ARCHITECTING GENAI COMMUNICATION PROTOCOLS

Model Context Protocol & Agent-to-Agent Protocol

~Shreya Singh

Building a better working world

Why Structured Communication is Non-Negotiable in GenAI

- Modern GenAI systems are multi-step, multi-agent, and context-sensitive.
- Protocols standardize communication between agents and memory systems.
- Helps EY deliver scalable, auditable, and modular GenAI solutions.

MODEL CONTEXT PROTOCOL – KEEPING CONVERSATIONS INTELLIGENT

- Defines how AI systems store, reference, and recall context.
- Example: Multi-turn conversations, document understanding.
- Essential for tools like internal copilots and dynamic query engines.

COMPANY RELEVANCE: WHERE MODEL CONTEXT PROTOCOL FITS

- Internal assistants summarizing regulatory docs.
- Long-chain question answering from EY's knowledge base.
- Context-aware task management assistants for audit teams.

AGENT-TO-AGENT PROTOCOL – MODULARIZING INTELLIGENCE

- Standard way for AI agents to pass data, tasks, or intent.
- Prevents redundancy, enables modular flows.
- Think: Summarizer agent → Validator agent → Formatter agent.

HOW EY CAN LEVERAGE AGENT MESHES IN GENAI SYSTEMS

- Automated engagement letter drafting from client inputs.
- Multi-agent pipeline for regulatory compliance checks.
- Risk scoring agents handing off to report generation agents.

PROOF OF CONCEPT (POC)

- **Concept 1 – Intelligent Audit Document Pipeline (Multi-Agent Audit Analyzer)**
- **Flow**: Parser Agent → 2. Clause Extractor → 3. Compliance Verifier
- **Context Protocol**: Retains document metadata
- **A2A Protocol**: Transfers compliance states downstream
- **Concept 2 – Autonomous Deal Assessment Framework (M&A Deal Review Bot)**
- **Functionality:**
- Contextual review of NDAs, financials, and deal terms
- Uses past case flags and threshold matchers
- Final output auto-formatted for Partner review
- **Concept 3 – Self-Navigating Policy AI Agent Network (EY Policy Navigator)**
- **Use Case:**
- Query: “Can I expense XYZ while on client site?”
- Retriever Agent → Policy Matcher → Approval Tracker
- Removes manual HR/legal lookup

EY Building a better working world

BUILDING THE ARCHITECTURE – EY-READY IMPLEMENTATION STACK

Tech Stack:

- OpenAI API, LangChain, Azure/OpenSearch, FastAPI

Security:

- Role-based masking, tenant isolation, data sanitization

Integration:

- Microsoft ecosystem (Teams, Outlook, SharePoint)

EY Building a better working world

DESIGNING WITH PROTOCOLS: INTERPLAY OF CONTEXT & COORDINATION

Feature	Model Context Protocol	Agent-to-Agent Protocol
Use	Memory, continuity	Modularity, interoperability
Risk	Context leakage	Message mismatch
Benefit	Smarter, personalized AI	Task handoff & scaling

CAPABILITIES AND LIMITATIONS

Capabilities – MCP & A2A Protocols

- **Context-Aware Intelligence**
  MCP enables memory and smarter multi-turn conversations.
- **Modular Task Execution**
  A2A allows agents to coordinate and delegate tasks efficiently.
- **Enterprise Fit**
  Designed for secure, auditable, and scalable GenAI at EY.
- **Versatile Applications**
  Supports audit automation, policy queries, deal reviews, etc.

Limitations – MCP & A2A Protocols

- **Context Overload (MCP)**
  Large inputs can reduce performance without summarization.
- **Agent Miscommunication (A2A)**
  Improper handoffs can cause errors without validation.
- **Data Governance Challenges**
  Needs masking, access control, and session limits.
- **Debugging Complexity**
  Multi-agent chains are harder to trace and troubleshoot.

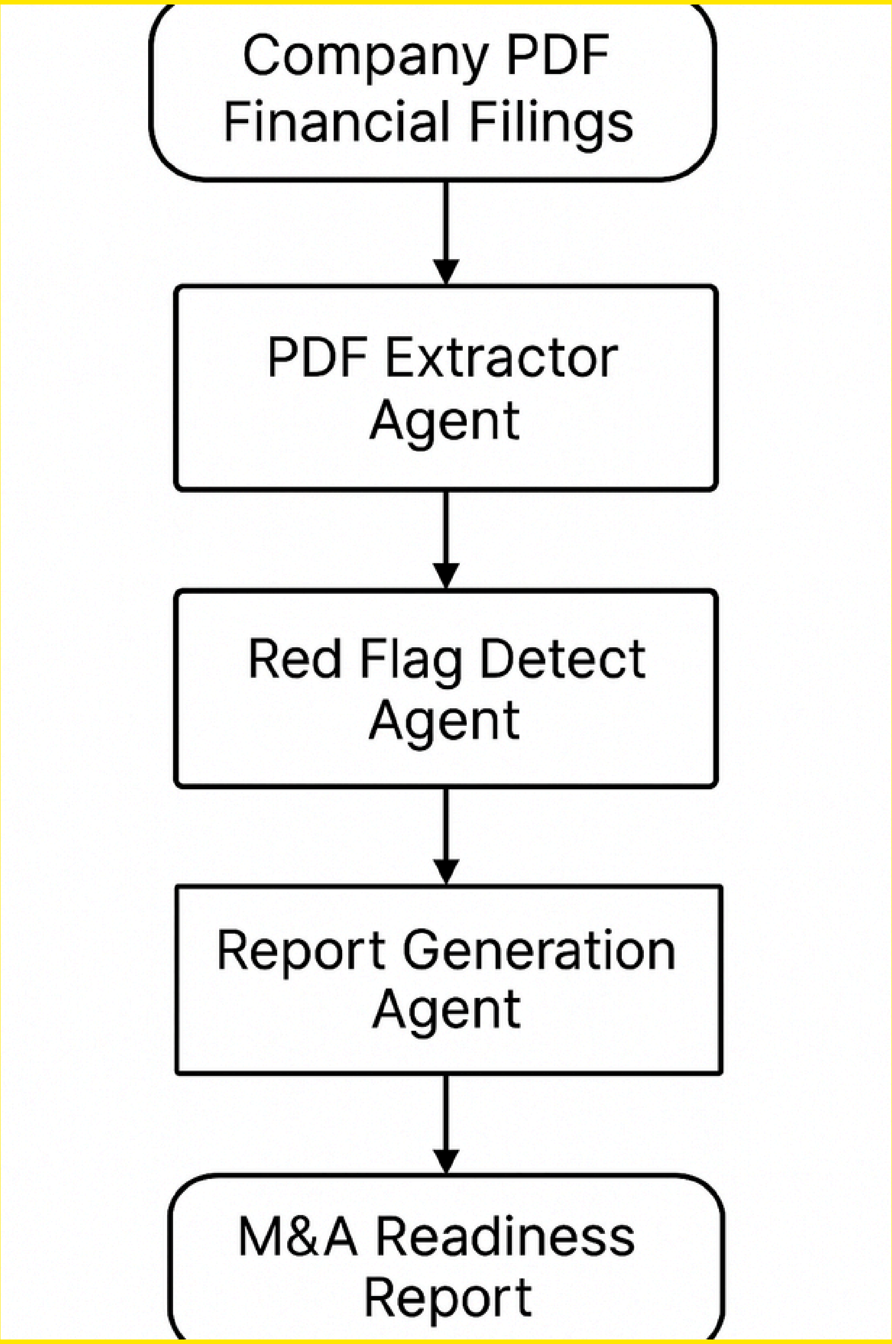
KEY LEARNINGS & STRATEGIC OUTCOMES

- These protocols unlock scale and intelligence in enterprise AI
- Support modular PoCs across EY functions
- Future-ready AI systems will be agent-based and context-rich

PATH FORWARD – FROM CONCEPT TO DEPLOYMENT

- Build pilot: Policy Navigator or Deal Review Bot
- Align with Legal, Risk, and AI Governance
- Evaluate rollout on EY's secure infrastructure

AUTONOMOUS DEAL ASSESSMENT FRAMEWORK (M&A DEAL REVIEW BOT) FLOWCHART



THANK YOU

Building a better working world