M&M CONSULTING

PROTOCOL · VERSION 1.0

MR³ AI Governance Protocol

Rules for the responsible use of artificial intelligence in financial analysis and decision support, aligned with the NIST AI Risk Management Framework.

AUTHOR
Mario Rodríguez Aguilera

ORGANIZATION
Consulting M&M LLC · Florida, USA

VERSION
1.0 · October 2026

PART OF
The MR³ Framework, Annex A

MR³ AI Governance Protocol

How artificial intelligence is used inside MR³ engagements: what it may do, what it may never do, who validates it and how it is recorded.

> **Principle.** AI is a decision-support instrument, never a decision-maker. Every material financial recommendation is validated by a named person, and no AI system executes financial transactions.

A.1 Scope of permitted uses

Permitted (with human validation)	Not permitted
Drafting scenario models and sensitivity tables	Approving or executing payments, transfers or restructurings
Variance analysis between budget and actuals	Making credit, hiring or capital-allocation decisions
Summarizing financial statements and trends	Processing personal or client data beyond what the task requires
Flagging threshold breaches and anomalies	Producing figures that enter official reports without review
Preparing first drafts of reports for review	Using tools not approved for the engagement

A.2 Validation workflow

1. **Request.** The task, data used and approved tool are recorded.
2. **Output.** The AI output is saved with date and version.
3. **Review.** A named reviewer checks figures against source data and assumptions.
4. **Decision.** The reviewer approves, corrects or rejects; the decision-maker is a person.
5. **Log.** Request, output, reviewer, changes and final decision remain in the engagement record.

A.3 Alignment with the NIST AI Risk Management Framework

NIST function	MR³ controls
Govern	Written AI-use policy per engagement; named owner and reviewers; approved-tools list; staff guidance on confidentiality; non-autonomous execution policy
Map	Each AI use is linked to a specific decision and its financial impact; data sources and limits are documented; high-impact decisions (debt, capital, payroll) are identified in advance
Measure	Outputs are reconciled with source figures; error and correction rates are tracked; periodic review of outputs for bias or systematic error
Manage	Threshold-based escalation to leadership; ability to suspend a tool or use; incident log and corrective actions; annual protocol review

A.4 Data protection

- Data minimization: only the data required for the task is shared with an AI tool.
- Client-identifying information is removed or masked whenever the analysis allows it.
- Access is role-based and protected with multi-factor authentication.
- Engagement records are retained for audit and traceability.

A.5 Roles

Role	Responsibility
Engagement lead	Approves AI uses for the engagement and owns the protocol
Reviewer	Validates each material output against source data before use
Decision-maker (client leadership)	Makes the final decision; never delegated to an AI system

A.6 Review triggers

The protocol is reviewed at least once a year and whenever a new tool is introduced, an output error reaches a decision, or applicable regulation or guidance changes.

A.7 Evidence of practice

Structured protocols for the governed use of analytical tools, preserving human accountability, have been implemented in prior engagements and attested in writing by client leadership (see Section 8 of the MR³ white paper).

Reference: National Institute of Standards and Technology, *Artificial Intelligence Risk Management Framework (AI RMF 1.0)*, NIST AI 100-1, January 2023. This protocol is aligned with the framework's functions; it is not a certification by NIST.