

GOVERNED ACCESS LAYER

# COLOSSOS

**Secure deployment of agentic AI on existing enterprise systems — without replatforming.**

Governance, compliance, IT security, and investment protection for agentic AI in the enterprise context.



Enterprise  
Systems

**COLOSSOS  
Governed  
Access Layer**

Agentic AI  
Processing

*The secure path to deploying agentic AI*

# The real enterprise gap

Standard processes are digitized. The cost-intensive, complex exception cases remain manually coordinated.



# Why agentic AI doesn't yet scale in production

The technology is here. Controlled execution on enterprise systems is missing.

1

## RPA

Strong with stable rules

---

**Breaks on exceptions  
and complexity**

2

## Copilots

Assist humans

---

**Don't execute  
autonomously**

3

## API / Middleware

Connect systems

---

**No compliance,  
no audit log**

4

## AI platforms

Bring agents

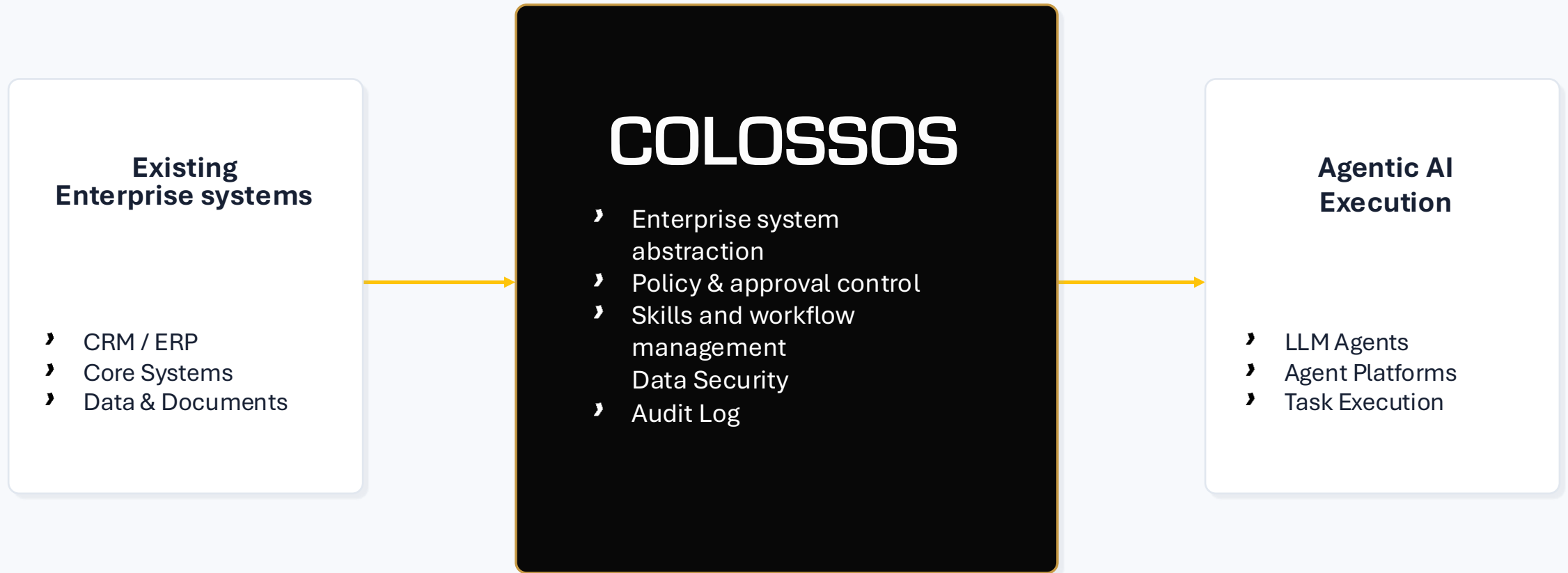
---

**Lock skills into their  
own platforms**

**The gap isn't "even more AI," but a secure operating layer  
between agents and existing systems.**

# COLOSSOS closes the gap

A governed access layer for secure agentic AI execution on existing enterprise systems.



**Without replatforming: COLOSSOS controls the path from AI deployment → case context & actions → auditability.**

# Security has three operational dimensions

COLOSSOS makes agentic execution legally secure and compliant.

1

## Compliance

Traceability, policy application, and an audit trail for auditable AI use.

2

## Governance

Authority over permitted actions, approvals, skills, and IT usage stays within the company.

3

## IT Security

Controlled data flow: agents work only with approved context and defined system access.

**The core benefit: agentic AI moves from a risky experiment to a controllable enterprise operating model.**

# Investment protection in an open agent market

Which agent platform will win is still unclear. The valuable process intelligence shouldn't be locked into it.

## WITHOUT COLOSSOS

Skills + workflows + enterprise connectors  
live in the agent platform

---

Platform switch = rebuild risk

## WITH COLOSSOS

Skills + workflows + enterprise connectors  
remain in COLOSSOS

The agent layer becomes  
interchangeable

OpenAI

Anthropic

Agent X

The investment stays in COLOSSOS — not in a potentially short-lived agent platform.

# From manual casework to controlled execution

COLOSSOS operationalizes exception cases for AI agents — without replacing existing systems.

## TODAY

### Human gathers context

from multiple systems

### Human interprets case

data, rules, status

### Human decides / escalates

with risk and waiting time



The COLOSSOS  
Transformation

## WITH COLOSSOS

### Case context is structured

agent-consumable case context, skills & workflows

### Policies + approvals control

permitted actions and approvals, human in the loop

### Legally secure, controlled execution

with audit logging and review

**Value lever: less manual coordination, faster processing, better control.**

# What COLOSSOS anchors in the enterprise

Two competency blocks that create value independently of the respective agent model.

## BLOCK 1

### Governance, Security & Audit Control

- › Policy Enforcement
- › Approval Gates
- › Data Security & Audit Trail

## BLOCK 2

### Skill & Workflow Management

- › Business Actions & Policies
- › Exception Workflows
- › Agent-consumable Case Context

**Together they form a controlled execution path for agentic AI — not just a technical integration.**

# The entry point: COLOSSOS Exception Casework Pilot

A clearly scoped pilot that proves value and deliverability — without a platform project.

## SCOPE

- › 1 exception process
- › 2–4 systems
- › 5–12 Business Actions
- › 1 Policy Pack
- › 1 Approval model

## DELIVERY

- › 45-day delivery commitment
- › after use-case review
- › deployable, not deployed

## GUARDRAILS

- › No happy paths
- › No replatforming story
- › No generic platform initiative
- › Scope changes only by agreement

**The pilot makes a real exception process agentically processable —  
secure, auditable, and on existing systems.**

# Why now?

Agentic AI is reality and will become the decisive differentiator in an efficient corporate cost structure.

The winner will be whoever keeps control over execution and data and brings agentic AI into production quickly and scales it successfully.

## Secure execution

Agents access context, systems, data, and actions only in a controlled way.

## No replatforming dependency

Existing systems remain. COLOSSOS adds the governance and execution layer dimension.

## Investment protection

Skills and workflows remain usable agent-agnostically.

## Provable entry

The pilot focuses on one exception process with clear value and transparent guardrails.

**Next step: qualify a suitable use case.**

GOVERNED ACCESS LAYER

# COLOSSOS

Thank you.



COLOSSOS is a product of ALLEHERZEN GmbH

Alwinenstr. 3 | 65189 Wiesbaden | Germany

[www.COLOSSOS.ai](http://www.COLOSSOS.ai) | [hello@COLOSSOS.ai](mailto:hello@COLOSSOS.ai)

