A project plan designed to understand, analyze, propose, and implement improvements to your organization's logging posture, specifically aligning with MAS TRM guidelines and notices.

**Project Plan: Enhancing MAS TRM Logging Compliance**

**Project Title:** MAS TRM Logging Maturity Improvement Project

**Project Goal:** To ensure the organization's logging infrastructure and practices fully comply with MAS Technology Risk Management (TRM) Guidelines and Notices, enhancing cyber resilience and auditability.

**Project Duration Estimate:** 12-24 weeks (Highly dependent on current maturity, scope, and resource availability)

**Key Assumptions:**

* Access to relevant IT systems, configurations, logs, and documentation will be provided promptly.
* Key personnel (IT operations, security, application owners, compliance) will be available for interviews and workshops.
* Budget and resources (tools, personnel) for proposed solutions will be approved.
* Existing log data is accessible for initial review (even if not optimally managed).
* Any critical findings will be addressed immediately as high-priority security incidents.

**Success Criteria:**

* A comprehensive understanding of the current logging state is documented.
* Identified gaps against MAS TRM requirements are clearly documented and prioritized.
* Approved proposals for remediation and enhancement are in place.
* Implemented logging controls meet MAS TRM guidelines and notices, as validated by internal/external audit.
* Improved ability to detect, investigate, and report security incidents.

**Phase 1: Understand Current Status (As-Is Assessment)**

* **Objective:** To gain a comprehensive understanding of the existing logging infrastructure, capabilities, and operational practices across the organization.
* **Estimated Duration:** 3-4 Weeks
* **Key Activities:**
  + **1.1 Kick-off Meeting:** Introduce project, scope, objectives, and roles to key stakeholders.
  + **1.2 Document Review:**
    - Collect and review existing IT policies, security policies, logging policies, incident response plans.
    - Review architecture diagrams (network, application, data flow).
    - Review existing IT asset inventory, focusing on critical systems.
    - Gather information on current log sources (types of logs generated: OS, application, database, network, security devices, cloud services).
    - Identify existing log collection, storage, and retention mechanisms/tools.
    - Identify existing log monitoring, analysis, and alerting processes/tools (e.g., SIEM, custom scripts).
  + **1.3 Stakeholder Interviews & Workshops:**
    - Conduct interviews with IT Operations, Security Operations Center (SOC) team, Application Owners, Database Administrators, Network Engineers, Cloud Engineers, Compliance/Risk personnel.
    - Discuss current logging practices, challenges, pain points, and unlogged critical events.
    - Understand incident detection and response workflows.
  + **1.4 Technical Verification (Initial Scan/Sampling):**
    - Verify logging configurations on a sample of critical systems (OS audit logs, application logging levels, database auditing).
    - Inspect log files/streams for content and format on selected systems.
    - Assess the protection mechanisms for logs (access controls, integrity).
    - Map log flows from sources to storage/analysis platforms.
* **Deliverables:**
  + Project Charter & Communication Plan.
  + Current State Assessment Report (documenting findings on what is logged, how, where, by whom, and current tools/processes).
  + Initial inventory of log sources and critical systems.
* **Key Stakeholders:** Project Sponsor, Project Manager, IT Ops Leads, Security Ops Leads, Application Owners, Database Owners, Network Team, Cloud Team.
* **Dependencies:** Stakeholder availability, access to documentation and systems.

**Phase 2: Confirm (Stakeholder Validation & Alignment)**

* **Objective:** To validate the accuracy of the "current status" findings with relevant stakeholders and gain consensus before proceeding to gap analysis.
* **Estimated Duration:** 1-2 Weeks
* **Key Activities:**
  + **2.1 Review Sessions:** Present the "Current State Assessment Report" to key stakeholders.
  + **2.2 Feedback Collection:** Gather formal and informal feedback on the accuracy, completeness, and interpretation of findings.
  + **2.3 Consensus Building:** Facilitate discussions to resolve discrepancies and ensure a shared understanding of the current state.
  + **2.4 Baseline Definition (Initial):** Re-confirm the critical systems and information requiring logging based on business criticality and regulatory impact.
* **Deliverables:**
  + Signed-off "Current State Assessment Report."
  + Confirmed list of critical assets for MAS TRM logging scope.
* **Key Stakeholders:** All stakeholders from Phase 1, especially Senior Management and Compliance.
* **Dependencies:** Completion of Phase 1.

**Phase 3: Perform Gap Analysis (Current vs. MAS TRM)**

* **Objective:** To identify and document the discrepancies (gaps) between the current logging state and MAS TRM Guidelines/Notices, including the severity and risk associated with each gap.
* **Estimated Duration:** 3-4 Weeks
* **Key Activities:**
  + **3.1 MAS TRM Review & Interpretation:** Detailed review of all relevant MAS TRM Guidelines (Sec 12.2, 5.4.3, 10.4.1 etc.) and applicable TRM Notices (FSM-NXX, CHN) specifically for logging requirements.
  + **3.2 Gap Identification:** Compare each point from the MAS TRM Logging Checklist (provided previously) against the confirmed "Current State."
  + **3.3 Risk Assessment & Prioritization:**
    - Assess the risk associated with each identified gap (e.g., High, Medium, Low based on likelihood x impact).
    - Prioritize gaps based on risk level, MAS mandatory requirements, and business impact.
  + **3.4 Root Cause Analysis (Preliminary):** For significant gaps, identify potential underlying reasons (e.g., lack of tools, resource constraints, awareness, policy gaps).
* **Deliverables:**
  + Detailed Gap Analysis Report (including MAS reference, current state, gap description, risk rating, and preliminary root cause).
  + Prioritized list of logging gaps.
* **Key Stakeholders:** Security Team, Compliance/Risk, Legal.
* **Dependencies:** Signed-off "Current State Assessment," current MAS TRM documentation.

**Phase 4: Propose (Solutions & Roadmap)**

* **Objective:** To develop and propose actionable solutions, a remediation roadmap, and resource requirements to close identified gaps and enhance logging maturity.
* **Estimated Duration:** 3-5 Weeks
* **Key Activities:**
  + **4.1 Solution Design:**
    - For each prioritized gap, propose one or more remediation options (e.g., new tool, configuration change, process improvement, training).
    - Consider various architectural options (e.g., expanding existing SIEM, new log management solution, cloud-native logging).
    - Define required logging content and format standards.
    - Design improved log retention and integrity mechanisms.
    - Design enhanced monitoring, alerting, and anomaly detection rules/use cases.
    - Develop or update logging policies and procedures.
  + **4.2 Cost-Benefit Analysis:** For significant proposals, outline estimated costs (tools, licensing, personnel) vs. benefits (reduced risk, improved compliance, operational efficiency).
  + **4.3 Develop Remediation Roadmap:** Create a phased plan with timelines, dependencies, and owners for addressing prioritized gaps.
  + **4.4 Business Case & Presentation:** Prepare a comprehensive proposal document and presentation for management approval.
* **Deliverables:**
  + Logging Remediation Plan & Roadmap.
  + Solution Architecture Design for improved logging (if applicable).
  + Updated Logging Policy and/or Standards drafts.
  + Business Case for investment (if required).
  + Presentation to management for approval.
* **Key Stakeholders:** Project Sponsor, IT Management, Security Management, Finance (for budget approval), Compliance.
* **Dependencies:** Completed Gap Analysis Report, vendor engagement (if new tools are considered).

**Phase 5: Implementation (Execute & Verify)**

* **Objective:** To implement the approved logging enhancements, verify their effectiveness, and ensure ongoing compliance and operationalization.
* **Estimated Duration:** 4-8 Weeks (Initial Phase, ongoing for larger rollouts)
* **Key Activities:**
  + **5.1 Planning & Resource Allocation:** Finalize detailed implementation plans, assign resources, and establish communication channels.
  + **5.2 Tool Deployment & Configuration (if applicable):** Deploy and configure new log management tools, SIEM, or security solutions.
  + **5.3 Log Source Integration:** Configure individual systems (OS, applications, databases, network devices, cloud services) to send logs to the centralized platform.
  + **5.4 Content & Rule Development:** Develop/refine log parsing rules, correlation rules, dashboards, and automated alerts within the log management/SIEM platform.
  + **5.5 Policy & Procedure Implementation:** Implement updated logging policies, standards, and Standard Operating Procedures (SOPs).
  + **5.6 Training:** Provide training to IT operations, security analysts, and relevant personnel on new tools, processes, and their roles in logging and monitoring.
  + **5.7 Testing & Validation:** Conduct comprehensive testing to verify:
    - Logs are being collected completely and correctly.
    - Log integrity mechanisms are functioning.
    - Alerts are firing as expected.
    - Logs are searchable and usable for investigations.
  + **5.8 Post-Implementation Review:** Review the project's success against objectives and ensure operational handover.
  + **5.9 Continuous Improvement:** Establish a framework for continuous monitoring, periodic review, and improvement of logging practices.
* **Deliverables:**
  + Implemented Logging Infrastructure and Controls.
  + Updated Logging Configurations and SIEM rules.
  + Formalized Logging Policy and SOPs.
  + Training materials and completed training sessions.
  + Post-Implementation Review Report.
* **Key Stakeholders:** IT Ops, Security Ops, Project Manager, Compliance, Internal Audit.
* **Dependencies:** Approved Proposal and Budget, vendor support (if applicable).