Emploi et Développement social Canada | Employment and Social Development Canada

Service Cana

Artificial Intelligence (AI) Reference Architecture

Architectural Review

Architecture is being presented to the Enterprise Architecture Review Board

December 16, 2025

Client Lead:	Daniel Desforges	Branch:	IITB
Lead Architect:	Gita Nurlaila	Responsible Director:	Dominique Bo

e Ask

eking approval for ESDC Artificial Intelligence (AI) Reference Architecture, which includes t
Reference Models and AI capabilities, to be implemented as the architectural guidance and
erence for any upcoming design and implementation of AI solutions.

tiative Outline

ve Description

ficial Intelligence (AI) evolves rapidly, ESDC aims to stay current with user expectation arted the use of AI and Generative AI (Gen AI) as part of its IM/IT implementations. To e the AI and Gen AI implementations, ESDC is creating the AI Reference Architecture to ensure all implementations leveraging AI and GenAI are done in a coherent way to plish an integrated effort. In face of these challenges, the AIRA focuses on the core ce analytics and AI capabilities and develop the architectural building blocks for ESDC mption.

its similar data flow requirement, the AIRA will leverage the previously endorsed nce model of Business Intelligence and Analytics Reference Architecture as the tion and show the evolution of the analytics capabilities that will be improved using AI en AI. The AIRA also attempts to display the various capabilities being enabled in the mental Application Capability Model (DACM) and the technology components that are o define the architecture building blocks.

RA is also aimed to connect the various GC AI strategies and policies from a mental perspective while addressing the gap related to the different definition and ology used across GC.

eliverables

y deliverables consist of 2 parts:
e first part contains AIRA artifacts that establish characteristics for AI architecture by fining a set of AI capabilities that can be used when developing IM/IT solutions that verage AI, as well as AI building blocks and AI Reference Model.
e second part contains the technology components, fit gap analysis and conceptual rget architecture will be added to the AIRA to help address the departmental needs.

nes

ines	Target Date
EARB Approval	2025-12-16
nceptual target architecture EARB Approval	2026-03-24

Drivers

- Strategic
  - Guide departmental strategic visions and objectives on artificial intelligence
  - Strategic planning and roadmap for enhancing departmental artificial intellige capabilities short, medium and long terms
  - Alignment with GC AI Use Policies
- Tactical
  - Need to update the DACM to reflect technology changes
  - Need to identify the AI Building blocks required for AI implementation
  - Need to identify technology components and fit gap analysis against existing implementation for future AI requirements
  - Need to create AI Reference Model to facilitate collaborations on AI initiative

Expected Outcomes

AIRA can be leveraged to yield positive outcomes in many ways, some examples:
- Leverage by decision makers in developing or formulating unified enterprise strategie approaches
- Act as the departmental architectural reference for advanced analytics and AI
- A modern AI architecture, leveraging new advances in technology and multi-layers o advanced analytics

Risks

- Lack of a common vocabulary and interpretation of AI capabilities.
- Potential misalignments and gaps with GC strategic visions, objectives on AI usage a implementation.

hat is AI Reference Architecture (AIRA)

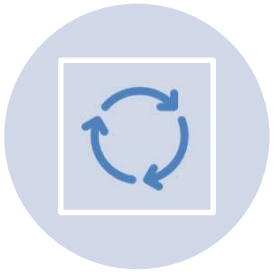
objective of the AIRA is to develop a reusable, enterprise-wide AI Reference Architecture to guide sistent, secure and scalable AI adoption across ESDC. The AIRA identifies the architectural building cks used to develop AI solutions as well as defines a set of AI capabilities that the building blocks nprised of.

the AI technology evolves, the additional elements of AIRA will be added and existing ones will be ated to help address business needs within the department, including:

APPLICATION/TECHNICAL CAPABILITIES

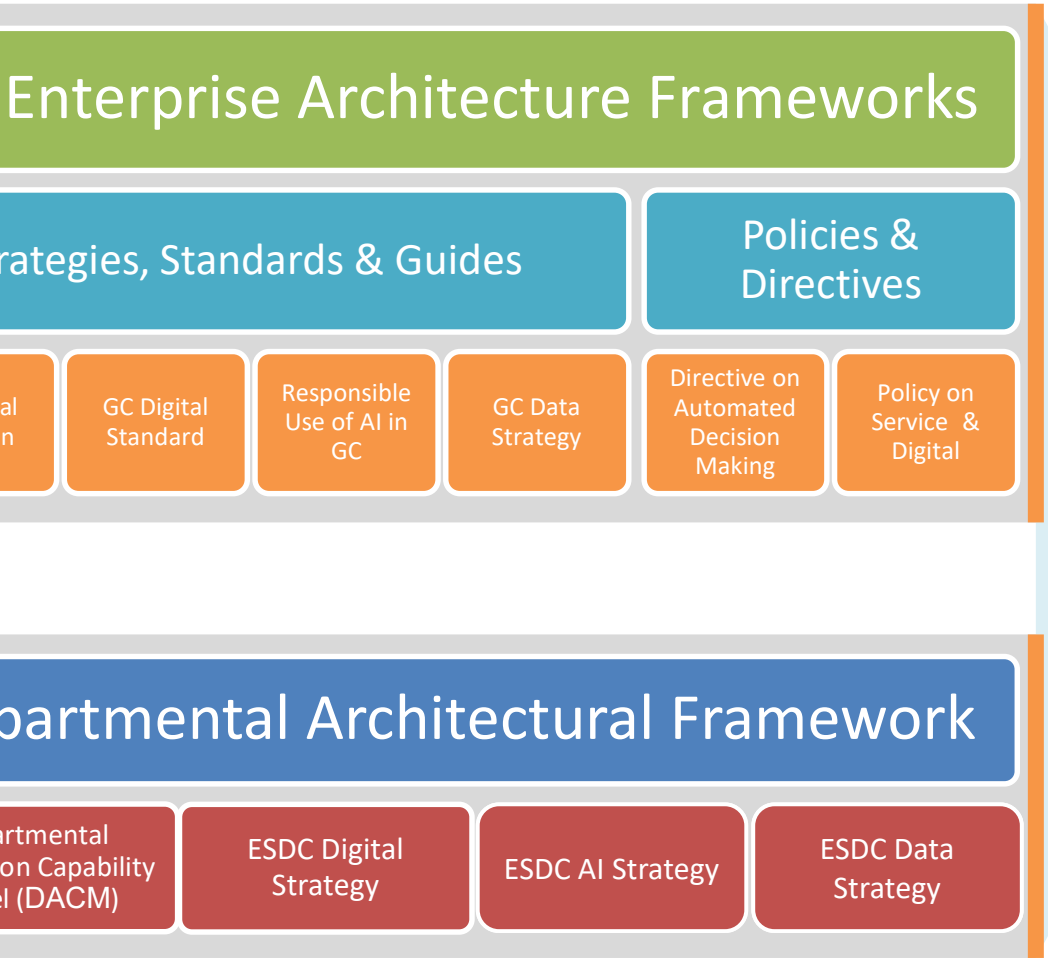
ARCHITECTURE BUILDING BLOCK

STANDARDIZE VOCABULARY



GUIDE AND MODERNIZE IMPLEMENTATION

ndation of the AIRA



ESDC Artificial Intelligence Reference Architecture

- Alignment to key
Enterprise Architect
Frameworks

- Leverage departme
architectural framew

- Help advancement
adoption in ESDC

- Evergreened in kee
with GC and AI
landscape change

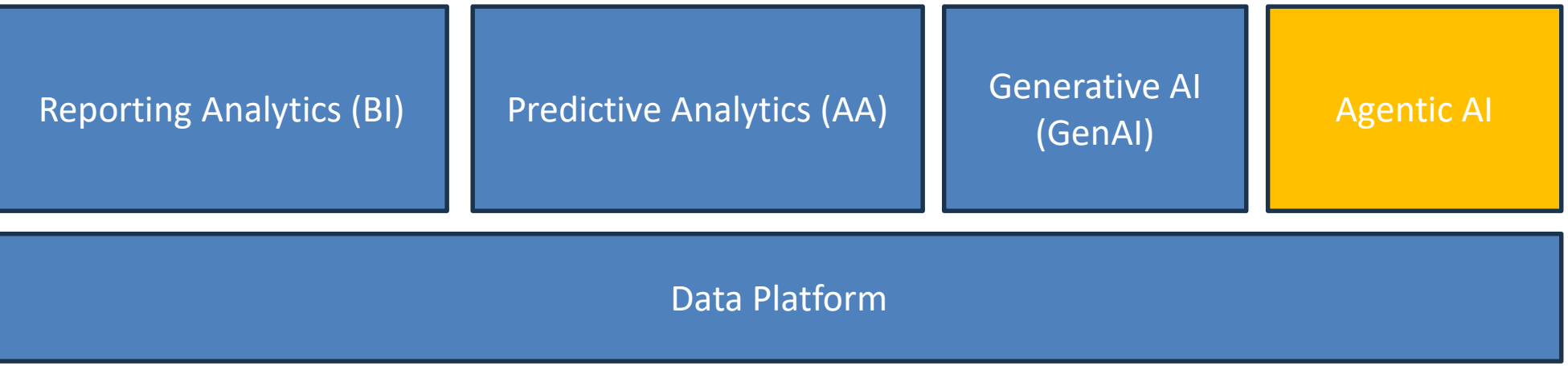
ope of AI Reference Architecture

- Includes: business/data/technology/security/solution capabilities – found elements
- Includes: Architecture Building Block – foundational elements
- Excludes: Tools invoked by AI, eg RPA
- Excludes: Fin Ops

ajor Building Blocks for AI

ndustry, AI implementation typically sits on top of a Data platform, as AI consumes Data.

following outlines AI capabilities can be easily grouped into major architecture building blocks lefine their conceptual mission:



Generative AI: Human-like ability to use language, reason and generate content

Agentic AI: It's GenAI with the ability to execute action plan tasks, perform actions, select and use tools

ously endorsed – BI Analytics Reference Architecture

ure state: EARB approved 2017

Data Integration Architecture

BDM Business Intelligence and Analytics

ources

- Social Media
- Text
- Voice
- Spreadsheets
- External Structured Data
- Cloud: Other Core Systems
- Cloud: Licensed
- Cloud: Public Open

Future Data Sources

- Web
- Image
- Social
- Video

Ingest

- Data Quality
- Batch
- Message
- Synchronisation

Interop

- ESDC Interoperability Platform (ESDC IP)
- GC Interoperability Platform (GC IP)
- Managed Secure File Transfer (MSFT)

Persist and Access

Repository of structured data (Certified)

- Enterprise Data Warehouse
- Repository Data Mart
- Dependant Data Mart
- Conditional Data Mart

Data Lake - Structured/unstructured (Non-Certified)

- Landing Zone
- Single-Tier: Unrefined data repository for data experts
- Two-Tier: Repository & analytics tools
- Three-Tier: Simplified, secured repository & analytics for exploration

Consumption

- Reports
- Real-Time Reporting
- Dashboard
- Scorecard
- Visualisation
  - Geomatics
  - Storyboarding
- Advanced Analytics
  - Artificial Intel
  - Machine Learning
  - Behavioral Analytics
  - Predictive Analytics
  - Big Data Analytics
  - Fraud detection

- Data Discovery
- Datasets (batch)
  - Open data
  - Entre-Exit
- Web API (Sync)
- Alerts (Async)
- Applications
- Optimisation
- Social Media
- Fraud Detection
- Forecasting
- Targeted Outreach
- Collaboration

Virtualisation/Federation

- Integration
- Database
- Delivery

Management

- Data & Analytics Governance
- Master Data Management
- Metadata Management
- Privacy
- Security

AI-specific Security Capabilities*- grouped by CSRA pillars

C1 - Cyber Security Operations

- Secure Model Deployment & Isolation
- AI-Driven Anomaly Detection for Abuse
- Adversarial Threat Detection

C2 – Identity and Credential Access Management

- AI Model Access Control
- Fine-grained Prompt Access Control

C3 - Data and Storage Security

- Model/Data Provenance Tracking
- Model Watermarking & Fingerprinting
- Privacy-preserving AI
- Sensitive Data Masking in Prompts
- RAG Security: Vector DB Access & Embedding Poisoning Defense

C4 - Application Security

- AI Model Input Validation & Sanitization
- Prompt Injection Defense (for LLMs)
- GenAI Response Grounding

C6 - Endpoint Security

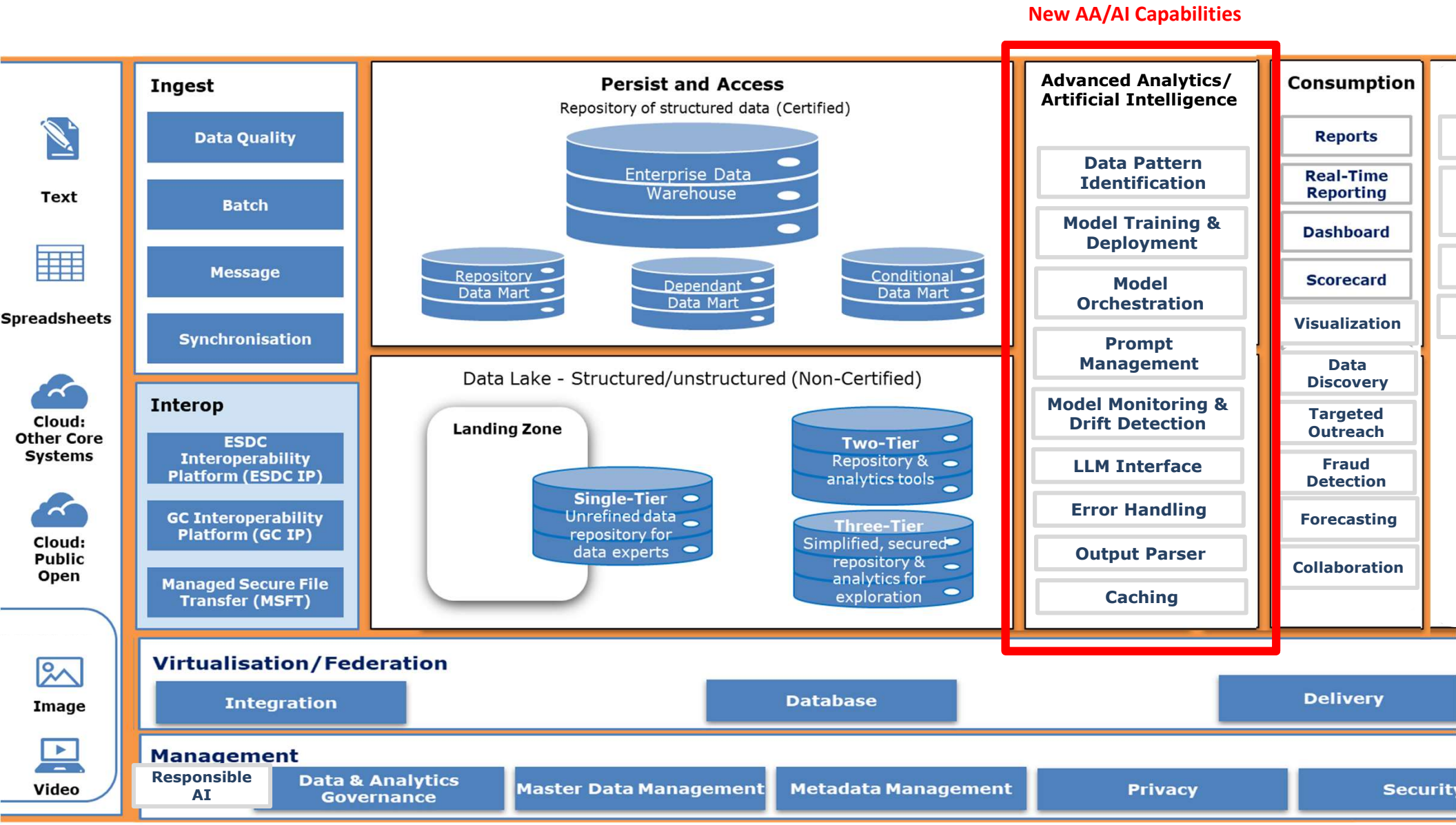
- AI Output Monitoring & Filtering

C7 - IT Risk Management

- Model Versioning & Change Management
- Model Red Teaming
- AI Audit Trails
- AI Model Lifecycle Security
- AI Supply Chain Security
- AI Policy Enforcement & Guardrails
- AI Threat Modeling
- LLM Fine-tuning Control & Oversight

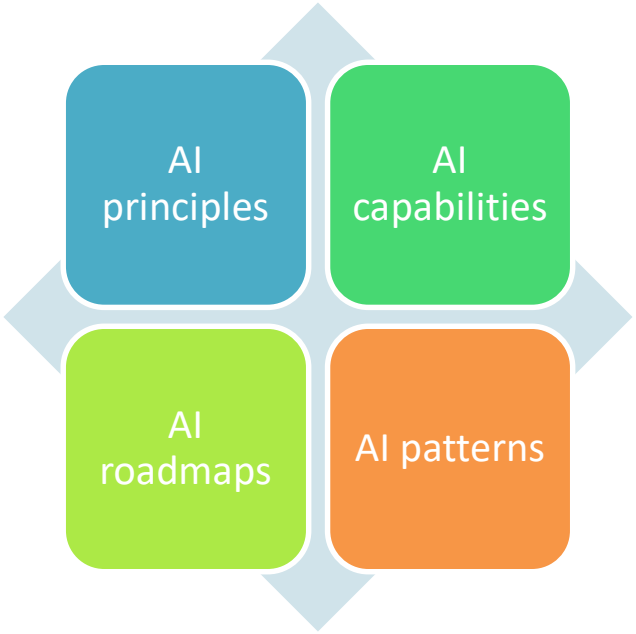
Note *: for definitions, refer to annex slide below

cial Intelligence (AI) Reference Architecture – new AI bilities



w AI Reference Architecture will be used

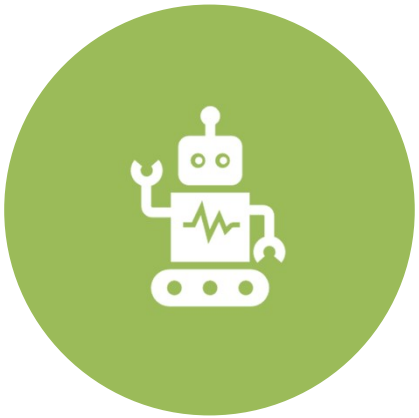
AI Reference Architecture document evolves, additional guidance in the form of :



be developed to offer guidance on how to implement more modern, secure, and flexi
nitectures.

xt steps

ORT TERM: DEVELOP CONCEPTUAL TARGET TATE ARCHITECTURE FOR AI AND GAP FIT ANALYSIS



LONG TERM: CONVERGENCE OF AI & GEN AI IMPLEMENTATION

CONTINUOUS IMPROVEMENT: EVOLUTION O AIRA, INCLUDING BUILDING BLOCK AND TECHNOLOGY COMPONENTS, WHEN APPLICAB

ARB Decision

dorsement for ESDC Artificial Intelligence (AI) Reference Architecture, which includes the
ference Models and AI capabilities, to be implemented as the architectural guidance a
erence for any upcoming design and implementation of AI solutions.

Annexes

nks

Guide on the use of generative artificial intelligence - Canada.ca
Responsible use of artificial intelligence in government - Canada.ca
Generative artificial intelligence (AI) - ITSAP.00.041 - Canadian Centre for Cyber Security
Government of Canada Enterprise Architecture Framework - Canada.ca
ESDC Digital Strategy
Employment and Social Development Canada Data Strategy 2023 to 2026 - Canada.ca

specific Security capabilities* mapped to AI layers & AI uses

AI Security Capability	Data Ingestion	Data Processing	Analytical Data Processing	AA/AI Models	Access	Predictive AI	Generative AI	Agentic AI
AI Model Input Validation & Sanitization	X	X		X	X	X	X	X
AI Model Access Control				X	X	X	X	X
AI Output Monitoring & Filtering				X	X	X	X	X
Model Versioning & Change Management		X	X	X		X	X	X
Adversarial Threat Detection	X	X	X	X	X	X	X	X
AI Audit Trails	X	X	X	X	X	X	X	X
Model/Data Provenance Tracking	X	X	X	X		X	X	X
Privacy-preserving AI	X	X	X	X	X	X	X	X
Secure Model Deployment & Isolation				X		X	X	X
Model Watermarking & Fingerprinting		X	X	X			X	X
AI Supply Chain Security	X	X	X	X	X	X	X	X
AI Threat Modeling	X	X	X	X	X	X	X	X
Model Red Teaming				X			X	X
Prompt Injection Defense (for LLMs)				X	X		X	X
Fine-grained Prompt Access Control					X		X	X
GenAI Response Grounding				X			X	X
AI Model Lifecycle Security	X	X	X	X	X	X	X	X
Sensitive Data Masking in Prompts			X	X	X		X	X
AI Policy Enforcement & Guardrails				X	X	X	X	X
LLM Fine-tuning Control & Oversight	X	X	X	X			X	X
AI-Driven Anomaly Detection for Abuse			X	X	X	X	X	X
RAG Security: Vector DB Access & Embedding Poisoning Defense		X	X	X	X		X	X

e *: for definitions, refer to annex slide below

efinitions - AI Security capabilities

AI Security Capability	Definition
AI Model Input Validation & Sanitization	Ensures inputs (prompts, files, APIs) are checked and sanitized to block malicious or poisoned content before reachi the model.
AI Model Access Control	Identity, RBAC/ABAC, token or API-key protections controlling which users/services can invoke specific models or endpoints.
AI Output Monitoring & Filtering	Monitors model responses and blocks/filters harmful, toxic, unsafe, or policy-violating outputs.
Model Versioning & Change Management	Controlled promotion, rollback, and approval of model versions to prevent unauthorized or accidental deployment, provide integrity assurance.
Adversarial Threat Detection	Detects adversarial inputs, output manipulation, prompt exploits, evasion attacks, or poisoning attempts
AI Audit Trails	A chronological, detailed record of all activities related to an AI system's lifecycle, including data inputs, model beha decisions, and changes.
Model/Data Provenance Tracking	Tracks origin, ownership, and transformation of training data and models to verify trustworthiness and auditability.
Privacy-preserving AI	Removes, masks, or mathematically preserves privacy in data or prompts (e.g., differential privacy).
Secure Model Deployment & Isolation	Runs models in isolated containers, VMs, or sandboxes to prevent lateral movement or model theft.
Model Watermarking & Fingerprinting	Embeds cryptographic marks to detect model theft, tampering, and track AI-generated output.
AI Supply Chain Security	Validates safety of datasets, pre-trained models, repos, and dependencies to prevent malicious insertion.
AI Threat Modeling	Systematic identification of AI-specific attack surfaces, threats, mitigations, and abuse patterns.
Model Red Teaming	Controlled adversarial testing to identify safety issues, prompt exploits, jailbreaks, and output misuse.
Prompt Injection Defense (for LLMs)	Detects and blocks prompt manipulation intended to override instructions, jailbreak, or steal data.
Fine-grained Prompt Access Control	Restricts which users, agents, or apps can issue high-risk prompts or privileged actions.
GenAI Response Grounding	Forces LLM outputs to reference trusted sources, reducing hallucination and misinformation.
AI Model Lifecycle Security	Ensures security from training → validation → deployment → monitoring → retirement.
Sensitive Data Masking in Prompts	Automatically scrubs or transforms secrets, PII, and confidential data before it reaches the model.
AI Policy Enforcement & Guardrails	Central enforcement of organizational policies for acceptable use, allowed tools, and trust boundaries.
LLM Fine-tuning Control & Oversight	Controls training datasets, permissions, and tamper-proof audit trail for model re-training.
AI-Driven Anomaly Detection for Abuse	Monitor the usage patterns of an AI system, identifying sudden, unusual, or suspicious behaviors that deviate from t established baseline.
RAG Security: Vector DB Access & Embedding Poisoning Defense	Prevents poisoning of embeddings, secures vector DB access, and verifies semantic retrieval trust.

Definitions – AA/AI Models

e	Definition
Orchestration	The coordination and management of AI and machine learning models to streamline workflows, enhance performance, and ens efficient integration across systems, eg AirFlow, QFlow.
omous Flow	Independent operation of managing and executing tasks without the need for human intervention across the entire suite of busi process. Eg. Agentic AI agents that can think autonomously and invoke a tool.
d Flow	Operation of managing and executing tasks across the business process that follows a pre-set steps or defined flow. Close to Wo definition (fixed, follows a pre-defined decision tree).
stration Agent	Specialized software entities that coordinate and manage multiple AI agents to achieve shared objectives. Looks at overall reque discover which agents can fulfill the request. the Eg. A2A.
(AI Router)	A component that directs incoming user requests to the appropriate functions or actions within AI systems. Eg. Piece of orchestr agent.
(AI Chain)	A structured sequence of AI processes or components that work together to achieve a specific goal. Eg. Langchain.
s (AI Models)	A trained software program designed to learn from data, identify patterns, make predictions and perform tasks with minimal hu intervention.
Source Models	Proprietary software systems where the source code, architecture and sometimes training data are not publicly available. Eg. Clo Open AI
Source Models	AI Model development and distribution approach that allows users to access, modify and distribute the source code of the mod LlaMA 3, Gemma, Mistral
m Source Models	AI models Based on open source and tuned into specific context. Eg. Deep Seek, Perplexity.
Support NE2	End-to-end management of AI models, including all activities to deploy , update, and versic NE1 the models. Part of AI lifecycle.
terface	Interface to access LLM. Eg. ChatGPT, CoPilot.
t Management	Method for memorizing, versioning, organizing and evaluating prompts used in LLM applications, including removing malicious p that would break the LLM model. Prompt is the way to interact with LLM.
Handling	Process of detecting, reporting and recovering from errors that occur during the execution of a computer program. Including det hallucination (flag it as errors) and remove it.
t Parser	Tool designed to transform the raw, often unstructured, output of a LLM into a structured and usable format. Usually model resp in vectors, responding back in natural language used by the models.
g	Short-term computer memory for storage of frequently or recently used instructions or data. Eg. Providing a response based on

Slide 20

NE1 Not sure I'd put Deep Seek / perplexity as examples here, especially given this is about custom models. We could highlight Record of Employment Comments model as one that falls under this category.
Edgar, Nicholas NC [NC], 2025-10-31T18:07:35.238

NE2 Suggested some alternative names in the diagram above.
Edgar, Nicholas NC [NC], 2025-10-31T18:08:06.211

efinitions - Data Ingestion, Data Processing, Data Analysis

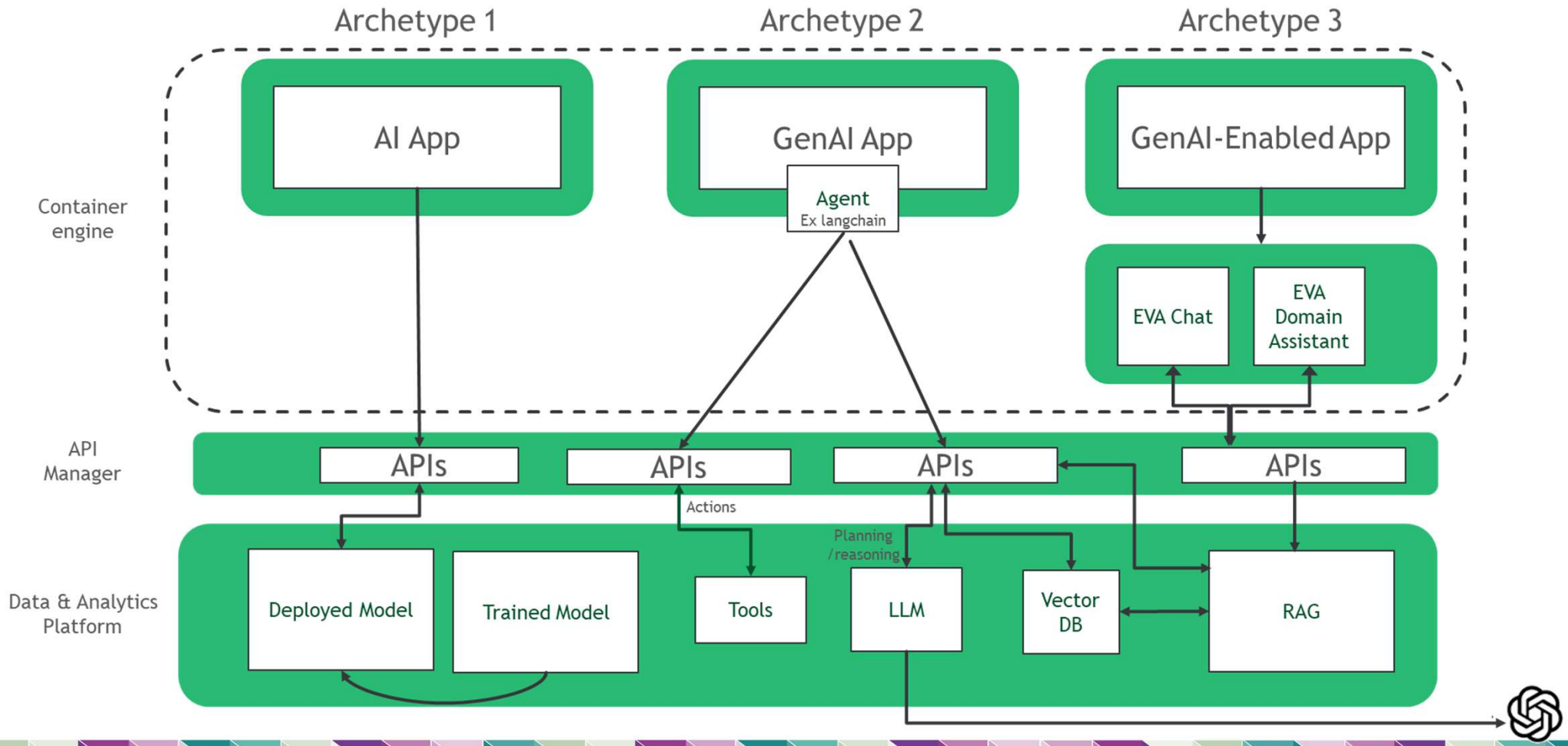
e	Definition
gestion	The process of importing, transferring, or loading data from various external sources into a centralized system or storage infrastructure.
ata Capture	The process of collecting raw data over time and processing it in large batches, which is efficient for handling frequent, repetitive
ne Data Capture	The process of collecting and processing data as it is generated, allowing for immediate availability and analysis.
Data Capture	
on of Data	The process for transferring data from one storage type, application, or system to another.
plication	The process of copying and synchronizing data from a primary source to one or more target systems to ensure high availability, fa tolerance and consistent access.
ocessing	Method of translating raw data into usable information.
eansing	The process of identifying and correcting errors, inconsistencies, and inaccuracies within a dataset.
rmalization	The process of organizing data in a database to reduce redundancy and improve data integrity, ensuring that each data item is sto only one place
ggregation	The process of collecting and summarizing data from various sources into a unified format for analysis and decision making.
uality	The measure of how well a dataset meets specific criteria such as accuracy, completeness, validity, consistency, uniqueness, time and fitness for purpose.
rocessing	Method to process data in groups or batches rather than individually
rocessing	Capture, Enrichment, formatting and emission of events, followed by routing and further processing.
ing Processing	Continuous analysis and processing of data as it flows in from various sources.
cal Data Processing	Comprehensive process of inspecting, cleaning, transforming and modeling data to discover and interpret meaningful information draw conclusions and aid decision making.
ed Data Analysis	Sophisticated techniques and tools used to analyze large volumes of data.
arch & Query	Process of finding information and specific request for information.
ttern Identification	Process of identifying recurring trends, relationships and structures observed within a dataset.

efinitions – Access

e	Definition
	Software component that provides a way other applications/system to interact with it.
s	Software components that adds specific functionality to an existing application or system
port	Process of saving or transferring data from one program to another in a specific format that can be recognized by other software
ase Connection	Method to allow client software to talk to database server software
ized Data Access	Method to allow users to view, access and analyze data from multiple sources without needing to know the physical location or technical format of that data
rketplace	Digital platform where developers can publish and sell AI models, datasets, APIs and services
rdrails	Safeguards that ensure artificial intelligence (AI) systems operate safely, responsibly and within defined boundaries

Different Archetypes of AI Apps

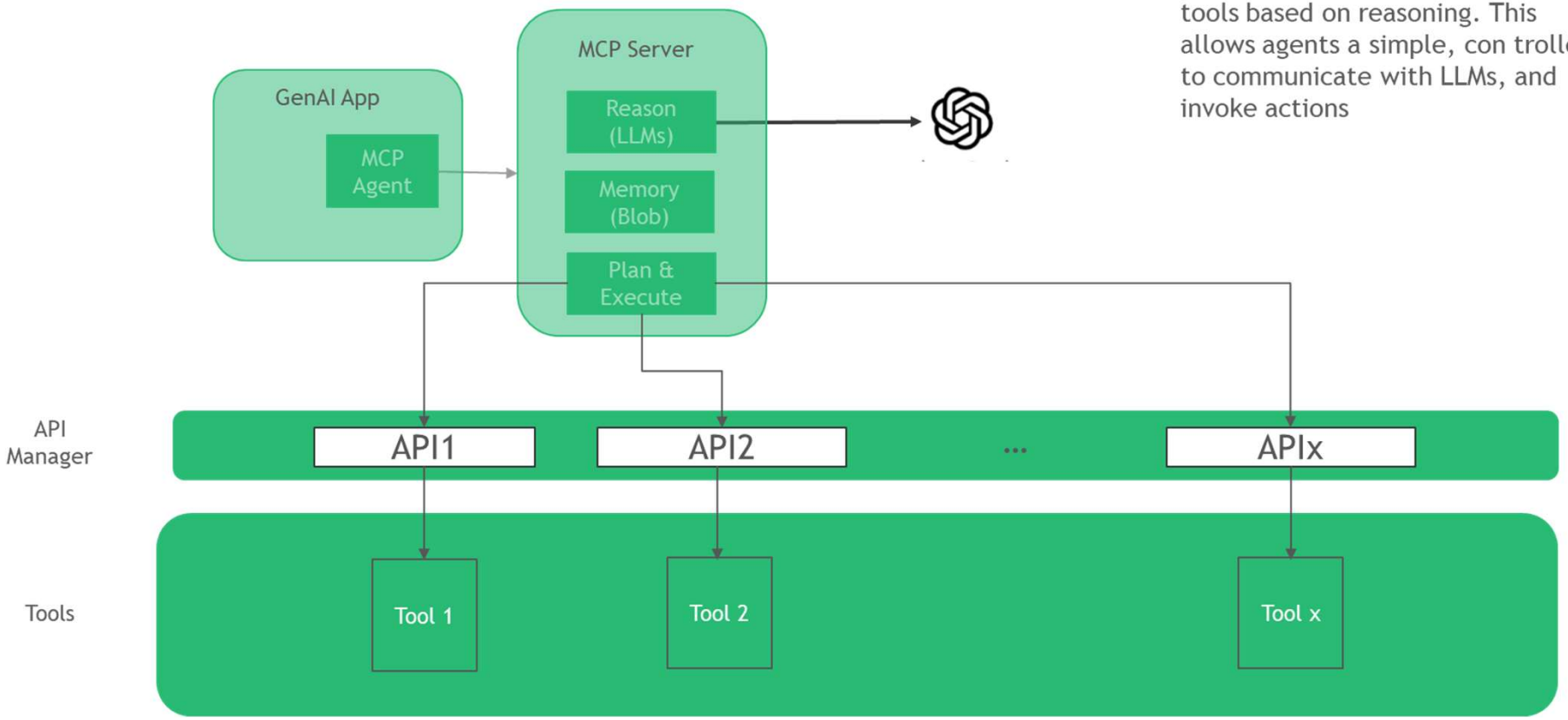
hen building AI apps, we can encounter 3 different archetypes



Archetype #2 & Agentic AI

chetype 2 requires an Agentic AI architecture, and is considered the future AI applications

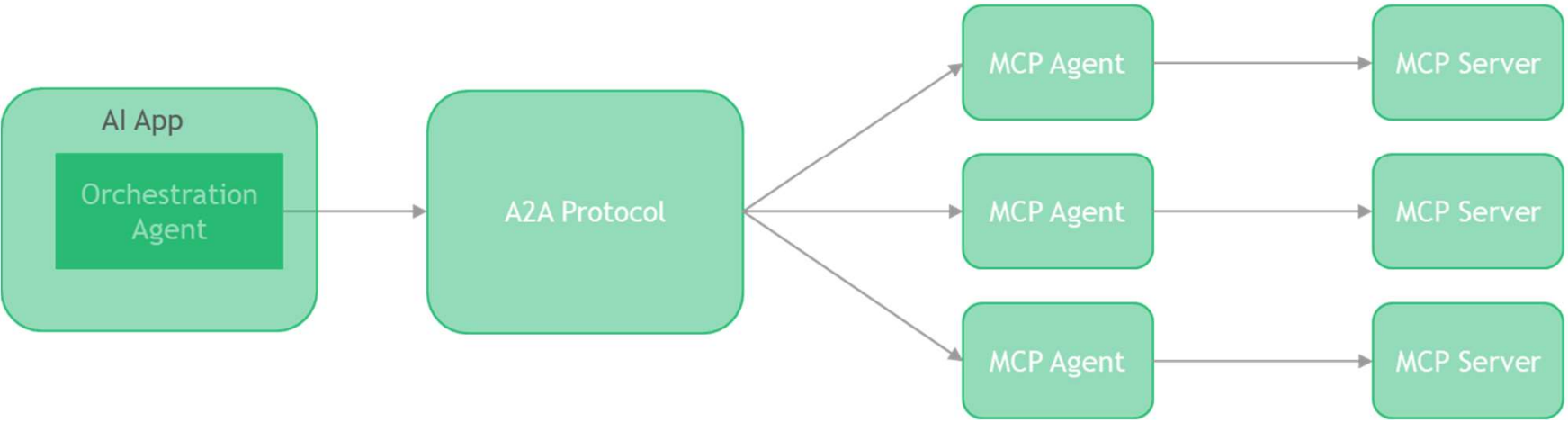
Archetype 2 is now implementable using a common protocol, MCP to standardize the way we invoke tools based on reasoning. This allows agents a simple, con trolled to communicate with LLMs, and invoke actions



ulti AI agents & Standard Protocols

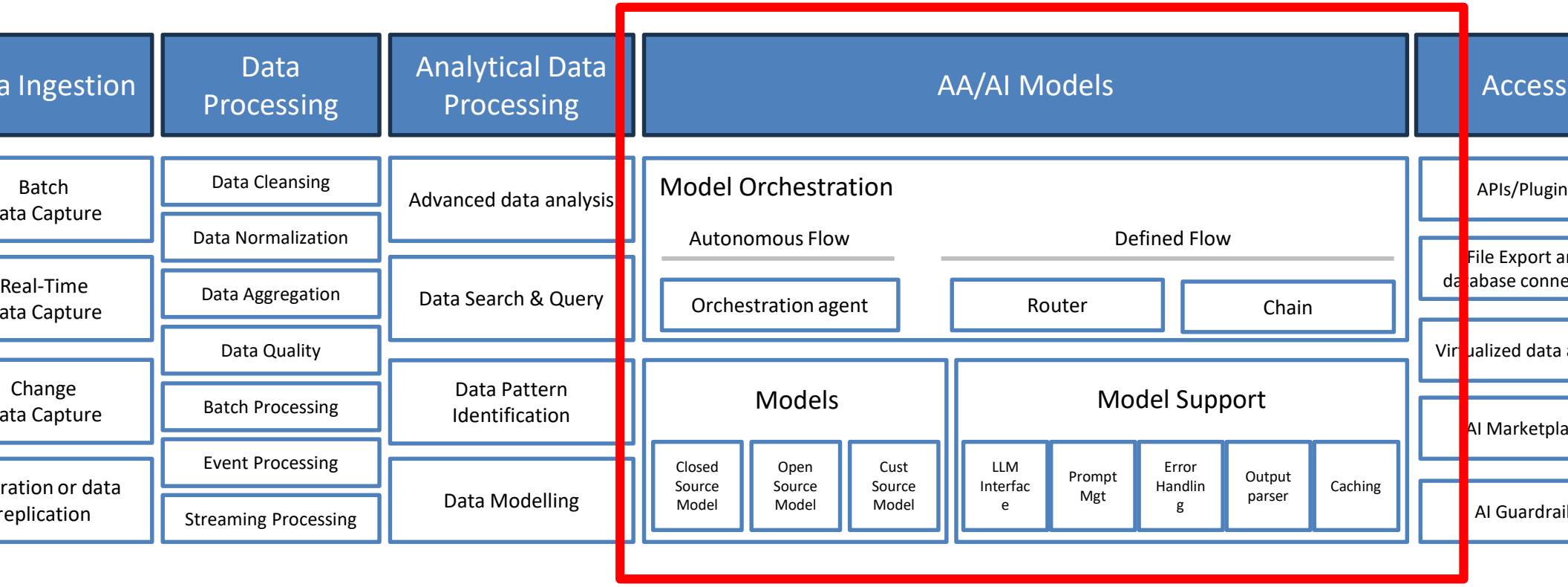
more complex interaction a multi-agent approach is necessary, and with it some standard protocc
CP, A2A)

Fore more complex activities, an agent can invoke other ”specialized” agents, in standard and orchestrated way. That standardization can happen using the A2A protocol that allows publishing and discovering capabilities, that can be further invoked using MCP

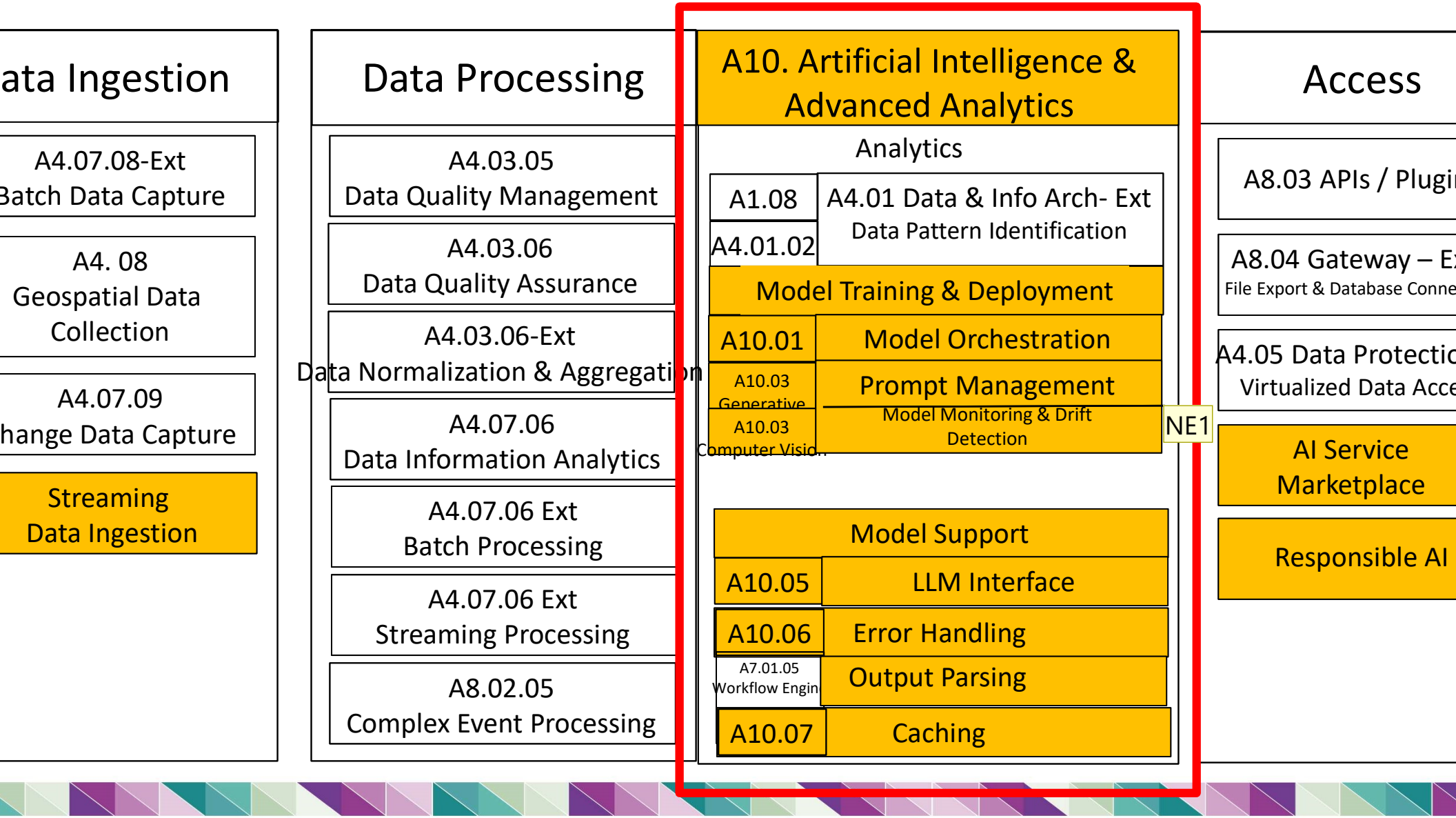


Reference Architecture – New Application/Technical Capabilities for A

rder to build a Data and Advanced Analytics architecture, it is important to define a North Star wit
necessary business and technical capabilities that meet the business needs



apping to DACM – AI Reference Architecture (to be verified)



Slide 27

NE1 Should not be classified as a category only for Computer Vision as this is important for all AI systems / models, even closed source ones.
Edgar, Nicholas NC [NC], 2025-10-31T17:56:36.807