquiries are specialised undertakings and require true independence to operate efficiently and effectively. The independent investigator will be asked to plan the investigation approach from the outset and to keep management fully informed throughout the process. |
|  | * Code of conduct |
|  | * The Fraud Control Officer and Public Interest Disclosure Coordinator will provide quarterly reports on fraud and corruption matters to the department’s Audit and Risk Committee |
|  | * Litigation Hold Procedures If an organization does not already have litigation hold procedures in place, management should institute them immediately. A litigation hold refers to the steps an organization takes to notify employees to suspend the destruction of potentially relevant records when the duty to preserve information arises. Litigation hold procedures are necessary to ensure that potentially responsive documents are not destroyed once evidence of misconduct arises. The failure to preserve relevant evidence could have several adverse consequences, including, but not limited to, the government’s questioning of the integrity of any fraud investigation, monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defense |
|  | * Preserving Relevant Documents When evidence of fraud arises, management should seek to preserve all relevant documents, especially those that an employee might want to hide or destroy. In a fraud investigation context, the term documents typically refers to, but is not limited to, contracts, invoices, correspondence, memoranda, weekly reports, presentations, telephone messages, emails, reports, performance reviews, performance improvement plans, medical records, and other written or recorded material. When evidence is misplaced, lost, or destroyed, it becomes more difficult to conduct an investigation. Thus, the response team and management must take action to preserve evidence as soon as the decision to investigate is made. There are a number of steps that management should take to preserve relevant documents. For one thing, management should work with legal counsel to issue a litigation hold to notify employees to suspend the destruction of potentially relevant records. Furthermore, management should suspend the organization’s record retention policy temporarily to avoid a piece of evidence accidentally being destroyed.   Also, management could lockdown access to emails or digital files that employees might want to conceal or destroy. Digital information can be found in virtually any type of media, and it is more fragile than tangible evidence. Therefore, employees can destroy this type of information if it is not protected properly. Often, when fraudsters become aware of an investigation, they try to destroy evidence in their computers or sabotage other evidence that could be used against them. Accordingly, it is a good idea to have IT personnel involved in this process each time the organization decides to conduct an investigation. The failure to preserve documents required to be maintained by statute or regulation could have several adverse consequences. First, the failure to preserve documents could result in the government’s questioning of the integrity of any fraud investigation. Second, documents destroyed when litigation is expected, or in progress, might give rise to claims of spoliation of evidence, which, if proven, could lead to monetary fines and sanctions, adverse inference jury instruction sanctions, or dismissal of claims or defenses. Spoliation is broadly defined as the act of intentionally or negligently destroying documents relevant to litigation. In today’s digital environment, digital spoliation is a major concern for organizations involved in litigation. When compared to the spoliation of tangible documents, digital spoliation carries additional risks. Management often lacks sufficient knowledge of the inventory of digital information, and electronic data might only be available for an evanescent time. Additional concerns include business practices designed to free up storage space by deleting digital information and the fact that electronic data can reside in numerous locations, as well as the fact that identifying relevant electronic data within today’s large and complex data systems can be challenging and costly. |

# 6.0 [FORMS & TEMPLATES](#TOC)

6.1 [CEO Approval Deck](https://megawideph.sharepoint.com/:p:/s/BusinessDevelopment-BDProcesses/EQ3Q7uDtWVdAiN2V_mVux80BGCXNcAAsTIM2efFob4OeKw?e=f6iAt0)

6.2 [Minutes of the Meeting](https://megawideph.sharepoint.com/:w:/s/BusinessDevelopment-BDProcesses/EXWJSeYXshNErgz5prYenKwBHGmNx7fjxsb2bD5PZ2Qy0w?e=uv5S4g)

# 7.0 [REFERENCES](#TOC)

## 7.1 Megawide EPC: 5PLMC Process

## 7.2 HoldCo Corporate Finance and Planning Business Process

# [ANNEXES](#TOC)

## [Glossary of Terms](#TOC)

**Accounting and Comptrollership**

see HoldCo Comptrollership Manual.

**Authority** contingent on the partnership or business Structure of the project, this may be composed of, but shall not be limited to, a joint committee between Megawide and an external party, assigned individuals from concerned and/or relevant SBUs, or assigned individuals agreed upon by the parties involved. However, in the event that the Authority is not yet defined, it shall de facto be composed of the MIC.

**AVP** Assistant Vice President.

**Bathymetric survey**

measures the depth of a water body as well as map the underwater features of a water body.

**BD** the Business Development Department of the Megawide Holding Company.

[**BD@megawide.com.ph**](mailto:BD@megawide.com.ph)

the email address that may be used by individuals interested in communicating with HoldCo BD. This is published on the Megawide website, and is a group email. To access this, please consult with or refer to procedures of Megawide’s Information and Technology Department.

**Business Implementation Plan**

the document that shall document all the planning and strategies used to implement the project.

**CAPEX** capital expenses, refers to expenses related to fixed structures or equipment required for the implementation of the project.

**CEO** Chief Executive Officer.

**Channel** a file and information sharing feature on MS Teams.

**Company**  Megawide Construction Corporation, duly organized and registered under the laws of the Philippines.

**Concept Massing** this consists of images or drawings showing the general shape and form of the project based on the Initial Concept Design.

**Consultancy / Service Agreement**

depending on the required service, this is the agreement detailing the terms of service as agreed on between Megawide and the potential consultant.

**Core testing / rebar testing**

test to measure the tensile strength of rebar steel and the tensile rebar-concrete bond strength.

**Corporate Finance and Planning**

see HoldCo Corporate Finance and Planning Manual.

**Counterparty** refers to the potential or engaged external party in a partnership.

**Design Criteria / Parameters**

refers to the operational qualities, features, and related requirements that must be considered in the design of project.

**Feasibility Study** a study undertaken to determine in detail the viability of a project. The study may include a summary of the proposed business model, partnership structure, technical analysis, financial model, economic model (if required) and other components depending on each project. The study shall be done in consideration of Megawide’s investment appetite, and its capability to implement in relation to available resources, and relevant external forces.

**Establish Business Requirement activity**

establishes critical activities of an enterprise that must be performed to meet the organizational objective(s) while remaining solution independent. A business requirements document (BRD) details the business solution for a project including the documentation of customer needs and expectations.

**HoldCo** the Megawide Holding Company.

**HoldCo BD** the Business Development Department of the Megawide Holding Company.

**HoldCo CFP** Corporate Finance and Planning section of the Finance Department of the Megawide Holding Company.

**HoldCo Corp Affairs**

the Corporate Affairs Department of the Megawide Holding Company.

**HoldCo Legal** the Legal Department of the Megawide Holding Company.

**Hydrological flood study**

study of movement of water, including the volume and rate of flow as it moves through a watershed, basin, channel, or man-made structure.

**Initial Concept Design**

refers to design based on preliminary data, high-level due diligence, and some desktop research.

**Investor Relations** see HoldCo Comptrollership Manual.

**Manual** pertains to this document that outlines the process of the department.

**MCC** Megawide Construction Corporation, duly organized and registered under the laws of the Philippines.

**Megawide** refers to the Megawide Holding Company, its Strategic Business Units, and its affiliate companies, or Megawide’s group of companies.

**Megawide EPC** refers to the specific SBU that leads Megawide’s primary operations of engineering, procurement, and construction.

**MIC** Management Investment Committee is composed of heads of the key departments of the Holding Company relevant to the decisions made in the company’s strategic investment.

**Minutes of the Meeting**

refers to the document listing the details and points of discussion of a specific meeting.

**MM Subway Project**

the Metro Manila Subway Project is the underground railway project of the Department of Transportation along the alignment of EDSA.

**MoA** Memorandum of Agreement is a agreement detailing the terms as agreed on by Megawide and the involved parties.

**MoU** Memorandum of Understanding is a agreement detailing the terms as agreed on by Megawide and the involved parties.

**MS Teams** Microsoft Teams, the software program, a digital organization platform used by Megawide for information, data, file sharing and communication.

**NDA** the Non-Disclosure Agreement that is used to protect Megawide from breaches in confidentiality or a leakage of material information.

**NSRP South Commuter**

the North-South Railway Project South Commuter is the Department of Transportation project to develop the Philippine National Railways’ rail-based transportation alignment between Tutuban to Calamba. This is tendered in several packages, cutting the alignment into to shorter sections, and separating the tenders for the operations and maintenance, supply, and installation of electro-mechanical works.

**O&M** operations and maintenance; reference to all functions, duties and labor associated with the daily operations and normal repairs, replacement of parts and structural components, and other activities needed to preserve an asset so that it continues to provide acceptable services and achieves its expected life.

**OPEX** operational expenses, refers to expenses related O&M activities.

**Opportunistic projects**

refers to projects that are not included in Megawide’s strategy map, but are considered to have potential viability if executed or awarded.

**PITx** the Paranaque Integrated Terminal Exchange is a road-based terminal that serves as an intermodal hub for connections between Metro Manila, Cavite, and other areas south of Metro Manila.

**Pre-Feasibility Study**

preliminary study undertaken to determine, analyze, and select the best business scenarios, significantly based on benchmarks and general industry behavior. In this study, we assume we have more than one business scenario, then we want to know which one is the best, both technically and financially.

**Project Budget** this refers to the budget that shall be proposed primarily in anticipation of the work required to complete the studies until the Award & Closing activities.

**Project Management Team / Project Steering Committee**

the main governing body accountable for the execution of the project.

**Project Risk Register**

refers to the file which details all the anticipated risks and mitigation plans used for the purpose of project planning and risk management.

**Project Team** refers to the group that shall implement the development of the project with members of HoldCo BD throughout the Pre-Award Planning stage.

**Project Team Lead**

the individual assigned to lead the development of the project. Often, this is an employee from Megawide EPC.

**Project Work Program**

the list of activities and anticipated timeline in which these must occur.

**SBU** Strategic Business Units.

**SD-1** Schematic Design-1 is a detailed design producing architectural, engineering, and other related drawings, usually detailing more specific requirements for the construction of the project.

**Soil investigation** physical testing on site to understand the ground conditions for geotechnical design (foundations, retaining walls & soil improvement).

**Stakeholder Map**

the file that lists and details stakeholders relevant to the implementation of the project.

**Structural investigation**

checking of the adequacy, structural integrity and soundness of structures and their components.

**TCD** Transport-Centric Development refers to projects in relation to road-based transportation infrastructure.

**Technical/land survey**

carried out to understand land boundaries and is performed in order to locate, describe, monument, and map the boundaries and corners of a parcel of land. It might also include the topography of the parcel, and the location of buildings and other improvements made to the parcel.

**TOR** the Terms of Reference is the list of activities detailing the scope of work for a potential consultant.

**Traffic impact assessment (TIA)**

technical analysis of traffic problems and safety issues relating to specific development. The objective of TIA is to identify and report whether a particular development project will have an impact on the safety and efficiency of adjacent roads.