Activeo

Deploying AI Agents with Robust Failover, Monitoring, and Governance Controls

Jonathan Mondon
Head of Enterprise,
Activeo

90%

Nearly 90% of executives believe their company delivers great customer experience

40%

but only about 40% of customers agree

PwC's 2025 Global Customer Experience Survey

CX Has Reached a Tipping Point

CHANNELS WITHOUT COHESION

Voice, chat, email, and social exist as siloed points of contact.

RISING EXPECTATIONS

Regardless of internal complexity, customers demand speed, consistency, and a unified experience.

PLATFORM & SYSTEM SILOS

Disconnected tools like CRM, CCaaS, and WFM create friction instead of seamless flow.

INVESTMENT VS. EXPERIENCE

Spending on technology has increased, yet significant CX quality gaps persist.

FRONT & BACK OFFICE GAP

Customer-facing and operations teams still operate as separate worlds; lacking connection.

INTEGRATION GAP

CHANNEL REACH

MARKET TREND

FRONT-OFFICE VIEW

BACK-OFFICE VIEW

Activeo

The Enterprise AI Challenge

80%

of companies reported AI agents took unintended actions

58%

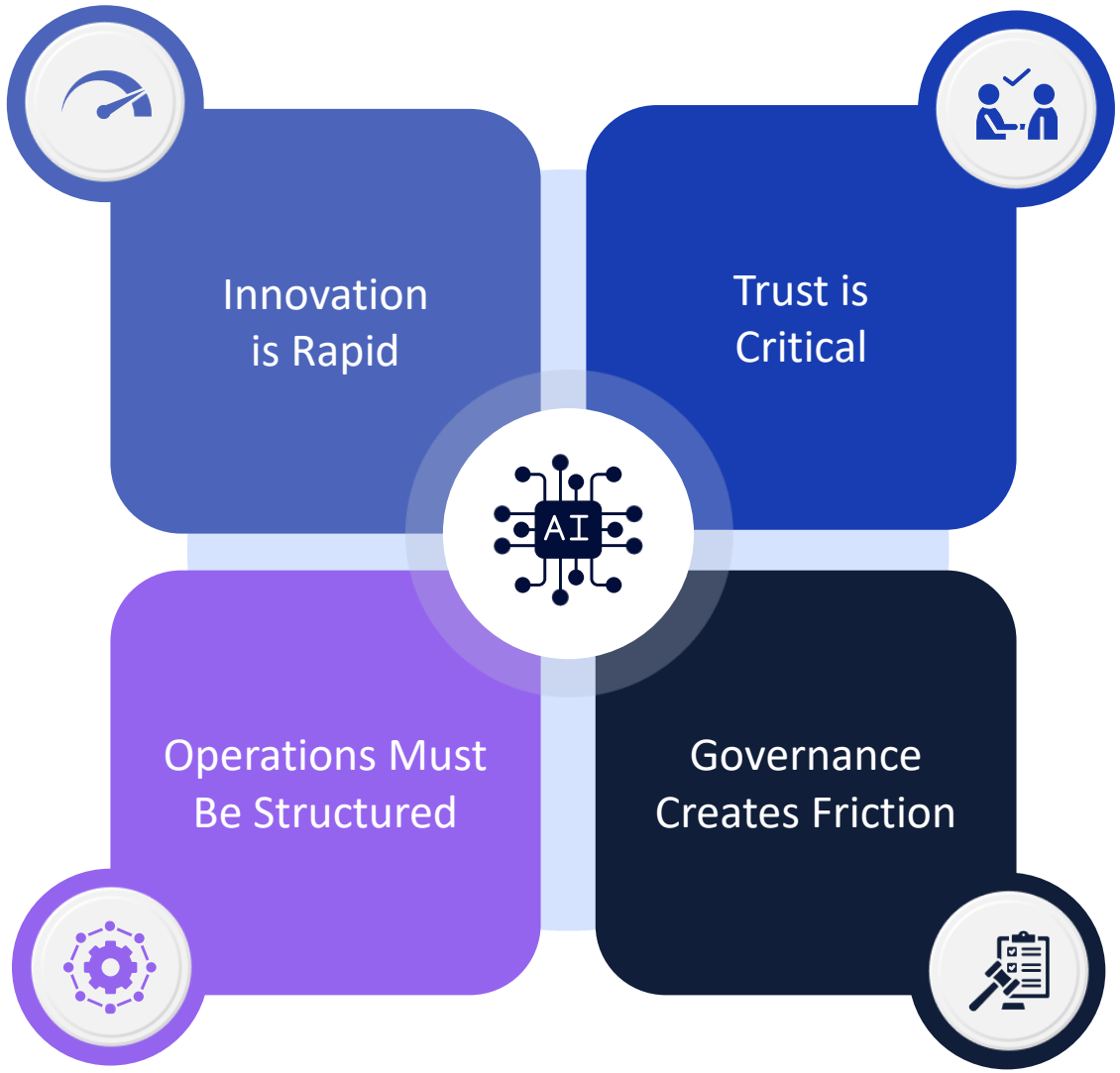
Cite potential for unintended actions as key risk

39%

Worry about unauthorized system access

Activeo

AI is Moving Fast, Adoption is Not



RAPID AI CAPABILITIES

TRUST
GOVERNANCE
COMPLIANCE
OPERATIONS

Activeo

Risks of Using Generative AI

Regulatory & Ethical Challenges


CNN Business

Sign In

Business / Tech

EU approves landmark AI law, leapfrogging US to regulate critical but worrying new technology

By Brian Fung, CNN

2 min read · Published 8:04 AM EDT, Wed March 13, 2024

Walter Zerla/Image Source/Getty Images/File

(CNN) — European Union lawmakers gave final approval Wednesday to a landmark law governing artificial intelligence, leapfrogging the United States once again on the regulation of a critical and disruptive technology.

[CNN March 2024](#)

Model Bias & Fairness Issues


Arnold&Porter

Menu

Advisories

August 1, 2023

Yet Another Warning From Banking Regulators About AI Bias

Advisory

By Amber A. Hay, Michael A. Mancusi, Kevin M. Toomey, Christopher L. Allen, Peter J. Schildkraut, Paul Lim

On July 18, 2023, Federal Reserve Vice Chair for Supervi Michael Barr cautioned banks against fair lending violati arising from their use of artificial intelligence (AI). Traini on data reflecting societal biases; data sets that are incomplete, inaccurate, or nonrepresentative; algorithms specifying variables unintentionally correlated with prote characteristics; and other problems can produce discriminatory results.

[Arnold & Porter, Aug 2023](#)

Data Privacy & Security


BBC

Register

Sign In

ChatGPT banned in Italy over privacy concerns

1 April 2023

Share Save

Shiona McCallum Technology reporter

OpenAI launched ChatGPT last November

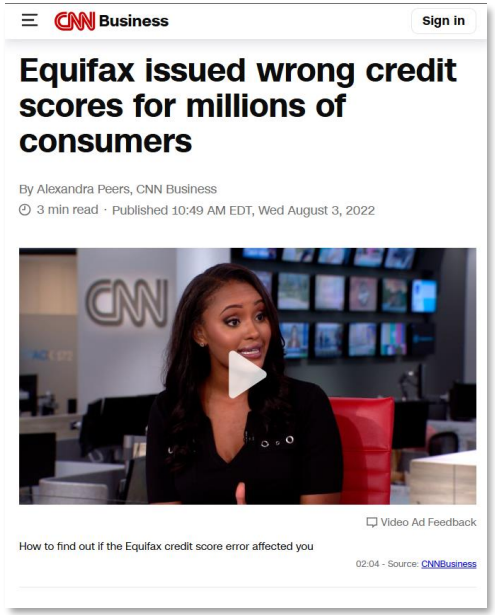
Italy has become the first Western country to block advanced chatbot ChatGPT.

The Italian data-protection authority said there were privacy concerns relating to the model, which was created by US start-up OpenAI and is backed by Microsoft.

The regulator said it would ban and investigate OpenAI "with immediate effect".

[BBC News, Apr 2023](#)

System Failures & Errors


CNN Business

Sign in

Equifax issued wrong credit scores for millions of consumers

By Alexandra Peers, CNN Business

3 min read · Published 10:49 AM EDT, Wed August 3, 2022

Video Ad Feedback

How to find out if the Equifax credit score error affected you

02:04 - Source: CNNBusiness

[CNN Business, Aug 2022](#)

Activeo

Architecture: Built for Reliability

AI

Process Definition Layer

- Explicit state management
- Mandatory flows encoded
- Audit trail for every decision

What AI is allowed to do

AI

Flexible Response Layer

- Natural language understanding
- Dynamic content generation
- Contextual responses

How AI communicates

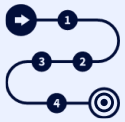
People

Safety & Compliance Layer

- Response validation
- Authority boundary enforcement
- Human escalation triggers

When AI must stop or escalate

Process



Orchestration Engine

- Real-time streaming
- Multi-system integration
- Smart routing
- Context preservation

How everything stays fast & connected

Activeo

Best Practice: Limit LLM Usage (Where the HUMAN Comes In)

Process Control

Explicit state machines

instead of

LLM interpreting from prompts

Error Handling

Deterministic recovery paths

instead of

LLM self-correction

Compliance

Enforced through architecture

instead of

Best-effort prompting

Flexibility

Controlled creativity within boundaries

instead of

Maximum LLM autonomy

Activeo

Unhappy Path: What Could Go Wrong Without Governance

Context:
A telco launches AI agent for plan upsell, billing disputes, and churn prevention
— with insufficient governance controls

No Failover → Cascade Failure

LLM provider outage. No fallback model. 4-hour AI Agent blackout during peak billing period. 38,000 customers hit dead ends.

No Monitoring → Silent Drift

A routine model update silently changed how the AI Agent described pricing plans. No regression testing. No alerting. 11 days of wrong answers.

No Audit Trail → Regulatory Breach

Regulator requested conversation logs for complaint investigation. No immutable logs existed. A significant regulatory fine.

Over-Automation → Trust Erosion

AI Agent autonomously processed RM500+ credits without human approval. Exploited by fraudster during 3 days before the company notice.

If this happens to an Enterprise in real life, the potential cost:
A significant regulatory fine · 6-month deployment freeze · Emergency remediation costs ·
NPS -31 · 14 months rebuilding customer trust

Activeo

Happy Path: AI Agent When It’s Done Right

Context:
SEA regional bank deploys AI agent for account servicing, fraud alerts & loan pre-qualification across WhatsApp + app + voice IVR

Fallback

Primary: AI Agent may fail, latency may raise, plan for an alternative path to ensure good Customer Experience.

Full Observability

Every AI Agent’s conversations logged with trace ID, logs of what system it accessed and actions it took, confidence score. Anomaly detected & flagged in <90 seconds.

Guardrails Active

PII auto-redacted before LLM call. Fraud topic triggers immediate human escalation. Zero regulatory breaches in 18 months.

Human-in-the-Loop

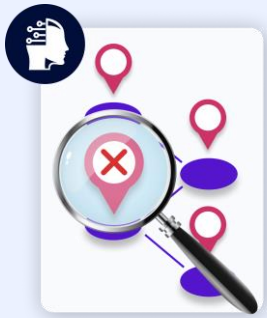
Confidence < 0.72 = routed to human agent with full context information. Human Agent’s resolution time cut by 28% with AI-assisted agent.

If this happens to any Enterprise in real life, possible outcomes:
AI Agents handled 3.2M interactions· 99.7% uptime · NPS +22 ·
Aligned to Technology Risk Management Guidelines

Activeo

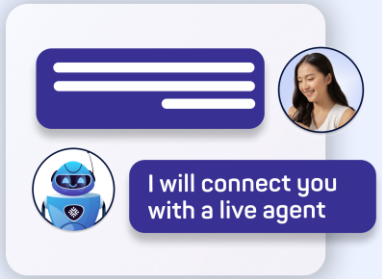
3 Takeaways Today

1



Map your AI Agent's failure modes — before your customers find them for you.

2



Define your human escalation threshold. “Under exactly which conditions should AI Agent transfer to a human?”

3

Ensure you have a Disaster Recovery (DR) plan for when AI Agent fails when there is a service outage.

"The question isn't whether your AI agent will fail.
It's whether you built it to fail safely."

Activeo

Activeo

Improving CX in APAC for more than 10 years

IN SINGAPORE

Since 2012

AI PROJECTS DELIVERED

30+ projects in APAC and beyond

EARLY ADOPTION

Started GenAI since March 2023

CUSTOMER DATA

CX & CUSTOMER ENGAGEMENT

IT HELPDESK

VOICE OF THE CUSTOMER

CX AND DX BUSINESS CONSULTING

IMPLEMENTATION

OPTIMISATION