

HỒ SƠ NỀN TẢNG & SẢN PHẨM · 2026



DBIZ Autonomous Agentic AI — Action Engine

AI hoàn thành công việc

cho

doanh nghiệp tự vận hành

Nền tảng AI Agent chạy 100% trên hạ tầng của bạn — không phí API, không rò rỉ dữ liệu, không phụ thuộc cloud

d b i z

BẢO MẬT

Các thông tin dưới đây là thông tin bảo mật của Công ty Cổ phần Nền tảng Kinh doanh Số (DBIZ). Việc sử dụng, sao chép, truyền tải hoặc tái bản cho bất kỳ mục đích nào mà không có sự đồng ý trước bằng văn bản của DBIZ đều bị nghiêm cấm.

Mục lục

Tài liệu dành cho lãnh đạo doanh nghiệp: agentic AI khác chatbot ở đâu, kiến trúc nào giúp AI hành động an toàn trên chính hạ tầng của bạn, và 97 AI Agents của DBIZ Autonomous đang tự động hoá những nghiệp vụ nào.

01	Chiến lược AI-Native	04
Từ "AI trả lời" đến "AI hoàn thành công việc" · vì sao agent cần nền tảng · bốn trụ cột của DBIZ Enterprise Platform		
02	Nền tảng công nghệ Agentic AI	08
Agent Core — điều phối có kiểm soát · 90+ model AI nội bộ · tri thức & RAG dẫn nguồn · guardrails · HITL · 97 agents · 5 cấp năng lực		
03	Sản phẩm: Agent trong thực chiến	19
AP Invoice Processing — chuỗi 20 agent · ChatbotAI + Knowledge Orchestrator · lộ trình trưởng thành theo quý		
04	Kết hợp Data Lakehouse & Foundation	23
Text-to-SQL trên nguồn sự thật · danh tính, số đăng ký & guardrails từ nền · hành trình một quyết định		
05	Tin cậy & Triển khai	26
Kiểm chứng ở quy mô ngân hàng · AI có trách nhiệm theo ISO 42001 · phương pháp OUM + Agile · ROI 6–12 tháng		

Cách đọc tài liệu này

15 phút

Đọc Phần 01 và Phần 05 — đủ bức tranh agentic AI, giá trị kinh doanh và cách kiểm soát rủi ro.

30 phút

Thêm Phần 03 và 04 — thấy agent làm việc trong sản phẩm thật và cách bốn trụ cột khớp nhau.

60 phút

Đọc trọn Phần 02 — nắm Agent Core, danh mục model nội bộ, guardrails và đội hình 97 agents.

PHẦN 01

Chiến lược AI-Native

The AI-Native Strategy — from answers to actions

Bước nhảy: từ "AI trả lời" sang "AI hoàn thành công việc"

Chủ quyền: 100% trên hạ tầng của bạn — không phí API, không rò rỉ dữ liệu

Đội hình: 97 AI Agents · 9 nhóm nghiệp vụ · 5 cấp năng lực

Từ "AI trả lời" đến "AI hoàn thành công việc"

Chatbot trả lời câu hỏi rồi dừng lại — con người vẫn làm nốt phần việc. **Agentic AI đi tiếp quãng đường còn lại:** tự lập kế hoạch, gọi công cụ, thực thi và tự đánh giá kết quả. DBIZ Autonomous là **Action Engine** — cỗ máy hành động của chiến lược AI-Native, chạy hoàn toàn trên hạ tầng của doanh nghiệp.



100% Private

Mô hình AI và dữ liệu chạy trên hạ tầng của bạn — dữ liệu nhạy cảm không đi qua bất kỳ API bên ngoài nào.

No API Costs

Không phí API theo token trả cho nhà cung cấp nước ngoài — chi phí AI là hạ tầng của bạn, dự toán được.

Full Controls · Low Latency

Toàn quyền kiểm soát model, tri thức và giới hạn hành động; suy luận tại chỗ cho độ trễ thấp.

97

AI Agents · 9 nhóm nghiệp vụ

90+

model AI nội bộ (self-hosted)

60–80%

giảm thời gian xử lý quy trình

6–12

tháng hoàn vốn điển hình

Agent chỉ đáng tin khi có nền tảng phía dưới

Sức mạnh của agent — tự hành động — cũng chính là rủi ro của nó. Một agent "thả rông" trên dữ liệu bản, không danh tính, không giới hạn, là tai nạn chờ ngày xảy ra. Vì vậy DBIZ không bán agent rời: **mỗi agent đứng trên nền dữ liệu tin cậy và khung quản trị đầy đủ của DBIZ Enterprise Platform.**

Agent "thả rông"

- Suy diễn trên dữ liệu phân mảnh, lỗi thời — trả lời tự tin nhưng sai (hallucination trên dữ liệu thật).
- Gửi dữ liệu nội bộ ra API AI nước ngoài — rủi ro rò rỉ và phụ thuộc không kiểm soát được.
- Không hạn mức chi phí — hoá đơn API theo token tăng vọt mà không ai phát hiện kịp.
- Không ghi vết — khi có vấn đề, không ai dựng lại được agent đã làm gì và vì sao.

Agent trên nền DBIZ

- Đọc dữ liệu hợp nhất của Data Lakehouse và tri thức có kiểm duyệt — trả lời kèm dẫn nguồn.
- Suy luận trên GPU nội bộ với model self-hosted — dữ liệu không rời hạ tầng doanh nghiệp.
- Danh tính, quyền tối thiểu và guardrails từ Foundation; cách ly tenant trước mọi truy vấn.
- Mọi suy luận ghi log bất biến: request · model · chi phí · nguồn · quyết định — kiểm toán lại được.

Ba câu hỏi lãnh đạo nên hỏi trước khi "tuyển" agent

Giao việc gì trước?

Việc lặp lại, quy tắc rõ, dữ liệu sẵn, rủi ro thấp — xử lý hoá đơn, đối soát, giám sát ngân sách là các điểm khởi đầu đã kiểm chứng.

Kiểm soát thế nào?

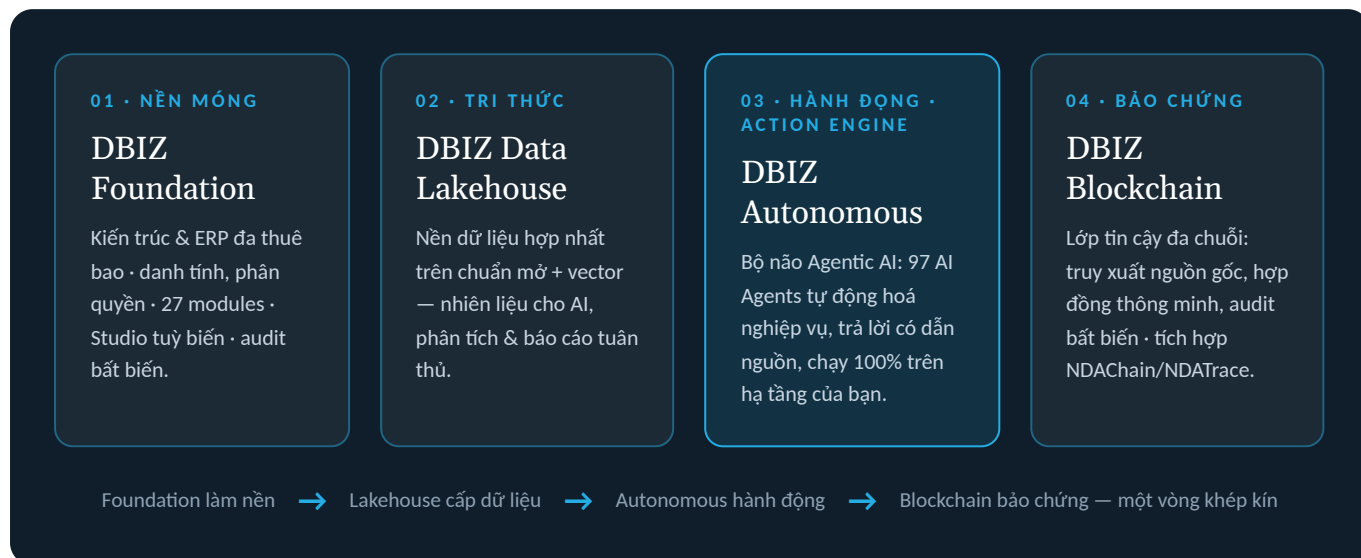
Bằng kiến trúc, không bằng lời hứa: quyền tối thiểu, ngưỡng phê duyệt, guardrails runtime, ghi vết đầy đủ.

Đo ROI ra sao?

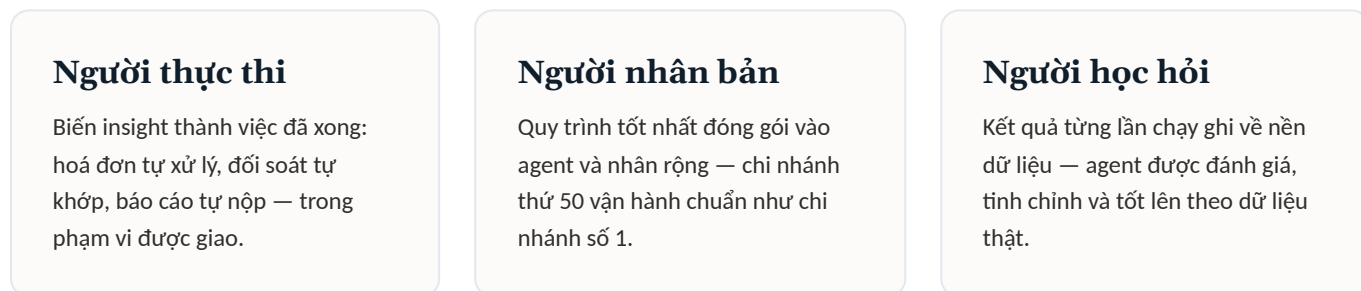
Thời gian xử lý, tỷ lệ tự động, năng suất — cam kết điển hình: giảm 60-80% thời gian xử lý, tăng ~40% năng suất.

Một nền tảng — bốn trụ cột công nghệ

DBIZ Enterprise Platform hợp nhất bốn trụ cột **chia sẻ chung hạ tầng, danh tính và bảo mật**, triển khai linh hoạt SaaS hoặc on-premise. Autonomous là "bộ não hành động" — đứng trên nền của ba trụ cột còn lại.



Vai trò riêng của Autonomous trong bốn trụ



PHẦN 02

Nền tảng công nghệ Agentic AI

Technology Platform — autonomy within guardrails

Agent Core: điều phối · suy luận · bộ nhớ — minh bạch từng bước

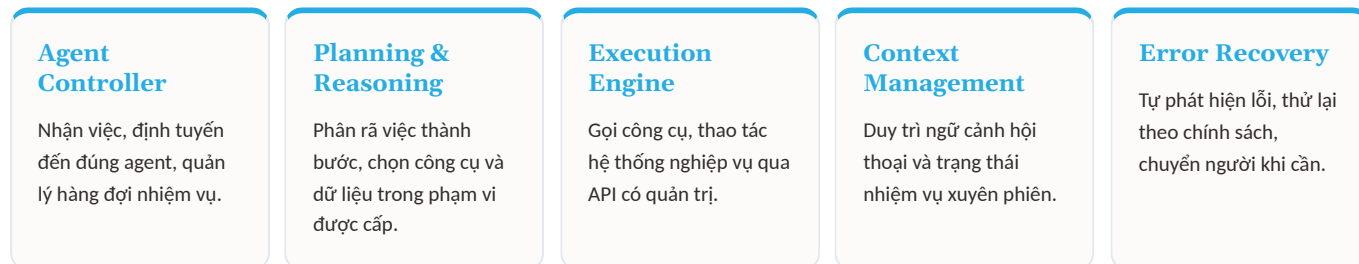
Chủ quyền trí tuệ: 90+ model AI chạy trên GPU của bạn

An toàn từ thiết kế: guardrails · Human-in-the-Loop · audit bất biến

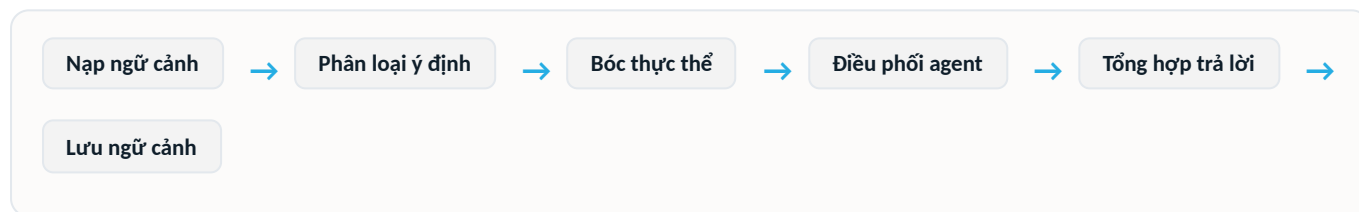
Agent Core — vòng lặp tự chủ có kiểm soát

Trái tim của Autonomous là **Agent Core** với ba khối: lớp điều phối, engine suy luận LLM và hệ thống bộ nhớ. Mỗi nhiệm vụ chạy qua vòng lặp chuẩn — agent tự chủ trong từng bước, nhưng cả vòng lặp nằm trong khuôn khổ đã được duyệt.

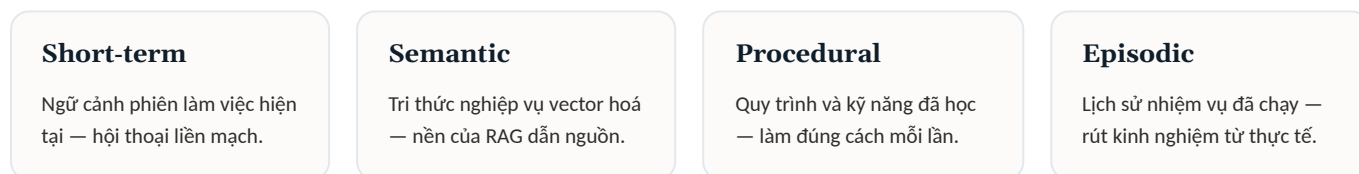
Lớp điều phối — năm thành phần



Pipeline hội thoại có trạng thái



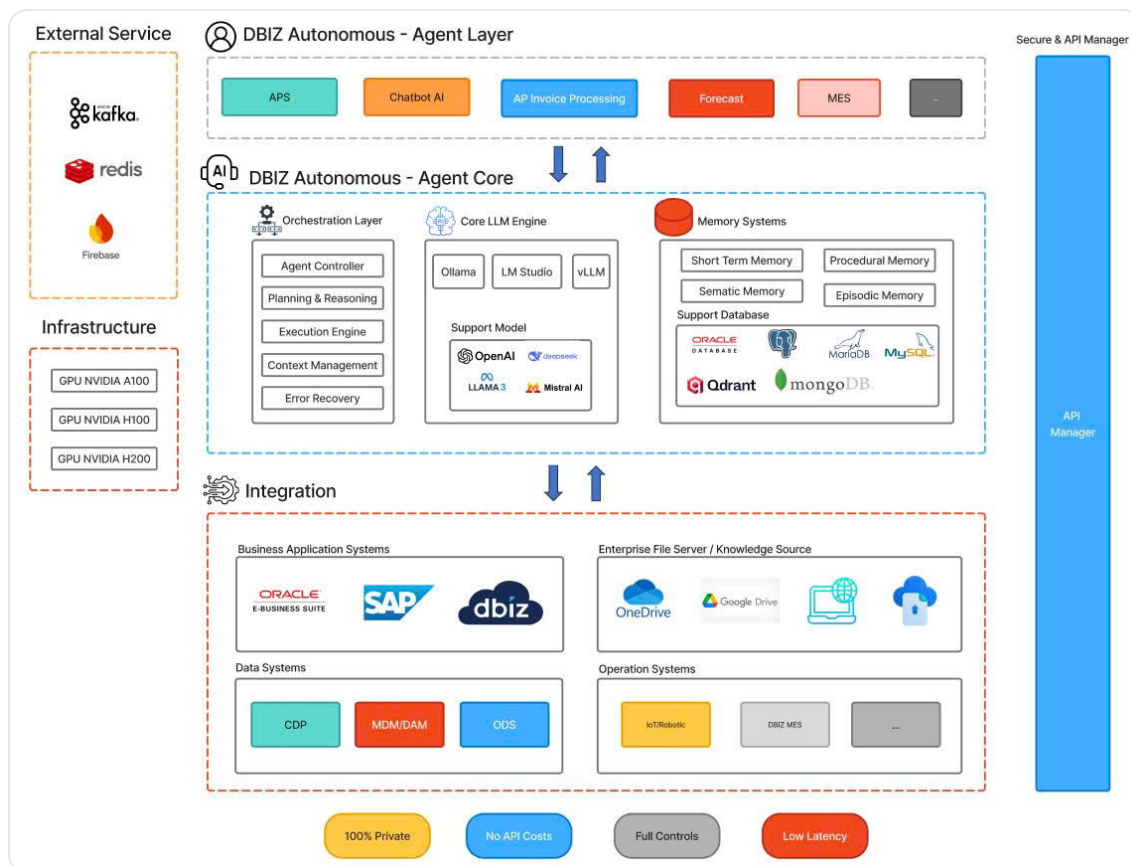
Bốn loại bộ nhớ — agent nhớ đúng thứ cần nhớ



Không phải "hộp đen": workflow agent định nghĩa tường minh trên nền LangGraph + CrewAI — kỹ sư nhìn thấy và chỉnh được từng bước; kiểm toán dựng lại được từng lần chạy. **Tự động hoá minh bạch, không phải phép màu.**

Kiến trúc tham chiếu end-to-end

Sơ đồ kiến trúc chính thức của DBIZ Autonomous: **Agent Layer** (các agent nghiệp vụ) đứng trên **Agent Core** (điều phối · LLM engine · bộ nhớ), kết nối hệ thống doanh nghiệp qua **lớp Integration** — tất cả sau một cửa API có bảo mật, trên GPU nội bộ.



Sơ đồ kiến trúc chính thức — Agent Layer (APS, Chatbot AI, AP Invoice Processing, Forecast, MES...); Agent Core (Orchestration · Core LLM Engine: Ollama/LM Studio/vLLM · Memory Systems); Integration (Oracle EBS, SAP, DBIZ; OneDrive/Drive; CDP/MDM/ODS; IoT/MES); hạ tầng GPU NVIDIA A100/H100/H200 — 100% Private · No API Costs · Full Controls · Low Latency

Nguyên tắc thiết kế

Chủ quyền trước hết

Model, tri thức, bộ nhớ và log đều trong hạ tầng doanh nghiệp; model cloud chỉ khi chính sách cho phép.

Tích hợp có quản trị

Mọi kết nối vào Oracle EBS, SAP, DBIZ và hệ thống dữ liệu đi qua Secure & API Manager — không "cửa sau".

Mở rộng ngang

Microservices trên Kubernetes, GPU đa thể hệ scale theo node — thêm agent, thêm tenant không tái cấu trúc.

90+ model AI nội bộ — chủ quyền trí tuệ

DBIZ vận hành danh mục **90+ model AI mã nguồn mở** trên GPU của doanh nghiệp — sáu hạng mục, chọn đúng model cho đúng việc qua bộ định tuyến chính sách: theo ý định, theo tenant, theo PII, theo chi phí và chất lượng.

Hạng mục	Vai trò	Đại diện tiêu biểu
LLM chủ lực	Suy luận đa bước, điều phối, soạn thảo — "bộ não" của agent cấp cao.	Llama 4 · Qwen3-235B/72B · DeepSeek-V3/R1 · Mistral Large 2
SLM gọn nhẹ	Tác vụ khối lượng lớn, độ trễ thấp: phân loại, tóm tắt, trích xuất.	Qwen3-32B và các model nhỏ hơn · Mistral 7B
Code models	Sinh SQL/code có kiểm soát, tự động hoá kỹ thuật.	Các model chuyên code mã nguồn mở
Vision & đa phương thức	Đọc hoá đơn, chứng từ, hình ảnh sản xuất (OCR + hiểu ngữ cảnh).	Vision-Language models
Embedding & RAG	Vector hoá tri thức đa ngôn ngữ cho tìm kiếm ngữ nghĩa.	Embedding models chuyên dụng
Speech	Chuyển giọng nói thành văn bản và ngược lại — trợ lý thoại nghiệp vụ.	ASR · TTS mã nguồn mở

Serving chuẩn mở

Ollama · vLLM · LM Studio — engine suy luận nội bộ đã kiểm chứng; thay model mới bất cứ lúc nào, không viết lại agent.

Định tuyến chính sách

Quyết định chọn model tách khỏi lớp thực thi — việc nhẹ vào SLM, việc khó vào LLM lớn; dữ liệu PII bắt buộc model nội bộ.

GPU đa thế hệ

NVIDIA A100 · H100 · H200 mở rộng ngang theo node; quản trị model tập trung; bật/tắt, đo mức dùng theo tenant.

Ý nghĩa với lãnh đạo: trí tuệ của doanh nghiệp không thuê ngoài theo token. Model là tài sản chạy trong nhà — **chi phí dự toán được, dữ liệu không rời lãnh thổ, và không ai tắt được AI của bạn.**

Tri thức doanh nghiệp & RAG có dẫn nguồn

Knowledge Base đưa tri thức nội bộ vào từng câu trả lời của agent — **lọc theo quyền truy cập trước khi trả kết quả, câu trả lời kèm nguồn, kiểm chứng được**. Và quan trọng nhất: hệ thống không tự học trực tiếp từ dữ liệu người dùng.

Permission-aware

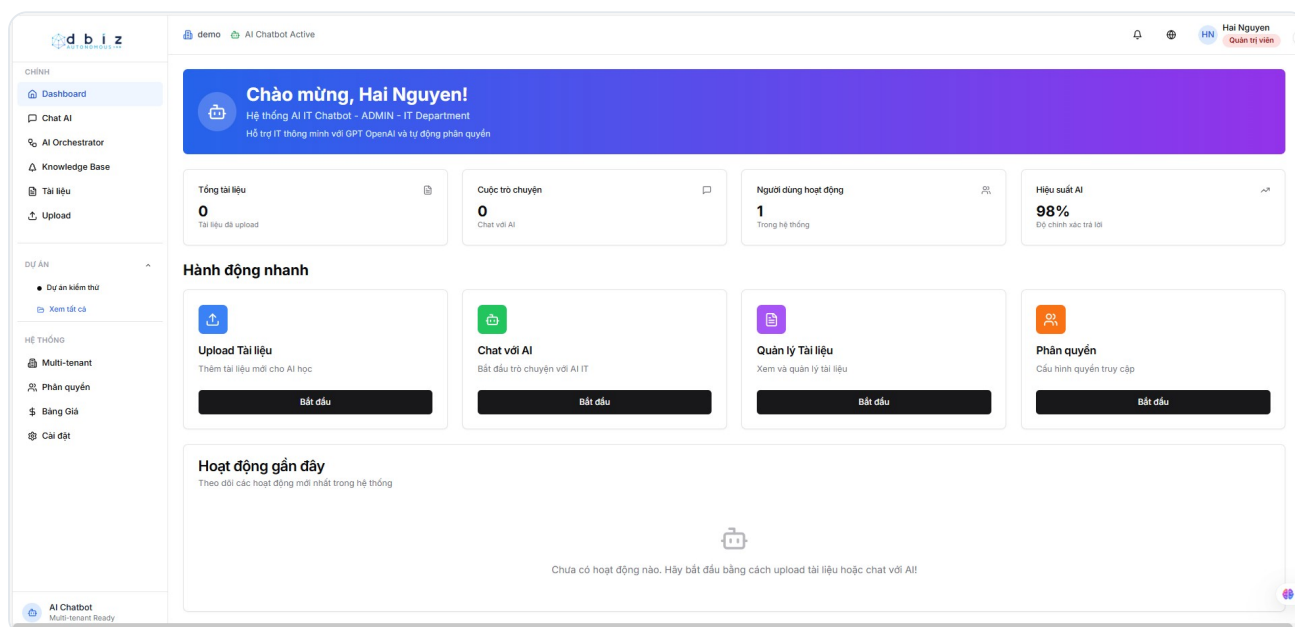
Kết quả tìm kiếm và RAG lọc theo quyền của người hỏi trước khi trả về — tri thức mật không "rò" qua câu trả lời AI.

Trả lời có dẫn nguồn

Mỗi câu trả lời kèm trích dẫn tài liệu gốc — người dùng kiểm chứng được, giảm mạnh rủi ro "AI bịa".

Knowledge Governance

Vòng kiểm duyệt: phản hồi → người thẩm định → biên tập → xuất bản → đánh giá. Mọi cập nhật tri thức qua kiểm duyệt và audit.



Màn hình thực tế — DBIZ Autonomous: dashboard Knowledge Base & ChatbotAI với thao tác nhanh (upload tài liệu, chat với AI, quản lý tài liệu, phân quyền), điều hướng AI Orchestrator, multi-tenant

Vòng đời tri thức khép kín

- **Nạp & vector hoá:** tài liệu từ OneDrive, Google Drive, file server nội bộ được nạp, gắn quyền và vector hoá cho tìm kiếm ngữ nghĩa.
- **Phục vụ agent (RAG):** agent truy tri thức đúng phạm vi quyền, ghép vào ngữ cảnh và trả lời kèm nguồn.
- **Học có kiểm duyệt:** phản hồi người dùng được tổng hợp cho người thẩm định — tri thức chỉ cập nhật qua tay con người, có vết.

Guardrails — hàng rào được dựng trước

Niềm tin vào agent không đến từ lời hứa "AI sẽ cẩn thận" — nó đến từ **những giới hạn kỹ thuật nằm ngay trong luồng suy luận** (data plane của AI Governance Control Plane). Mỗi agent của DBIZ vận hành trong năm lớp rào chắn.

Rào chắn	Cách hoạt động
1 • Lọc đầu vào	Chống prompt injection và jailbreak ngay tại cửa; yêu cầu ngoài phạm vi mục đích đăng ký bị từ chối.
2 • Cách ly tenant & PII	RLS/CLS áp trước mọi truy vấn dữ liệu; PII được nhận diện và che (redaction) theo chính sách trước khi vào model.
3 • Phạm vi công cụ	Danh sách công cụ được phép cấp lúc đăng ký agent — agent báo cáo không có công cụ tạo giao dịch, dù "muốn" cũng không gọi được.
4 • Ngưỡng hành động & chi phí	Hành động vượt ngưỡng giá trị/rủi ro tự chuyển người phê duyệt; rate-limit và hạn mức tài nguyên theo agent, theo tenant.
5 • Kiểm soát đầu ra	Lọc nội dung độc hại và dữ liệu nhạy cảm trước khi trả lời; định dạng ràng buộc theo mẫu; nhãn "AI-generated" minh bạch.

Cấu hình, không lập trình

Ngưỡng, hạn mức, chính sách PII đặt trong hồ sơ agent — đội quản trị điều chỉnh không cần sửa mã nguồn.

Vi phạm là dữ liệu

Mọi lần chạm rào được ghi và thống kê — nơi agent hay "đòi vượt" chính là nơi cần xem lại quy trình.

Nói dẫn theo niềm tin

Agent chứng minh độ tin cậy qua số liệu → ngưỡng phê duyệt nâng dần — tự động hoá mở rộng có kiểm soát.

Triết lý của DBIZ: an toàn AI là bài toán kiến trúc, không phải bài toán niềm tin. Rào chắn nằm ở tầng hạ tầng — **agent không thể vượt qua thứ nó không chạm tới được.**

Human-in-the-Loop — con người quyết định

Tự động hoá tốt không loại con người khỏi vòng lặp — nó đưa con người về **đúng chỗ có giá trị nhất: điểm ra quyết định**. Agent chuẩn bị mọi thứ; người có thẩm quyền xem, hiểu và bấm nút cuối — trên chính workflow phê duyệt của Foundation.

Ba bậc uỷ quyền theo mức rủi ro

Tự động hoàn toàn

Việc lặp lại, rủi ro thấp, đảo ngược được: xuất báo cáo, nhắc hạn, đồng bộ dữ liệu — agent làm và ghi vết, người xem lại khi cần.

Duyệt trước khi thực thi

Hành động chậm tiền, khách hàng, nhân sự: agent chuẩn bị trọn gói — phương án, số liệu, bản nháp — người duyệt một chạm.

Chỉ tham mưu

Quyết định chiến lược: agent phân tích kịch bản và khuyến nghị kèm căn cứ — hành động hoàn toàn thuộc con người.

Ví dụ: luồng duyệt một đề nghị chi phí (Expense Approval Agent)

Agent kiểm tra — hoá đơn hợp lệ, đúng chính sách, không trùng lặp, không bất thường so với lịch sử.



Dưới ngưỡng & đạt chuẩn — tự phê duyệt trong phút, ghi vết đầy đủ; phần lớn đề nghị đi lối này.



Vượt ngưỡng / bất thường — chuyển người duyệt kèm phân tích của agent: vì sao đáng chú ý, so sánh với gì.

Phê duyệt mọi nơi

Điểm dừng phê duyệt đến thẳng web và mobile — quyết định trong phút, không nghẽn quy trình.

Ngữ cảnh đầy đủ

Người duyệt thấy toàn bộ căn cứ agent đã dùng — không phải "ký mù" theo đề xuất của máy.

Trách nhiệm rõ

Ai duyệt, lúc nào, dựa trên gì — tất cả trong nhật ký audit; uỷ quyền có kỳ hạn và có vết.

Ghi vết từng suy luận — minh bạch tuyệt đối

Câu hỏi quan trọng nhất với AI trong doanh nghiệp không phải "nó thông minh cỡ nào" mà là "nó vừa làm gì, và vì sao?". Mọi lần suy luận của agent DBIZ đều được ghi log bất biến và dựng lại được.

Log bất biến mọi inference

Prompt · model · phiên bản · kết quả · độ tin cậy · quyết định chọn model — từng lần suy luận một bản ghi không sửa được.

Truy vết chi phí & nguồn

Mỗi request gắn tenant, agent, chi phí tính toán và nguồn dữ liệu đã dùng — ROI và trách nhiệm đo được đến từng nhiệm vụ.

Neo blockchain

Quyết định trọng yếu được neo bằng chứng lên blockchain (trụ cột thứ tư) — bằng chứng bất biến cho kiểm toán độc lập.

Giám sát chất lượng liên tục

Đánh giá & phát hiện drift

Bộ đánh giá (eval harness) chạy định kỳ trên bộ kiểm thử chuẩn; chất lượng suy giảm hoặc thiên lệch (bias/drift) được phát hiện và cảnh báo sớm — model được tinh chỉnh hoặc thay thế có kiểm soát.

Dashboard vận hành AI

Chất lượng trả lời, chi phí theo agent/tenant, tỷ lệ con người phải can thiệp (override) — lãnh đạo nhìn sức khỏe đội AI như nhìn P&L.

Giá trị của minh bạch

- **Kiểm toán nội bộ & cơ quan quản lý:** xuất trọn chuỗi suy luận – hành động – phê duyệt của bất kỳ nhiệm vụ nào — đáp ứng chuẩn giải trình ngành tài chính.
- **Cải tiến liên tục:** nhiệm vụ thất bại là dữ liệu quý — đội vận hành thấy chính xác bước gãy để tinh chỉnh agent hoặc quy trình.
- **Niềm tin của người dùng:** nhân viên tin và dùng agent nhiều hơn khi luôn mở ra xem được "nó đã làm gì với việc của mình".

Năm cấp độ năng lực — từ Bot đến Optimizer

Không phải việc nào cũng cần một agent "nặng ký". DBIZ phân cấp agent theo **năm mức năng lực** — doanh nghiệp bắt đầu nhỏ với các Bot tác vụ đơn, nâng dần lên Master điều phối và Optimizer tối ưu hoá liên tục.

L1 · Bot

Tự động hoá tác vụ đơn, lặp lại, đầu ra chuẩn — báo cáo theo lịch, gửi email tự động.

L2 · Scout

Giám sát chủ động: quét liên tục, phát hiện bất thường, cảnh báo và đề xuất hành động.

L3 · Pro

Chuyên gia một lĩnh vực: phân tích sâu, đối thoại nhiều lượt, dùng nhiều công cụ một phiên.

L4 · Master

Điều phối đa bước, đa hệ thống: phân rã việc, gọi agent khác, tổng hợp kết quả.

L5 · Optimizer

Tối ưu hoá liên tục: học từ dữ liệu vận hành, đề xuất cải tiến quy trình và tham số.

Mỗi agent là một "nhân sự số" được trang bị đầy đủ

Công cụ (Tools)

Được cấp quyền dùng đúng bộ công cụ theo phạm vi: truy vấn dữ liệu, thao tác nghiệp vụ, gửi báo cáo — qua API có quản trị.

Mô hình AI (Models)

Kết hợp LLM/SLM/vision cho từng việc — do bộ định tuyến chính sách quyết định, chạy trên GPU nội bộ.

Tri thức (Knowledge)

Đầu nối kho tri thức đúng phạm vi: quy định nội bộ, quy trình, dữ liệu nghiệp vụ — trả lời có căn cứ, có trích dẫn.

Tùy biến theo doanh nghiệp — không cần chờ DBIZ

Agent Studio — tạo agent không cần code

Đội nghiệp vụ tự dựng agent mới từ khối có sẵn: chọn công cụ, tri thức, ngưỡng duyệt — đóng gói kinh nghiệm của chính doanh nghiệp thành "nhân sự số".

Agent Extension Contract

Chuẩn mở rộng chuẩn hoá cho yêu cầu đặc thù sâu — thêm năng lực riêng ngành mà vẫn giữ nguyên khung security, audit và kiểm soát chi phí.

97 AI Agents — bức tranh toàn cảnh

Đội hình 97 agents phủ **9 nhóm nghiệp vụ**, quản lý tập trung trong một màn hình cấu hình — kích hoạt theo nhu cầu, mỗi agent hiển thị rõ cấp năng lực, model sử dụng và trạng thái sẵn sàng.

Quản trị Dữ liệu & Analytics • 27

Bán hàng & Marketing • 13

Tài chính & Kế toán • 12

Trải nghiệm Khách hàng (CX) • 11

Chuỗi cung ứng • 11

Nhân sự • 7

Sản xuất (MES/APS) • 6

Tích hợp • 5

Chung • 5

AI CHATBOT + KNOWLEDGE ORCHESTRATOR							
Trạng thái: Online Core Engine: Local AI (Ollama - Mistral 7b / Llama 3) Knowledge Base: Đã kết nối (Vector DB: Qdrant) Autonomous Platform: Đã kết nối API							
Cấu hình Agent Kịch bản tương tác Knowledge Manager Orchestration AI Monitor							
Cấu hình Agent Quản lý 97 AI Agents được phân nhóm theo chức năng nghiệp vụ và sản phẩm từ DBIZ Autonomous Platform.							
Tìm kiếm agent (tên, code, nhiệm vụ)... Tắt cả sản phẩm							
Tất cả (97) Bán hàng (13) Chung (5) Chuỗi cung ứng (11) Nhân sự (7) Quản trị Dữ liệu (27) Sản xuất (MES/APS) (6) Trải nghiệm Khách hàng (CX) (11) Tài chính (12) Tích hợp (5)							
Kích hoạt	Code	Agent	Nhiệm vụ	Level	Mô hình	Sản phẩm	Trạng thái
☒	SR-002	CampaignPro	Trợ lý Chiến dịch Marketing - Tối ưu chiến dịch marketing marketing campaigns optimization	Pro	LLM Llama 3	CX	Ready
☐	SR-011	CompetitorScout	Trợ lý Giám sát Đối thủ - Theo dõi cạnh tranh competitive-analysis monitoring intelligence	Scout	LLM Llama 3	CX	Off
☒	SR-004	ContentMaster	Trợ lý Tạo Nội dung AI - Tạo nội dung marketing content-creation copywriting marketing	Master	LLM GPT-4	CX	Ready
☐	SR-009	CustomerScout	Trợ lý Phân tích Khách hàng - Phân khúc khách hàng customer-analysis segmentation insights	Scout	LLM Llama 3	CX	Off
☒	SR-005	EmailBot	Trợ lý Email Marketing - Tự động gửi email marketing email-marketing automation campaigns	Bot	SLM Mistral 7b	CX	Ready

Màn hình thực tế — AI Chatbot + Knowledge Orchestrator: quản lý 97 AI Agents theo nhóm nghiệp vụ; mỗi agent hiển thị cấp năng lực (Bot/Scout/Pro/Master), model sử dụng (LLM Llama 3, GPT-4 theo chính sách · SLM Mistral 7B) và trạng thái kích hoạt

Một đội — không phải một trăm công cụ rời

- Phối hợp được:** agent Master gọi agent con qua chuẩn chung — quy trình liên phòng ban (đơn hàng → kho → hoá đơn → công nợ) tự động trọn chuỗi.
- Danh mục tiếp tục mở rộng:** kiến trúc thiết kế cho 110 agents — nhóm mới bổ sung theo lộ trình và theo ngành của khách hàng.
- Quản trị một chỗ:** toàn bộ hồ sơ agent trong một sổ đăng ký, một màn hình cấu hình, một nhật ký audit.

Đội agent Tài chính — 12 "nhân sự số" tiêu biểu

Nhóm Tài chính & Kế toán là nhóm trưởng thành nhất — 12 agents phủ trọn chu trình từ hoá đơn đến dòng tiền, mỗi agent một nhiệm vụ rõ ràng, phối hợp qua Agent Core.

Agent	Nhiệm vụ & giá trị
InvoiceBot	Xử lý hoá đơn AI: OCR + kiểm tra tự động, đối chiếu 3 chiều PO – nhận hàng – hoá đơn.
ExpenseGuard	Phê duyệt chi phí theo chính sách: tự duyệt trong ngưỡng, phát hiện bất thường, chống gian lận.
CashFlowPro	Dự báo dòng tiền và tài chính bằng ML — tối ưu vốn khả dụng hằng ngày.
AuditMaster	Kiểm toán tuân thủ tự động: rà soát giao dịch, đối chiếu chính sách, cảnh báo lệch chuẩn.
ReconBot	Đối soát tự động ngân hàng với sổ sách — kỳ đối soát rút từ ngày còn giờ.
TaxGenius	Tính và tối ưu thuế thông minh — cập nhật theo quy định thuế Việt Nam.
BudgetWise	Giám sát ngân sách thời gian thực, cảnh báo vượt ngân sách trước khi phát sinh.
CreditScout	Đánh giá rủi ro tín dụng khách hàng bằng ML — hỗ trợ quyết định bán chịu.
DebtCollector	Tự động hoá quy trình thu hồi công nợ: nhắc nợ theo bậc, đề xuất phương án.
CashMate	Quản lý dòng tiền & treasury: cân đối tài khoản, tối ưu nguồn.
ExpenseTracker	Theo dõi chi phí thời gian thực theo đơn vị, dự án, hạng mục.
CostOptimizer	Phân tích và tối ưu cấu trúc chi phí từ dữ liệu vận hành.

Đóng gói sẵn, tùy chỉnh nhanh

Mỗi agent có kiến trúc, quy trình và KPI chuẩn — tinh chỉnh theo chính sách của doanh nghiệp trong sprint, không xây từ đầu.

Phối hợp trọn chu trình

InvoiceBot chuyển ExpenseGuard duyệt, ReconBot khớp ngân hàng, CashFlowPro cập nhật dự báo — chuỗi tài chính tự chạy.

8 nhóm còn lại tương tự

Bán hàng, CX, chuỗi cung ứng, nhân sự, sản xuất, dữ liệu, tích hợp — cùng chuẩn đóng gói và quản trị.

PHẦN 03

Sản phẩm: Agent trong thực chiến

The Product — agents at work, on real screens

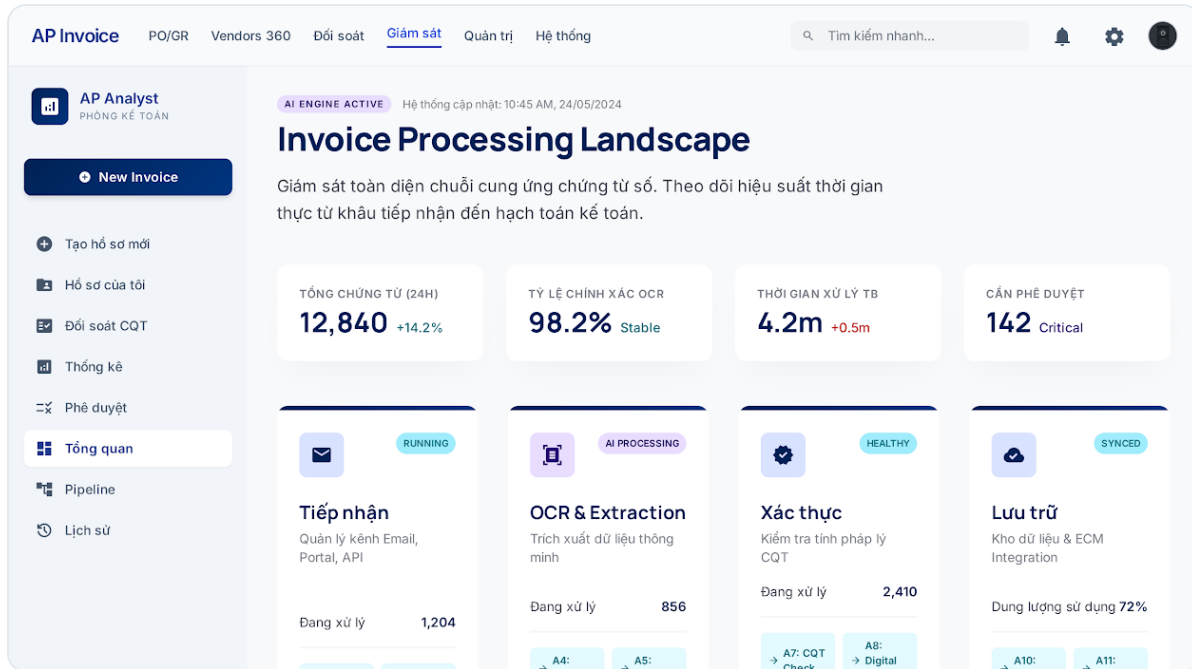
AP Invoice Processing: chuỗi 20 agent xử lý 12.840 chứng từ/ngày

ChatbotAI + Knowledge Orchestrator: giao việc bằng tiếng Việt

Lộ trình trưởng thành: thắng nhanh trước, nâng tự chủ dần

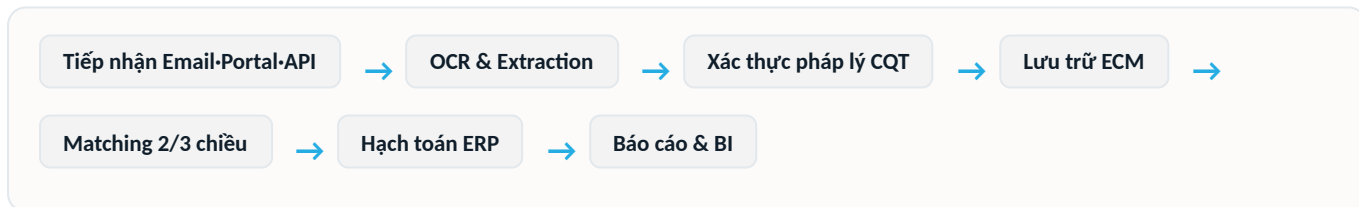
AP Invoice Processing — chuỗi 20 agent

Quy trình xử lý hoá đơn đầu vào được "agent-hoá" trọn chuỗi: **20 agent (A1-A20)** chia nhau 8 khâu từ tiếp nhận đến hạch toán — con người chỉ xử lý ngoại lệ và phê duyệt các trường hợp cần thẩm quyền.



Màn hình thực tế — Invoice Processing Landscape: 12.840 chứng từ/24h · chính xác OCR 98,2% · thời gian xử lý trung bình 4,2 phút; các khâu Tiếp nhận (A1-A3) → OCR & Extraction (A4-A6) → Xác thực CQT (A7-A9) → Lưu trữ (A10-A12) chạy song song

Trọn chuỗi 8 khâu — mỗi khâu một đội agent



Tỷ lệ khớp tự động 91,4%

Đối chiếu PO – nhận hàng – hoá đơn tự động; chỉ ngoại lệ mới đến tay người — đúng nguyên tắc quản lý theo ngoại lệ.

AI đề xuất tối ưu

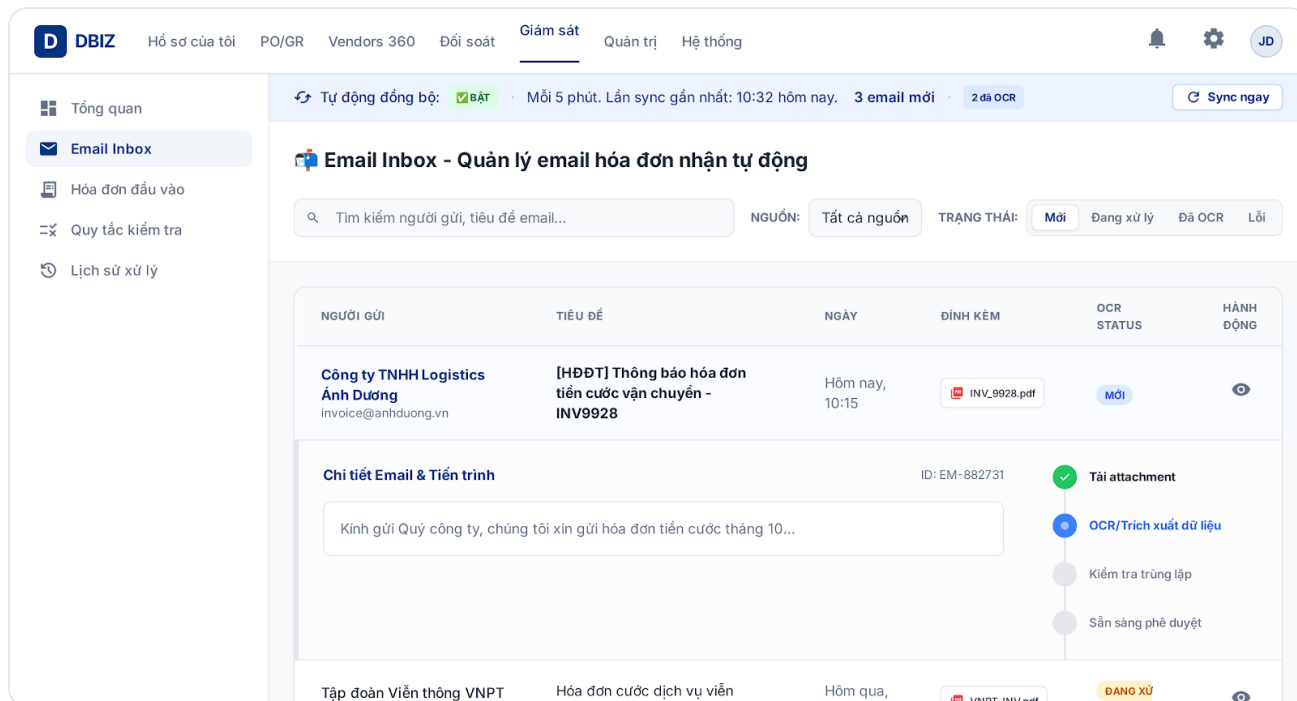
Hệ thống tự phát hiện điểm nghẽn (ví dụ khâu xác thực CQT chậm) và đề xuất cấu hình nâng tỷ lệ tự động — kèm nút thực thi.

Chuẩn nền thừa hưởng

Danh tính, phân quyền, workflow duyệt và audit đến từ Foundation — agent tập trung đúng việc nghiệp vụ.

Tiếp nhận thông minh — từ email thành dữ liệu

Điểm bắt đầu của nhiều quy trình là chiếc hộp thư. Agent tiếp nhận đọc email đến, **nhận diện chứng từ đính kèm**, **phân loại và đưa thẳng vào pipeline xử lý** — không ai phải "chép tay" từ email vào hệ thống nữa.



Màn hình thực tế — Email Inbox của AP Invoice: thư đến được agent quét, nhận diện hoá đơn đính kèm, gán trạng thái xử lý và đưa vào hàng đợi pipeline tự động

Nguyên tắc áp dụng cho mọi kênh tiếp nhận

Đa kênh về một hàng đợi

Email, cổng nhà cung cấp, API đối tác — mọi kênh đổ về một pipeline chuẩn với cùng quy tắc kiểm tra và ưu tiên.

Phân loại bằng AI

Model vision + ngôn ngữ đọc chứng từ tiếng Việt: hoá đơn, biên bản, đề nghị thanh toán — định tuyến đúng quy trình.

Trạng thái minh bạch

Từng chứng từ có trạng thái theo thời gian thực — người phụ trách biết chính xác hồ sơ đang ở khâu nào, kẹt vì sao.

Một mẫu số chung: mọi agent của DBIZ đều bắt đầu bằng việc "đón" công việc ở nơi nó phát sinh — hộp thư, cổng dữ liệu, cảm biến — và kết thúc bằng dữ liệu sạch trong hệ thống kèm vết đầy đủ. **Con người bước vào đúng lúc cần phán đoán, không phải để gõ lại dữ liệu.**

Lộ trình trưởng thành — bắt đầu từ đâu?

Sai lầm phổ biến nhất là khởi đầu bằng use-case khó nhất. DBIZ khuyến nghị con đường ngược lại: **thăng nhanh ở việc nhỏ, xây niềm tin bằng số liệu, rồi nâng dần mức tự chủ.**

Bốn tiêu chí chọn use-case đầu tiên

Lặp lại đủ nhiều

Việc diễn ra hằng ngày/tuần — tự động hoá mới tích lũy đủ giờ công để thấy rõ giá trị.

Quy tắc rõ ràng

Có chính sách, ngưỡng, mẫu chuẩn — agent học được khuôn khổ thay vì phán đoán mơ hồ.

Dữ liệu sẵn sàng

Nguồn dữ liệu đã hợp nhất, chất lượng đạt — không bắt agent làm việc trên nền mù.

Rủi ro thấp

Sai sót đảo ngược được, có người rà lại — an toàn để học và tinh chỉnh trong thực tế.

Lộ trình khuyến nghị theo quý

Quý 1 — Bot & Scout: xử lý hoá đơn, theo dõi chi phí, cảnh báo ngân sách — giá trị nhanh, rủi ro thấp, xây niềm tin.



Quý 2-3 — Pro: đối soát tự động, dự báo dòng tiền, duyệt chi phí bán tự động — mở rộng theo phòng ban.



Quý 4+ — Master & Optimizer: điều phối quy trình liên phòng ban, tối ưu hoá liên tục bằng dữ liệu vận hành.

Mỗi quý một cột mốc đo được

Thời gian xử lý, tỷ lệ tự động hoá theo từng quý — lộ trình được nghiệm thu bằng số, không bằng cảm nhận.

Niềm tin đi trước tự chủ

Mức uỷ quyền nâng theo thành tích thực tế của agent — không "thả" quyền lớn khi chưa có dữ liệu tin cậy.

Con người được nâng cấp

Song song lộ trình agent là đào tạo đội ngũ: giao việc, phê duyệt, đọc số liệu — tự động hoá cùng con người.

PHẦN 04

Kết hợp Data Lakehouse & Foundation

Better Together — trusted data, governed autonomy

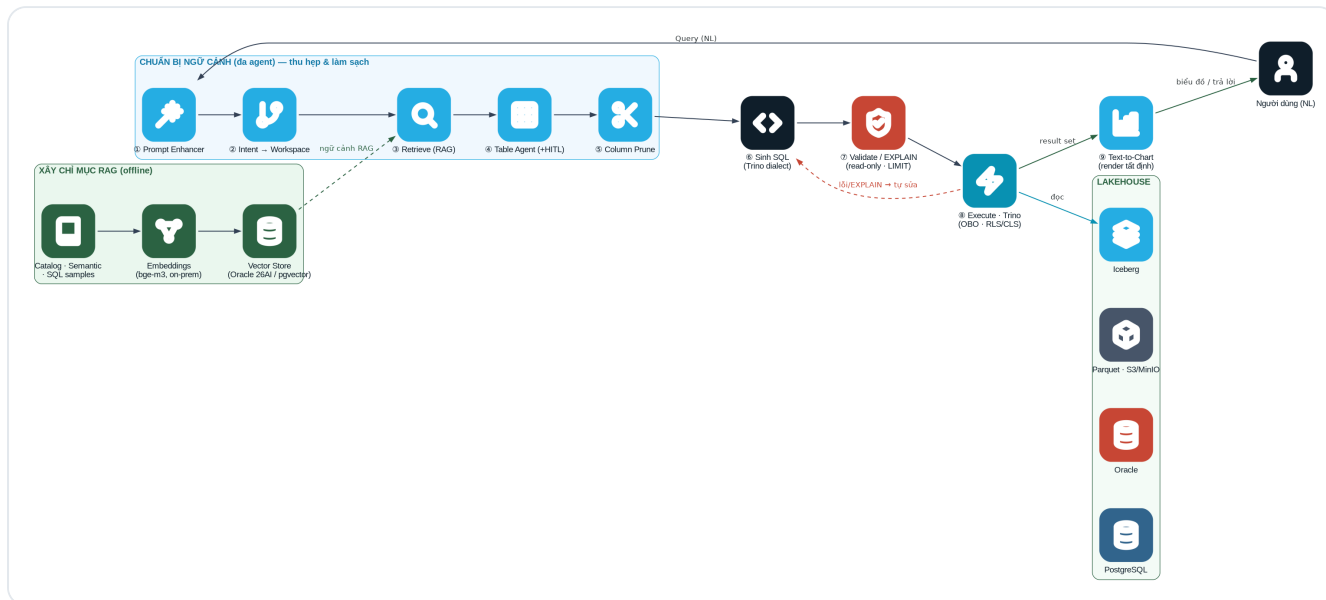
Với Data Lakehouse: Text-to-SQL trên một nguồn sự thật

Với Foundation: danh tính, sổ đăng ký & guardrails cho từng agent

Kết quả: tự động hoá mạnh dạn mà vẫn ngủ ngon

Autonomous × Data Lakehouse

Trí thông minh của agent bắt đầu từ dữ liệu nó được đọc. Kiến trúc tham chiếu **Text-to-SQL** của DBIZ cho thấy cách agent truy vấn nguồn sự thật một cách an toàn: qua semantic layer, tường lửa SQL và phân quyền của người hỏi.



Sơ đồ chính thức — kiến trúc tham chiếu Text-to-SQL của DBIZ Autonomous: câu hỏi tiếng Việt đi qua semantic layer và các lớp kiểm soát trước khi chạm dữ liệu, kết quả trả về kèm nguồn

Semantic layer — nói cùng ngôn ngữ

Chỉ số, chiều phân tích và thuật ngữ nghiệp vụ định nghĩa một lần — "doanh thu thuần" của agent trùng khớp tuyệt đối với báo cáo tài chính.

An toàn nhiều lớp

SQL sinh ra bị giới hạn trong phạm vi bảng được phép; phân quyền dòng/cột của người hỏi áp dụng tự động; truy vấn nguy hiểm bị tường lửa chặn.

Một con số duy nhất

Agent, dashboard và báo cáo cùng đọc một nguồn — hết cảnh "AI nói một đằng, báo cáo nói một nẻo".

Kết quả ghi ngược

Nhiệm vụ hoàn thành ghi kết quả về nền dữ liệu — dữ liệu vận hành của chính agent trở thành nguồn đo hiệu quả và tinh chỉnh vòng sau.

Autonomous × Foundation

Foundation biến đội agent từ "rủi ro mới" thành **lực lượng lao động số có kỷ luật**: mỗi agent một danh tính, một hồ sơ trong sổ đăng ký, một bộ giới hạn — và một vết audit không đứt đoạn.

Danh tính agent

Danh tính máy riêng, token có thời hạn — thu hồi tức thì, không tài khoản dùng chung.

Sổ đăng ký & phê duyệt

AI System Registry: đăng ký — thẩm định — phê duyệt trước khi lên môi trường thật.

Cách ly tenant

RLS/CLS áp trước mọi truy vấn; usage tracking và billing đo mức dùng theo từng tenant.

Audit hợp nhất

Suy luận, hành động, phê duyệt — một nhật ký bất biến phục vụ kiểm toán và thanh tra.

Hành trình của một quyết định — bộ máy cùng vận hành

BƯỚC 1 • FOUNDATION

CFO đăng nhập SSO; agent CashFlowPro mang danh tính riêng — hai chủ thể, một chuẩn định danh.

BƯỚC 2 • LAKEHOUSE

Agent đọc dữ liệu dòng tiền qua semantic layer, trong đúng phạm vi tổ chức được cấp.

BƯỚC 3 • AUTONOMOUS

Agent dự báo thiếu hụt, lập ba phương án; kịch bản vượt ngưỡng rủi ro chờ CFO phê duyệt.

BƯỚC 4 • VÒNG LẶP

Phương án duyệt được thực thi qua API Manager; kết quả và toàn bộ vết ghi ngược về nền dữ liệu.

Tự động mạnh dạn hơn

Vì giới hạn nằm ở kiến trúc, doanh nghiệp dám giao agent những việc lớn hơn — với tốc độ niềm tin tăng dần.

Không phát sinh cơ chế riêng

Từ 5 lên 97 agent vẫn một khung quản trị — chi phí kiểm soát không tăng theo số agent.

Sẵn sàng cho quy định

Khi khung pháp lý AI siết lại, sổ đăng ký và audit là lời giải có sẵn — không phải dự án chữa cháy.

PHẦN 05

Tin cậy & Triển khai

Trust & Delivery — responsible AI, measurable value

Kiểm chứng: module AI trong dự án quy mô ngân hàng

AI có trách nhiệm: ISO 42001 · guardrails · không tự học từ dữ liệu người dùng

ROI: giảm 60–80% thời gian xử lý · hoàn vốn 6–12 tháng

Kiểm chứng ở quy mô ngân hàng thương mại

Trong khuôn khổ liên danh với SSG, bộ module AI của DBIZ Autonomous là **điểm khác biệt cạnh tranh lớn nhất** trong hồ sơ giải pháp dữ liệu cho một ngân hàng TMCP tại Việt Nam — nơi mọi cam kết đều phải đo được.

Giá trị cam kết của các module AI trong hồ sơ

Module AI	Giá trị cam kết
Invoice Processing	Thời gian xử lý hoá đơn giảm 80% (5–7 ngày → 4–8 giờ); lỗi nhập liệu từ 3–5% xuống dưới 0,5%.
Expense Approval	60% đề nghị chi phí tự phê duyệt trong 30 phút; phát hiện bất thường, chống gian lận.
Cash Flow Forecasting	Dự báo 7 ngày với mục tiêu chính xác ≥ 95% — tối ưu 0,1–0,3% trên vốn khả dụng.
AR/AP Reconciliation	Tự khớp trên 85% công nợ; kỳ đối soát cuối tháng từ 5–7 ngày còn 1–2 ngày.
Budget Management	Kiểm soát ngân sách 100% thời gian thực; cảnh báo vượt ngân sách trước 2–4 tuần.
Credit Scoring	Chấm điểm tín dụng thời gian thực dưới 3 giây; AI giải thích được bằng tiếng Việt.
PII Detection (tiếng Việt)	Tự nhận diện và che dữ liệu cá nhân đặc thù Việt Nam — đáp ứng ND 13/2023 không cần thao tác tay.

Số liệu theo hồ sơ đề xuất kỹ thuật của liên danh (2026); danh tính khách hàng được bảo mật theo cam kết dự án. KPI nghiệm thu chốt theo baseline thực tế.

Vì sao thắng thầu kỹ thuật

Các nhà thầu khác chào hạ tầng dữ liệu thuần túy — DBIZ chào hạ tầng **cộng** lớp AI nghiệp vụ trên cùng một kiến trúc.

Chuẩn ngành khắt khe

Kiến trúc module vượt qua thẩm định của môi trường ngân hàng: bảo mật, tuân thủ, giải trình từng quyết định AI.

Nhân rộng đa ngành

Cùng bộ agent đang phục vụ sản xuất, bán lẻ, phân phối, dịch vụ — ngân hàng là phép thử khó nhất, không phải duy nhất.

Điểm khác biệt quyết định: khách hàng nhận cả "kho vàng" lẫn "đội thợ kim hoàn" trong một dự án — dữ liệu hợp nhất và đội agent biến dữ liệu đó thành công việc đã hoàn thành.

AI có trách nhiệm theo chuẩn ISO 42001

DBIZ đạt chứng nhận **ISO/IEC 27001:2022** và xây dựng **ISO/IEC 42001** thành năng lực sản phẩm — mọi nguyên tắc AI có trách nhiệm được hiện thực hoá bằng kiến trúc, không dừng ở cam kết trên giấy.

ISO/IEC 42001

Quản trị AI: sổ đăng ký, đánh giá tác động, model card, giám sát bias/drift — qua AI Governance Control Plane.

ISO/IEC 27001:2022

An toàn thông tin: quy trình bảo mật được chứng nhận và kiểm toán độc lập định kỳ trên toàn hệ thống.

Bốn cam kết AI có trách nhiệm của DBIZ

Cam kết	Hiện thực hoá trong sản phẩm
Giải thích được	Câu trả lời kèm dẫn nguồn kiểm chứng được; quyết định chấm điểm kèm yếu tố ảnh hưởng — bằng tiếng Việt.
Chống ảo giác	RAG bắt buộc trích dẫn; Text-to-SQL qua semantic layer và tường lửa; độ tin cậy thấp → chuyển người xử lý.
Không tự học từ dữ liệu người dùng	Mọi cập nhật tri thức qua vòng kiểm duyệt của con người (review → curation → publication) — có vết audit đầy đủ.
Con người chịu trách nhiệm	Mỗi agent có chủ sở hữu; hành động rủi ro có người phê duyệt; nhãn "AI-generated" minh bạch với người dùng cuối.

Chủ quyền dữ liệu

Model và dữ liệu trong hạ tầng doanh nghiệp — tuân thủ Luật ATTT, ND 13/2023 và yêu cầu data localization.

Đánh giá định kỳ

Eval harness chạy theo chu kỳ; drift và bias được phát hiện, xử lý sớm — chất lượng AI là chỉ số vận hành.

Chứng minh, không tuyên bố

Hồ sơ quản trị AI đầy đủ theo 42001 — sẵn sàng cho thẩm định của khách hàng và cơ quan quản lý.

Phương pháp Oracle OUM + Agile

DBIZ triển khai theo chuẩn quốc tế Oracle Unified Method kết hợp nhịp Agile (sprint 2–4 tuần), theo cách tiếp cận **use-case-first**: mỗi sprint bàn giao một năng lực agent chạy thật trên dữ liệu thật — không "chờ 12 tháng mới thấy kết quả".

1 • Inception

Chọn use-case theo 4 tiêu chí; chốt KPI & baseline; thiết kế guardrails ban đầu.

2 • Elaboration

Thiết kế workflow agent, đầu nối dữ liệu & tri thức, dựng hạ tầng GPU.

3 • Construction

Xây theo sprint — agent bàn giao cuốn chiếu, chạy thử với người dùng thật.

4 • Transition

UAT, đào tạo giao việc & phê duyệt, hypercare sát cánh sau go-live.

5 • Production

Vận hành & tối ưu — đánh giá quý bằng số liệu, nâng mức tự chủ, thêm use-case.

ROI cam kết — đo trên dữ liệu thật

60–80%

giảm thời gian xử lý quy trình được agent-hoá

~40%

tăng năng suất đội ngũ vận hành

6–12

tháng hoàn vốn điển hình của dự án agent

ođ

phí API AI trả cho nhà cung cấp nước ngoài

Ước tính tiêu biểu từ các dự án DBIZ; con số thực tế thay đổi theo hiện trạng doanh nghiệp.

Mô hình license linh hoạt

Mua theo agent

Kích hoạt từng agent hoặc từng nhóm nghiệp vụ — bắt đầu đúng chỗ đau nhất, mở rộng khi thấy giá trị.

Subscription theo tenant

Usage tracking và billing đo mức dùng thực tế — chi phí minh bạch, dự toán được.

SaaS hoặc On-premise

Khách hàng regulated triển khai on-premise trọn bộ, kể cả GPU và model — không phiên bản "rút gọn".

Sẵn sàng để **AI làm việc thật** cho doanh nghiệp của bạn?

Đội ngũ DBIZ sẵn sàng cùng bạn chọn use-case đầu tiên và đề xuất lộ trình
Autonomous — Data Lakehouse — Foundation phù hợp quy mô của bạn.

www.dbiz.com • crm.dbiz.com • contact@dbiz.com • 0968 695 865

Tầng 4, Toà nhà Savina, Số 1 Đinh Lễ, Hoàn Kiếm, Hà Nội

d b i z