

AI is Here: Now What? A Credit Union Playbook for Responsible Adoption

Amy Travers

Sponsored By:

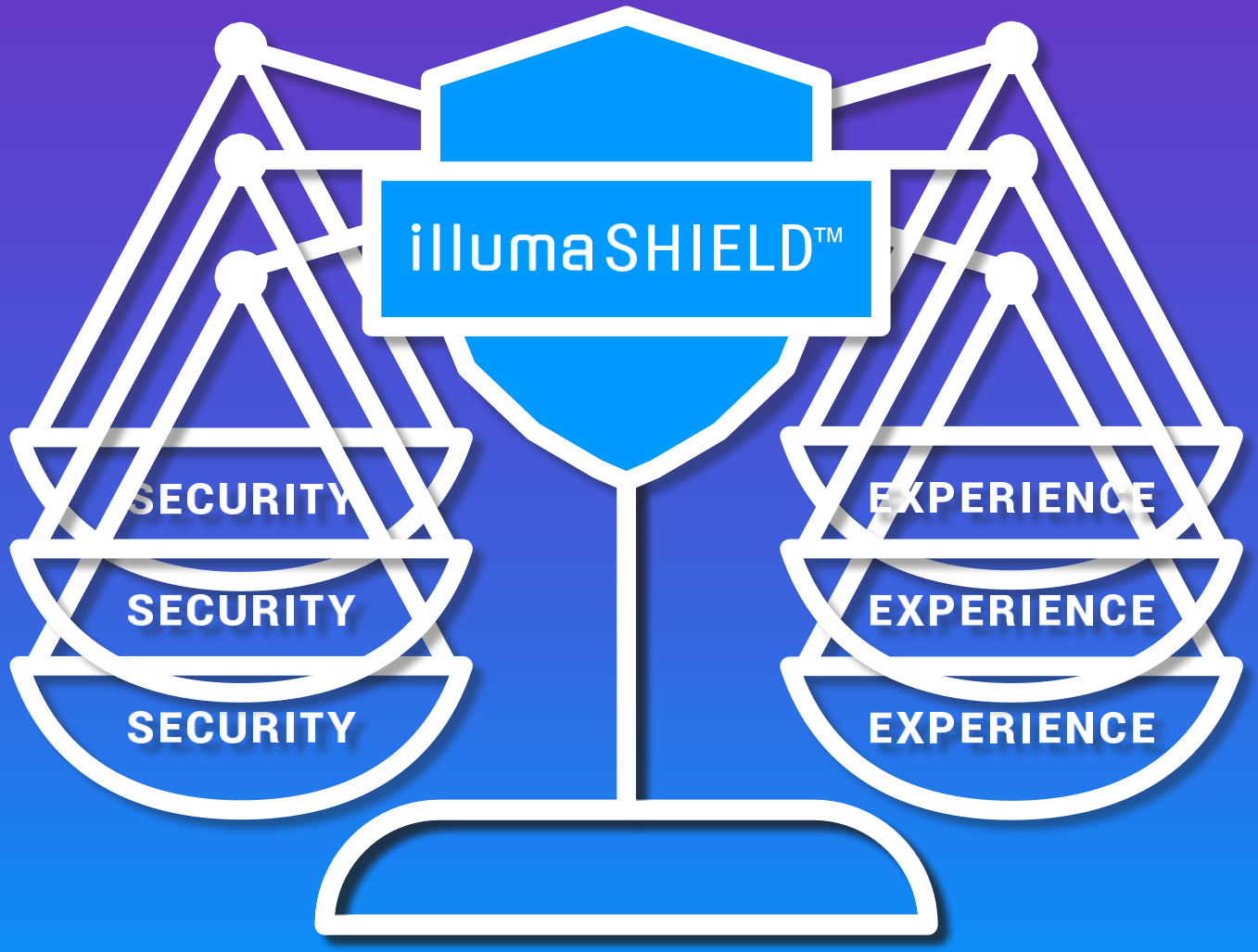
illuma

illuma

AI IS HERE — NOW WHAT?

A CREDIT UNION PLAYBOOK FOR RESPONSIBLE ADOPTION

BALANCED VOICE SECURITY



illuma

HOMELAND SECURITY SUCCESS STORY

DHS
SUCCESS STORIES

Illuma Labs



TOTAL DHS SBIR INVESTMENT
$1.9M

IMPACT
Millions of dollars saved in operating costs; heightened security against fraudsters

www.illuma-labs.com
7700 Windrose Ave, Suite G300
Plano, TX 75024

Each year, Americans lose an estimated $10 billion through phone scams, as reported in research from TrueCaller. Whether scammers claim they are from the Internal Revenue Service, a credit card company, or a host of other hypothetical entities, nearly one in six Americans reported losing money to phone scams in 2017, an almost 70% increase over the previous year. Scammers target individual consumers as well as large financial institutions, who have a growing problem with criminals stealing identities to take over legitimate customers' accounts and commit fraud. With help from the Department of Homeland Security (DHS) Small Business Innovation Research program (SBIR), Illuma Labs has developed a tool to outmaneuver these fraudsters.

CYBERSECURITY, INFRASTRUCTURE PROTECTION, AND INNOVATION SUBCOMMITTEE BRIEFING

APRIL 2, 2019

Roundtable Briefing on the Science and Technology Directorate's Use of the Small Business Innovation Research Program



Pictured (from left): Richard Shockey, Mark D. Collier, Milind Borkar, Dani Charles

illumaSHIELD™

SOME OF OUR CUSTOMERS















































illuma

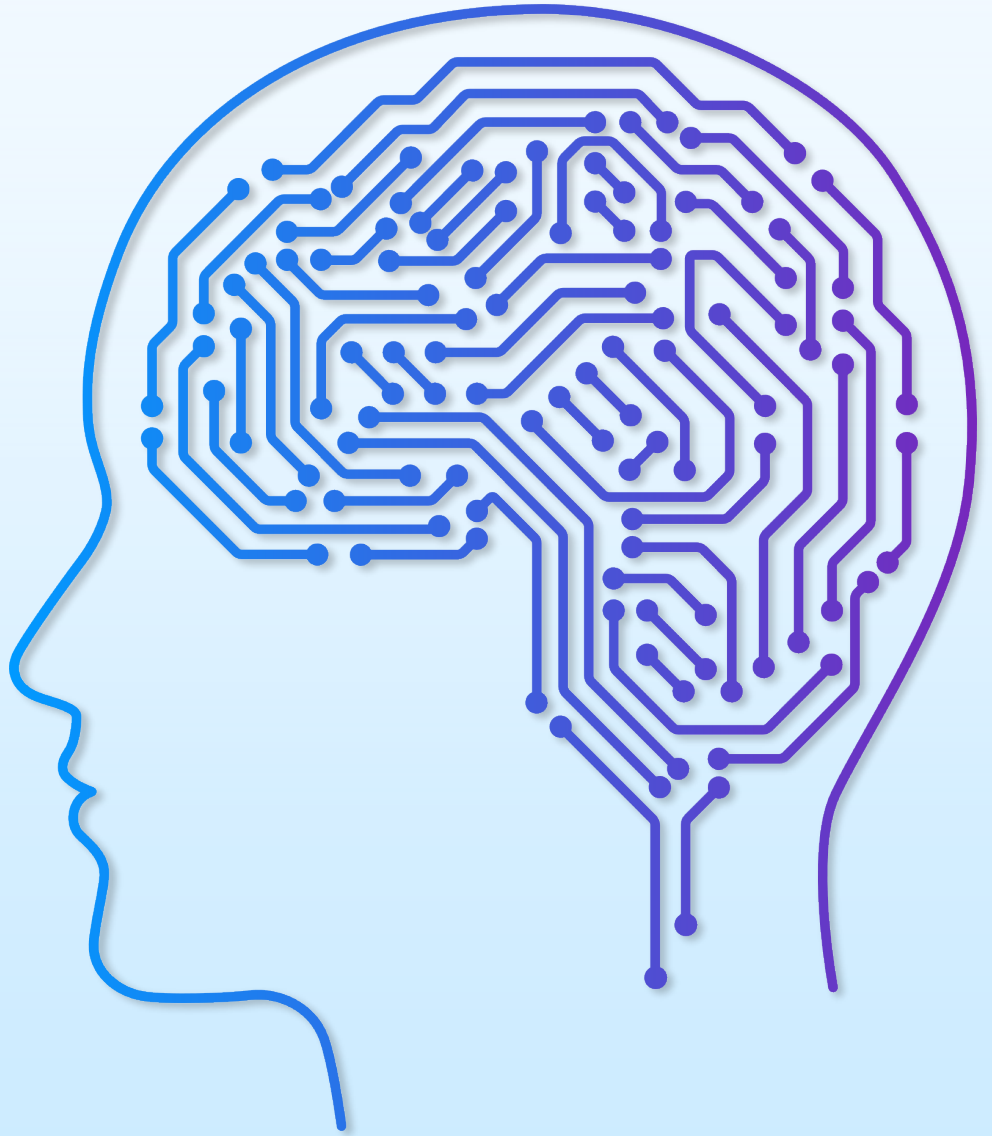
WHAT IS AI?

According to ChatGPT

- AI (Artificial Intelligence) refers to the simulation of human intelligence in machines that are designed to think, learn, and problem-solve.

Types of AI

- **Narrow AI (Weak AI) –** AI designed for specific tasks like virtual assistants (Siri, Alexa), recommendation systems (Netflix, YouTube), and self-driving cars.
- **General AI (Strong AI) –** AI with human-like cognitive abilities that can perform any intellectual task a human can.
- **Superintelligent AI –** A hypothetical AI surpassing human intelligence, capable of independent reasoning and problem-solving.



EVOLUTION OF AI

THEORETICAL FOUNDATIONS

1920s – 1950s

- Robot and Artificial Intelligence terms introduced
- First paper on artificial neurons
- Alan Turing introduces Turing Test

RULE BASED AI

1960s – 1980s

- IF-THEN rules mimicking human decision making
- ELIZA: First chatbot
- AI Winter: Limited computational power, data and funding

MACHINE LEARNING & DATA DRIVEN AI

1990s – 2000s

- IBM's Deep Blue defeated chess champion Kasparov
- WWW enables access to vast amounts of data
- Growing computational power enables shift from rule-based to data-driven models

DEEP LEARNING, GENERATIVE & AGENTIC AI

2010s – 2020s

- IBM Watson wins Jeopardy
- AlexNet revolutionizes image recognition
- Google AlphaGo defeats humans
- Generative & Agentic tolos available to public

AI IN THE CONTACT CENTER

SIMPLIFY VERIFICATION FOR AGENTS AND MEMBERS

Member Contact Center:

The Value of Voice Biometric Authentication

ConneXus Credit Union

GENERATIVE AI





DEEPFAKE ATTACKS ARE A GROWING THREAT

CereProc

RESEMBLE.AI

TTS

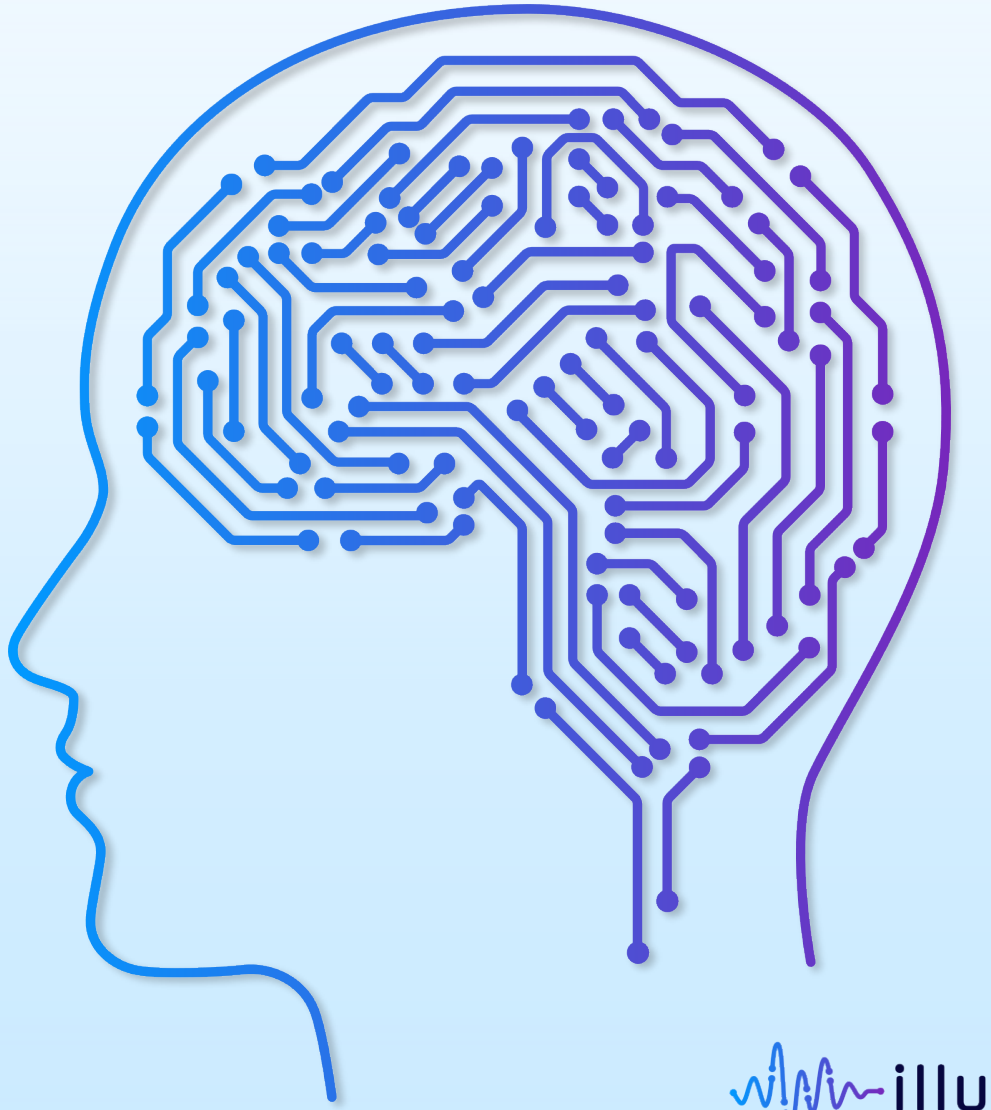
reSpeecher

IIElevenLabs

descript

VALL-E

REPLICA



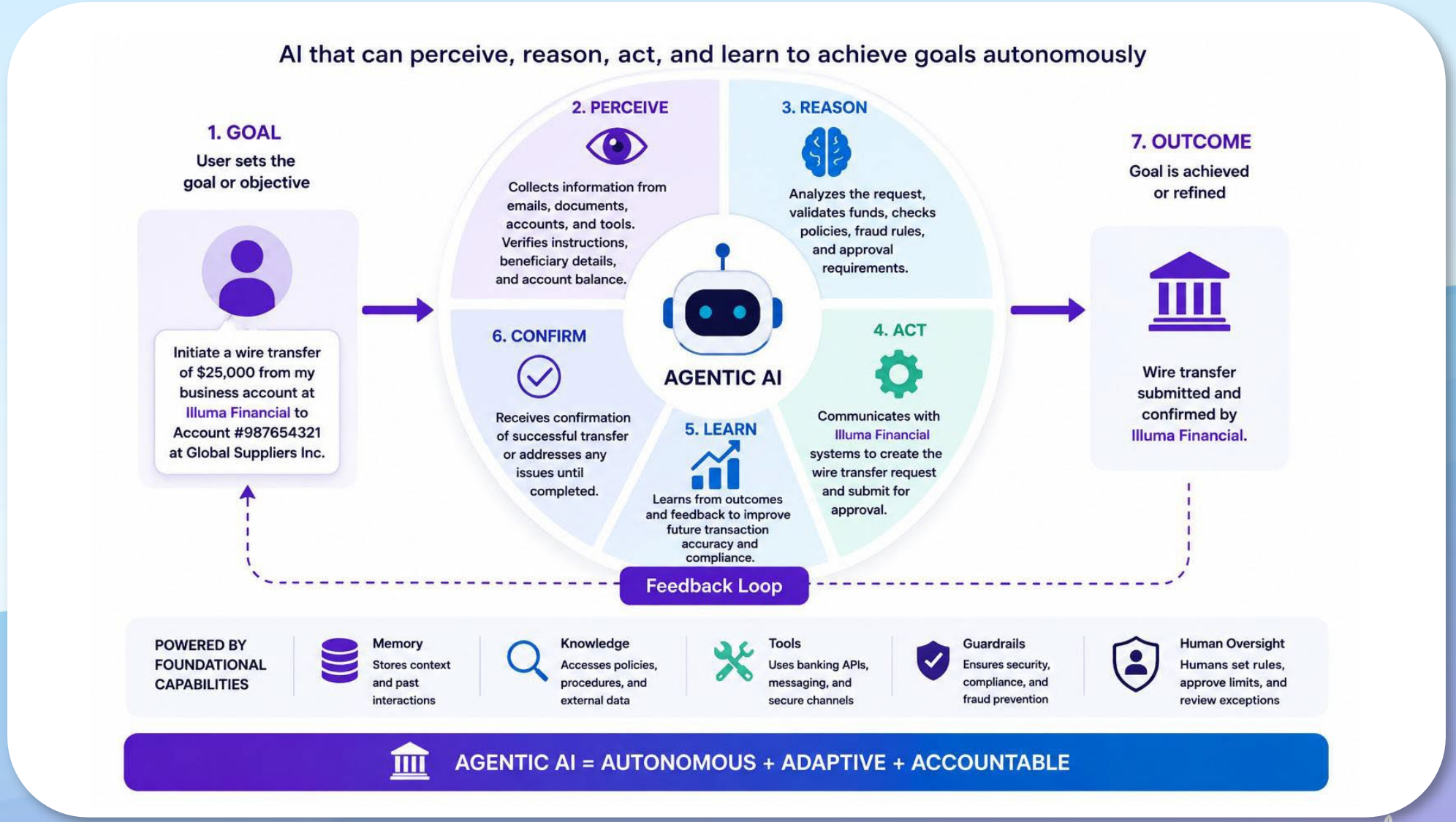
illuma

FRAUDSTERS HAVE IT EASY





AGENTIC AI


AI that can perceive, reason, act, and learn to achieve goals autonomously
1. GOAL
User sets the goal or objective
Initiate a wire transfer of $25,000 from my business account at Illuma Financial to Account #987654321 at Global Suppliers Inc.
2. PERCEIVE
Collects information from emails, documents, accounts, and tools. Verifies instructions, beneficiary details, and account balance.
3. REASON
Analyzes the request, validates funds, checks policies, fraud rules, and approval requirements.
AGENTIC AI
4. ACT
Communicates with Illuma Financial systems to create the wire transfer request and submit for approval.
5. LEARN
Learns from outcomes and feedback to improve future transaction accuracy and compliance.
6. CONFIRM
Receives confirmation of successful transfer or addresses any issues until completed.
7. OUTCOME
Goal is achieved or refined
Wire transfer submitted and confirmed by Illuma Financial.
Feedback Loop
POWERED BY FOUNDATIONAL CAPABILITIES
Memory
Stores context and past interactions
Knowledge
Accesses policies, procedures, and external data
Tools
Uses banking APIs, messaging, and secure channels
Guardrails
Ensures security, compliance, and fraud prevention
Human Oversight
Humans set rules, approve limits, and review exceptions
AGENTIC AI = AUTONOMOUS + ADAPTIVE + ACCOUNTABLE

FRAUD IS RAMPANT

‘Fraud on a massive scale’: Baseball star Shohei Ohtani’s ex-interpreter faces federal charge after allegedly stealing $16M

Hong Kong police Hong Kong / Law and Crime

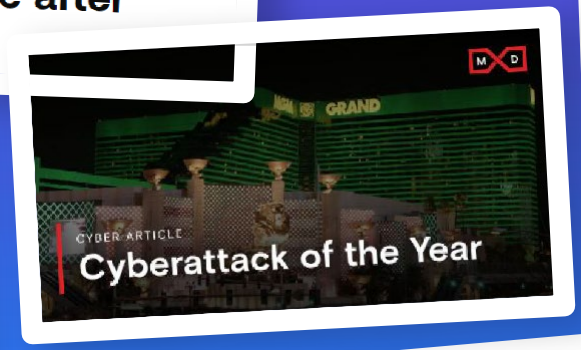
‘Everyone looked real’: multinational firm’s Hong Kong office loses HK$200 million after scammers stage deepfake video meeting

Employee fooled after seeing digitally recreated versions of company’s chief financial officer and others in video call

Bloomberg

MGM Resorts Hackers Broke In After Tricking IT Service Desk





Arizona Mother Recounts Horror of Deepfake Kidnapping Scam

HEADLINE JUN 15, 2023

U.S. Treasury: Gen AI and Deepfakes Make it Easier to Con Financial Institutions

by Technology Specialist Tim Keary · Fact Checked by Eddie Wrenn · Updated on 29 March 2024



CBC

Hackers steal $14.2M from Alberta-base bank, sparking court battle with B.C. crypto fi n

CBC
April 12, 2024 · 6 min read

Finance worker pays out $25 million after video call with deepfake ‘chief financial officer’

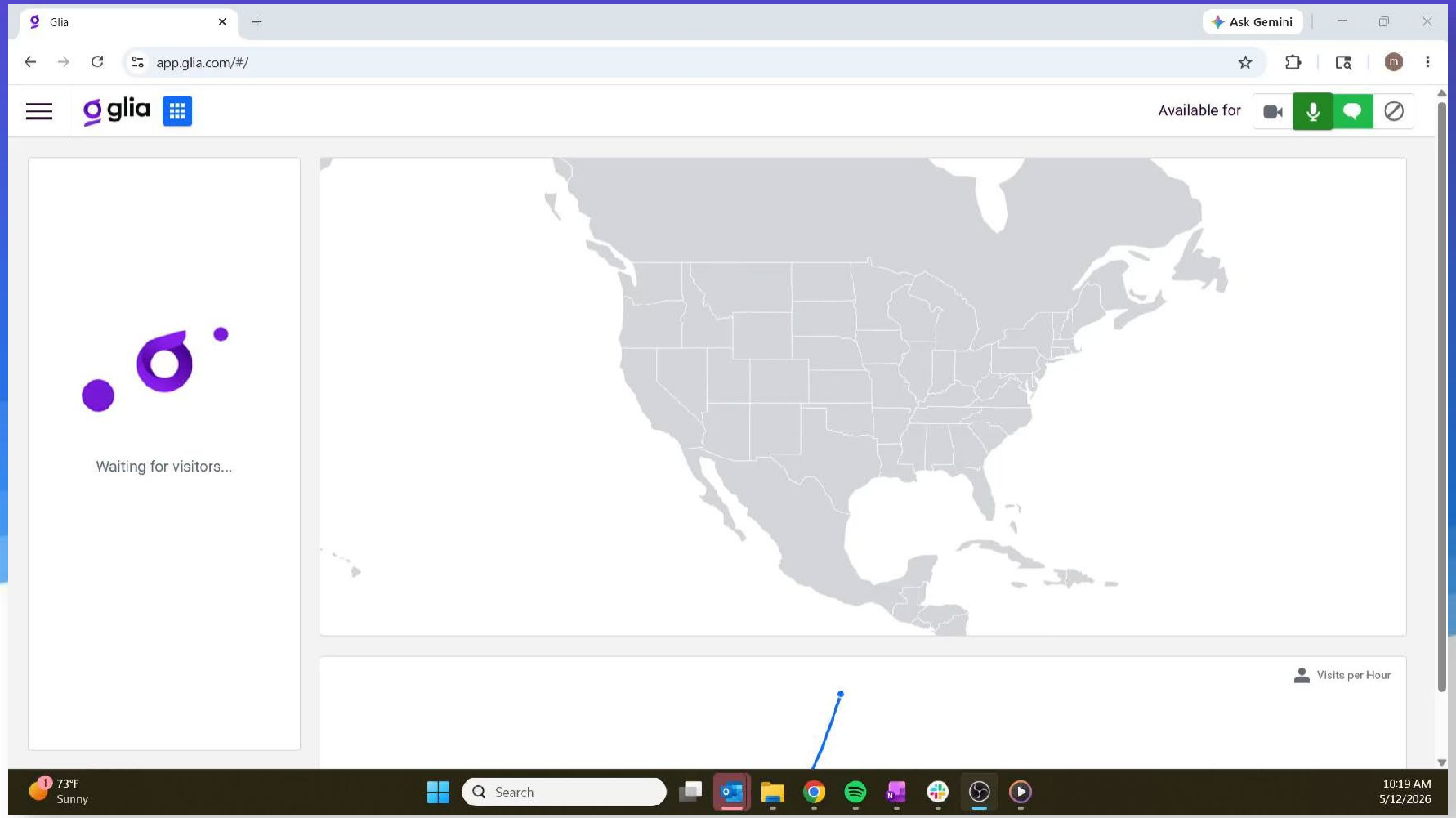
By Heather Chen and Kathleen Magramo, CNN
2 minute read · Published 2:31 AM EST, Sun February 4, 2024

Wiz CEO says company was targeted with deepfake attack that used his voice

October 28, 2024

illuma

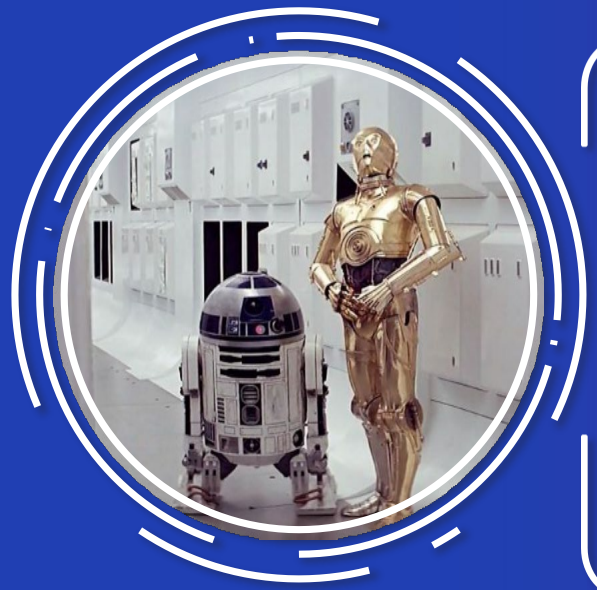
WE NEED AI TO BATTLE AI



WHAT IS THE FUTURE OF AI?

R&D Focus on Artificial General Intelligence (AGI)

Machines that can think and reason like humans



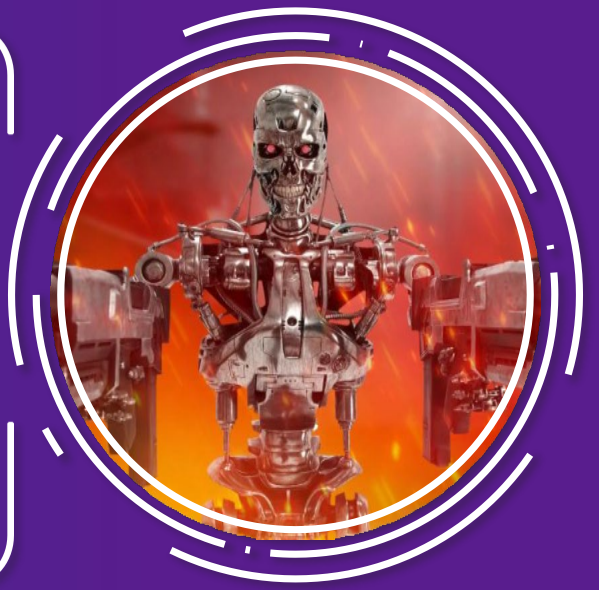
A FUTURE OF COLLABORATION

AI that enhances human potential, solves complex problems, and improves lives.

OR

A FUTURE OF RISK

AI that is misused, uncontrolled, or misaligned with human values.



Ethics, Regulation and Responsible AI Development are Key Concerns

WHAT IS ETHICAL AI?

Goal: Ensure that AI technologies benefit society while minimizing harm



FAIR & UNBIASED

Free from biases in data and decisions



TRANSPARENT & EXPLAINABLE

Understand how and why a decision was made



ACCOUNTABLE & RESPONSIBLE

Accountability for decisions made by AI



PRIVACY & SECURITY

Protect user data and comply with privacy laws



HUMAN CENTRIC DESIGN

Prioritize human well-being and not replace human judgment

ETHICAL AI



FAIR & UNBIASED

- DOCUMENT KNOWN LIMITATIONS AND FAILURE MODES
- TRAIN MODELS ON COMPREHENSIVE DATASETS WITH REAL-WORLD VARIATION
- CAREFULLY SELECT VARIABLES IN HIGH-STAKES DECISIONS
- CONDUCT REGULAR BIAS AUDITS TO IDENTIFY AND CORRECT SKEWED OUTPUTS
- BUILD CROSS-FUNCTIONAL TEAMS WITH VARIED EXPERTISE TO STRESS-TEST MODEL DESIGN
- USE ESTABLISHED METRICS TO EVALUATE MODEL PERFORMANCE

ETHICAL AI



TRANSPARENT & EXPLANABLE

- AVOID BLACK-BOX DEPLOYMENTS IN HIGH-STAKES DOMAINS
- PROVIDE CLEAR EXPLANATIONS FOR AI-DRIVEN DECISIONS
- DOCUMENT TRAINING DATA SOURCES, TRAINING METHODS AND INTENDED USE CASES
- USE EXPLAINABILITY TOOLS AND VISUALIZATIONS WHERE POSSIBLE
- MAKE CONFIDENCE SCORES AND UNCERTAINTY ESTIMATES VISIBLE WHEN APPROPRIATE
- CLEARLY DISCLOSE WHEN USERS ARE INTERACTING WITH AN AI SYSTEM

ETHICAL AI



ACCOUNTABLE & RESPONSIBLE

- ENSURE HUMAN OVERSIGHT IS MAINTAINED FOR IRREVERSIBLE OR HIGH-STAKES DECISIONS
- ASSIGN CLEAR OWNERSHIP FOR AI SYSTEMS THROUGHOUT LIFECYCLE
- CONDUCT PRE-DEPLOYMENT IMPACT ASSESSMENTS
- ESTABLISH AI GOVERNANCE COMMITTEE
- DEFINE ESCALATION PATHS WHEN AI SYSTEMS PRODUCE HARMFUL OR ERRONEOUS OUTCOMES
- MAINTAIN AUDIT TRAILS FOR MODEL DECISIONS, UPDATES, AND DATA USAGE

ETHICAL AI



PRIVACY & SECURITY

- SECURE AI SYSTEMS AGAINST CYBER THREATS, ADVERSARIAL ATTACKS, AND DATA LEAKS
- APPLY DATA MINIMIZATION — COLLECT ONLY WHAT IS STRICTLY NECESSARY FOR THE TASK
- CONDUCT REGULAR SECURITY TESTING
- ANONYMIZE OR PSEUDONYMIZE PERSONAL DATA USED IN TRAINING AND INFERENCE
- PROTECT SENSITIVE DATA THROUGH ENCRYPTION AND SECURE STORAGE PRACTICES
- COMPLY WITH APPLICABLE REGULATIONS AND SECTOR-SPECIFIC LAWS

ETHICAL AI



HUMAN-CENTRIC DESIGN

- KEEP HUMANS INVOLVED IN AND ACCOUNTABLE FOR HIGH-IMPACT DECISIONS
- DESIGN AI TO AUGMENT, NOT REPLACE, HUMAN JUDGMENT
- INCORPORATE CONTINUOUS USER FEEDBACK AND IMPROVEMENT
- ENSURE USERS CAN OVERRIDE, CHALLENGE, OR APPEAL AI-GENERATED RECOMMENDATIONS
- BUILD INTUITIVE USER EXPERIENCES
- TEST SYSTEMS WITH THE USER POPULATIONS THEY ARE BUILT TO SERVE

AI GOVERNANCE IS ESSENTIAL FOR SUCCESS

Policies, regulations, and frameworks to ensure that AI systems are developed, deployed and used responsibly

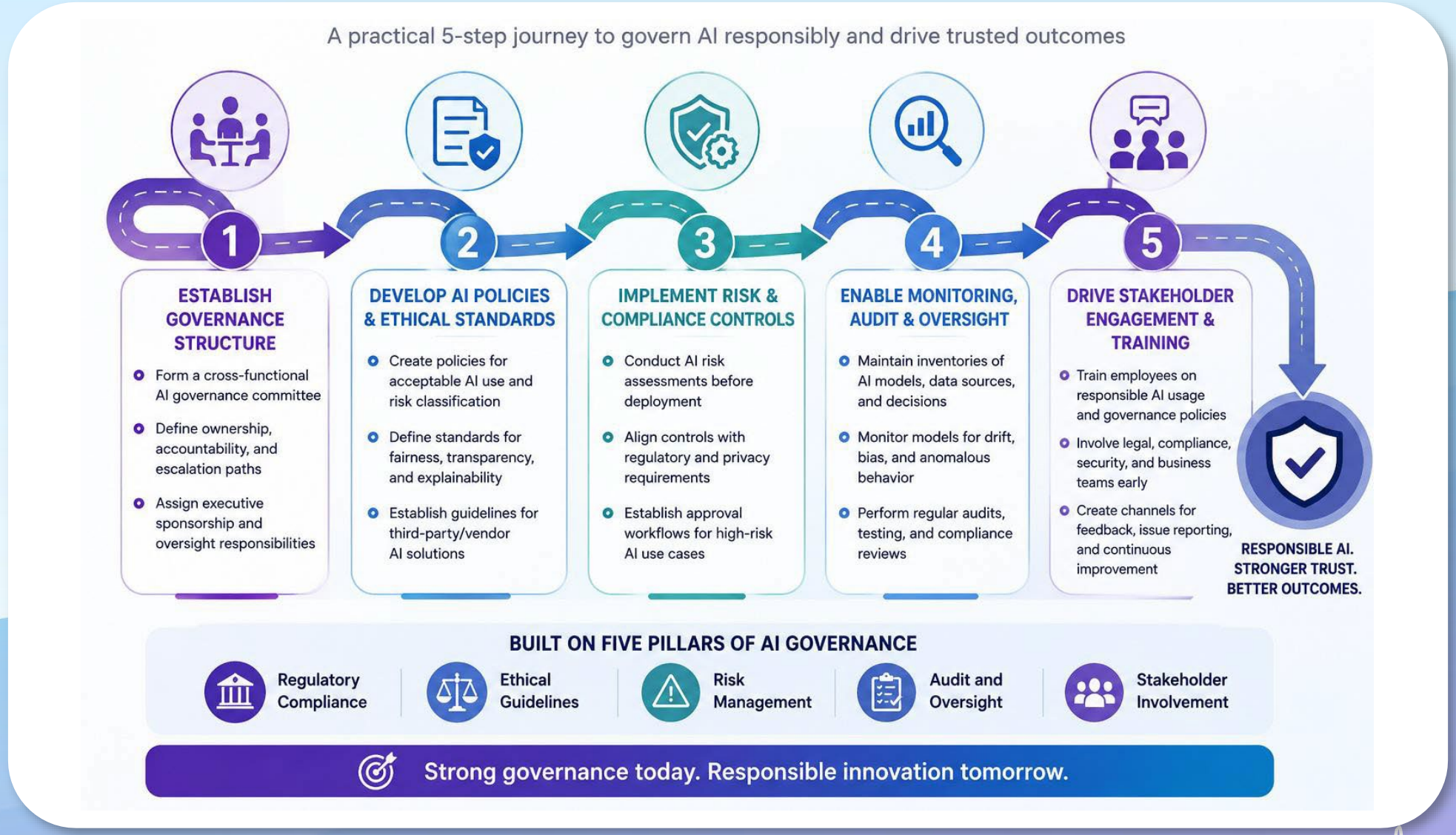


PRACTICAL STEPS FOR AI GOVERNANCE FRAMEWORK

Five key steps to operationalize responsible AI across your institution



YOUR ROADMAP TO AN AI GOVERNANCE FRAMEWORK



illuma



MCUL
MICHIGAN CREDIT UNION LEAGUE & AFFILIATES

YOUR TRUSTED PARTNERS FOR RESPONSIBLE AI ADOPTION



illuma

SHORTER CALLS • BETTER SECURITY • EASIER BANKING

info@illuma.cx

+1 (972) 217-7106