Emerging Use of Artificial Intelligence (AI) Technologies

CITY OF

SAN ANTONIO

— TEXAS —

Council B Session
15 May 2024

Craig Hopkins
Chief Information Officer/ IT Director

We should not treat AI as just a technology, or a business case. AI is shaping our society and **changing what it means to be human.**

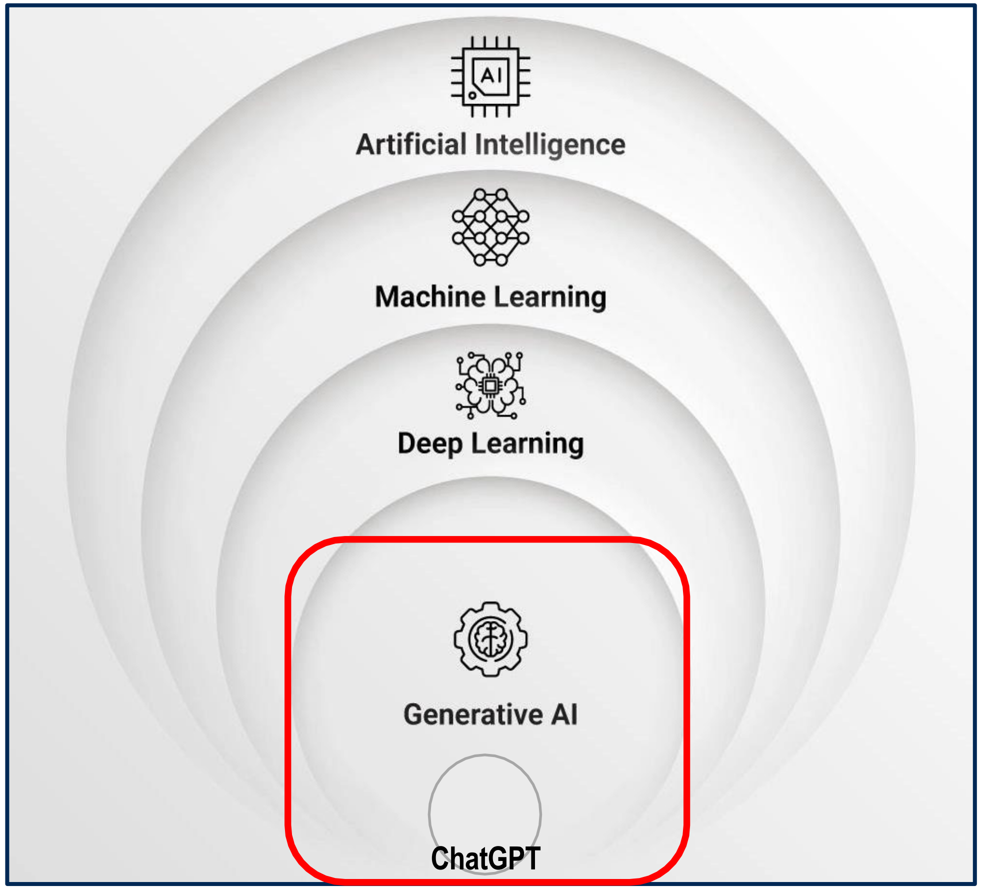
Agenda

- Definitions
- The Hype Cycle
- Potential Use Cases; Industry, COSA
- GenAI Concerns, Risks, Models
- It’s About the People
- “AI-Ready”; Security, Data, Principles
- Multi-Agency Collaboration
- COSA Policies, Standards, Roles
- Transformation Strategy

<u>Recognition</u>

- Gartner Research
- San Antonio Municipal Agency CIO Colleagues
- City of San Jose; GovAI Coalition
- National Institute of Standards and Technology (NIST)
- ITSD, HR, and Smart Cites Teams
- ChatGPT- OpenAI

Artificial Intelligence (AI) Defined



AI refers to systems or machines that ***mimic human intelligence*** to perform tasks and can iteratively improve themselves based on the information they collect.

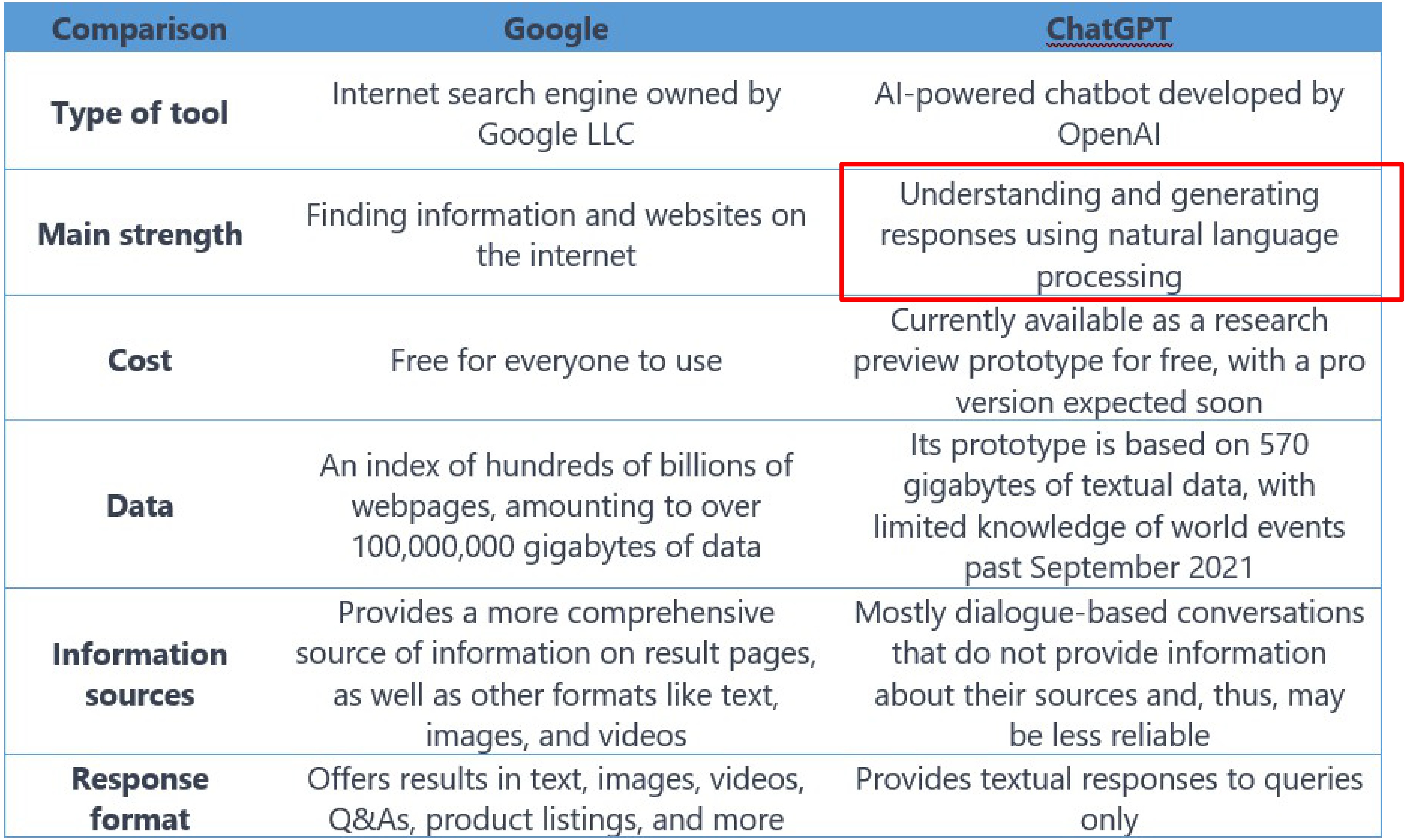
ML focuses on developing algorithms and models that ***enable computers to learn*** from and make predictions or decisions based on data, without explicit programming.

DL leverages deep neural networks for intricate pattern recognition.

GenAI focuses on ***creating or generating new content***, such as text, images, video, audio, or even code, through machine learning algorithms.

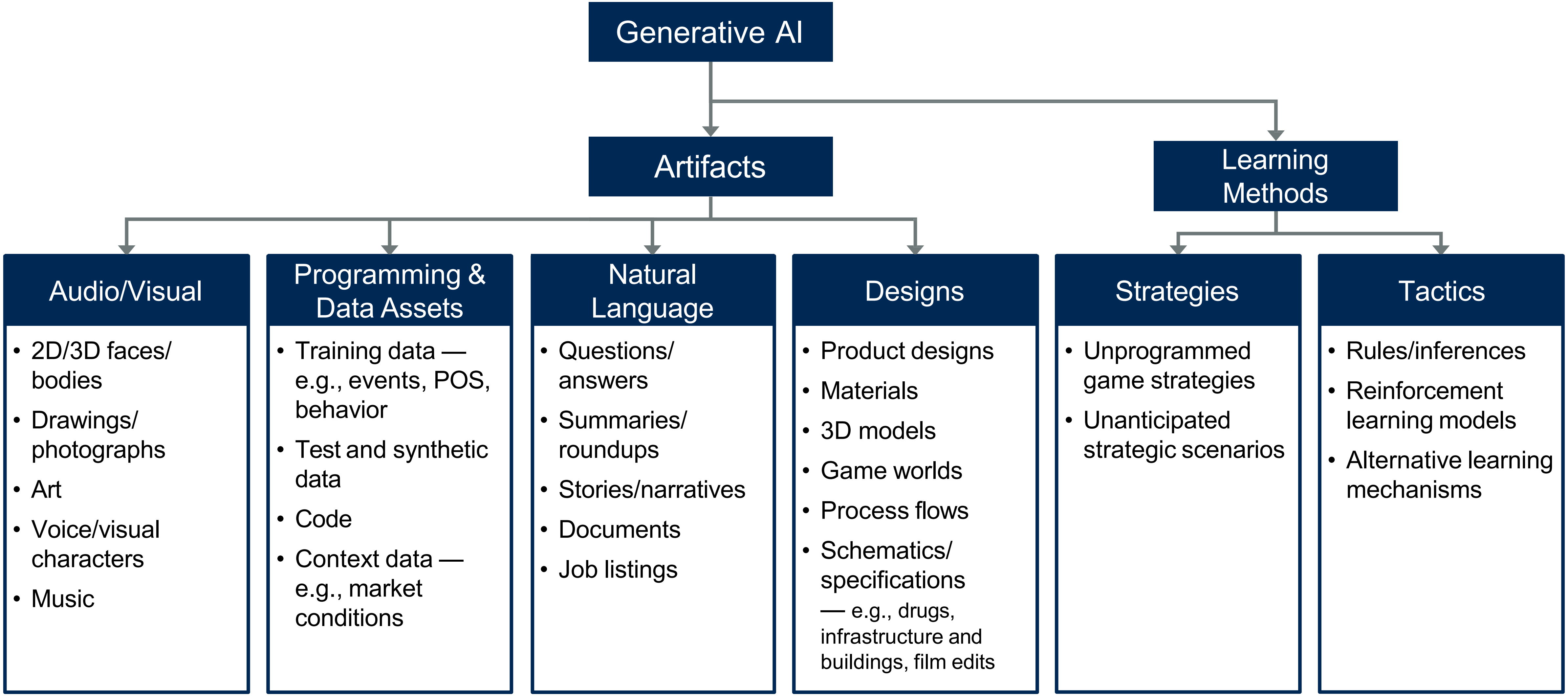
ChatGPT excels at natural language processing tasks, such as ***generating human-like text***, answering questions, and engaging in text-based conversations.

Google vs ChatGPT Today



Comparison	Google	ChatGPT
Type of tool	Internet search engine owned by Google LLC	AI-powered chatbot developed by OpenAI
Main strength	Finding information and websites on the internet	Understanding and generating responses using natural language processing
Cost	Free for everyone to use	Currently available as a research preview prototype for free, with a pro version expected soon
Data	An index of hundreds of billions of webpages, amounting to over 100,000,000 gigabytes of data	Its prototype is based on 570 gigabytes of textual data, with limited knowledge of world events past September 2021
Information sources	Provides a more comprehensive source of information on result pages, as well as other formats like text, images, and videos	Mostly dialogue-based conversations that do not provide information about their sources and, thus, may be less reliable
Response format	Offers results in text, images, videos, Q&As, product listings, and more	Provides textual responses to queries only

Business Artifacts That GenAI Can Generate Today



Generative AI

Artifacts

Learning Methods

Audio/Visual

- 2D/3D faces/ bodies
- Drawings/ photographs
- Art
- Voice/visual characters
- Music

Programming & Data Assets

- Training data — e.g., events, POS, behavior
- Test and synthetic data
- Code
- Context data — e.g., market conditions

Natural Language

- Questions/ answers
- Summaries/ roundups
- Stories/narratives
- Documents
- Job listings

Designs

- Product designs
- Materials
- 3D models
- Game worlds
- Process flows
- Schematics/ specifications — e.g., drugs, infrastructure and buildings, film edits

Strategies

- Unprogrammed game strategies
- Unanticipated strategic scenarios

Tactics

- Rules/inferences
- Reinforcement learning models
- Alternative learning mechanisms

RESTRICTED DISTRIBUTION

By 2025:

Generative AI will support authors, marketers and others in 50% of new content generation.

35% of large organizations will have named a **Chief AI Officer** reporting to a CEO or COO.

Possible Scenarios and Trajectories for GenAI

2024

40% of enterprise applications will have embedded conversational AI, up from less than 5% in 2020.

2025

30% of enterprises will have implemented an AI-augmented development and testing strategy, up from 5% in 2021.

2026

Generative design AI will automate **60%** of the design effort for new websites and mobile apps.

Over **100 million** humans will engage robocolleagues (synthetic virtual colleagues) to contribute to enterprise work.

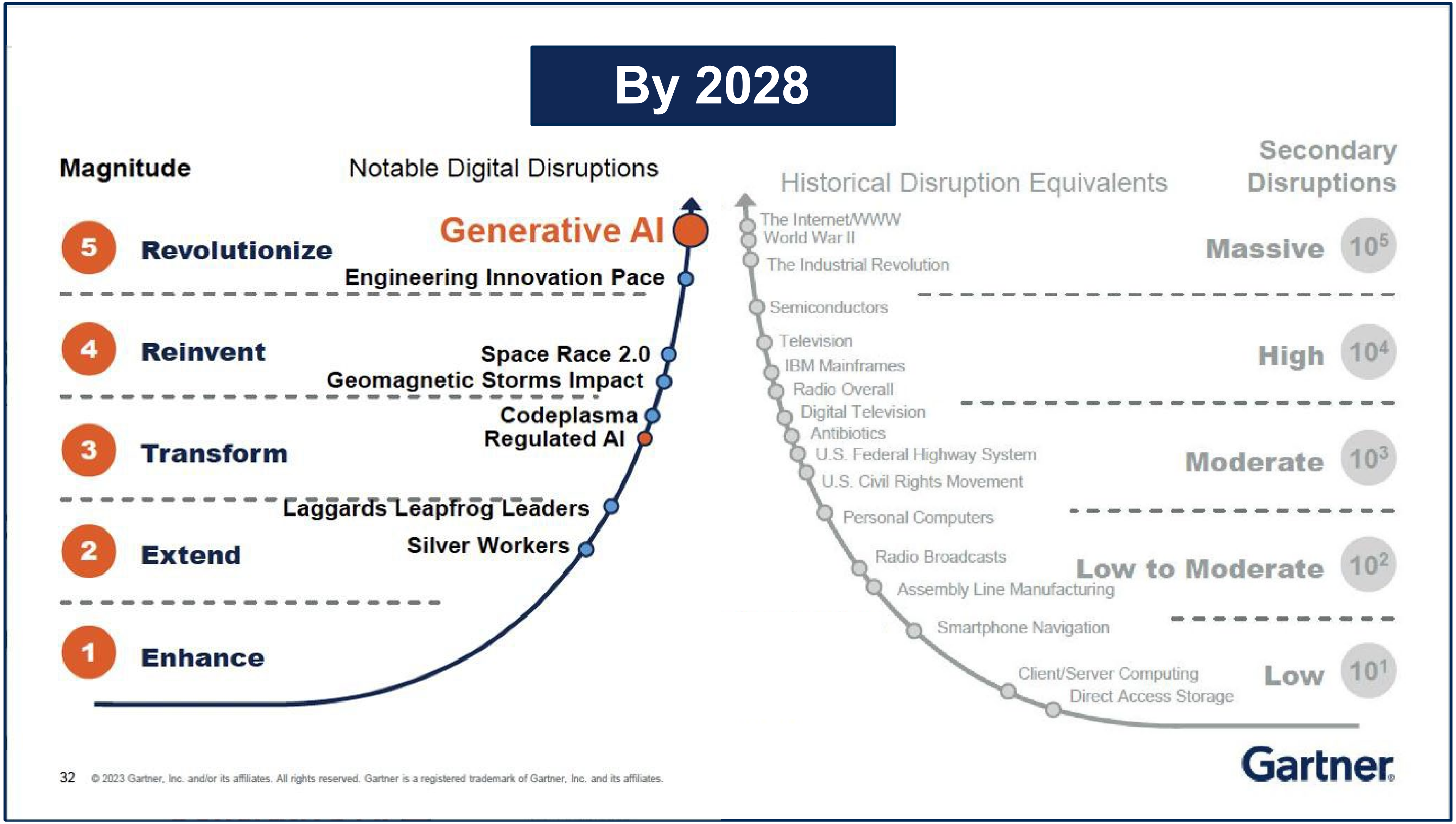
2027

By 2027, nearly **15%** of new applications will be automatically generated by AI without a human in the loop, up from 0% today.

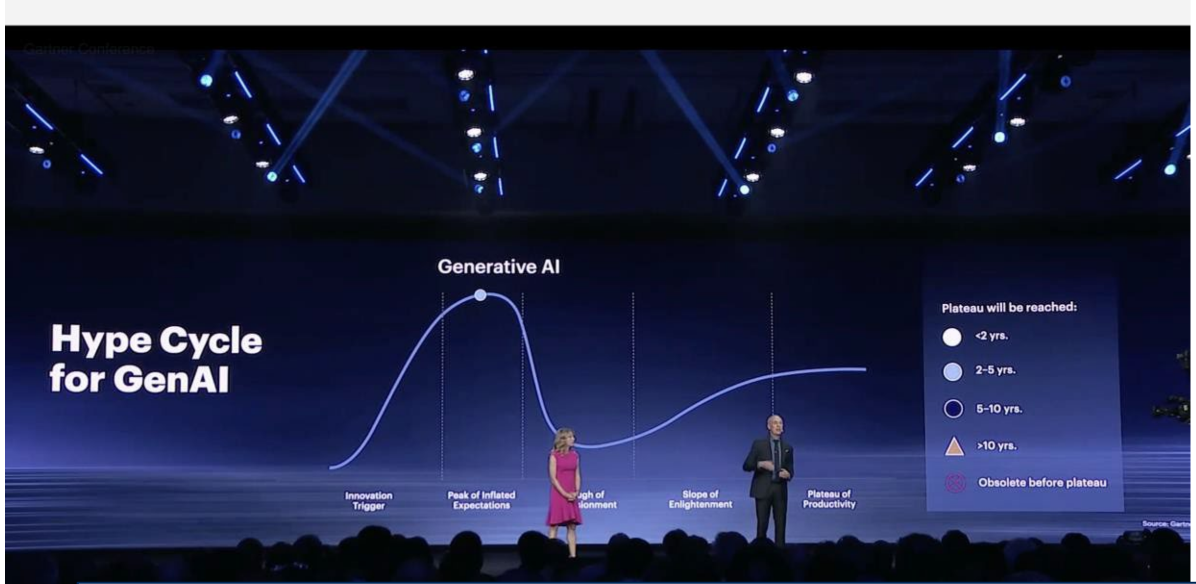
> ***"By 2030, 80% of humans will engage with smart robots on a daily basis."***

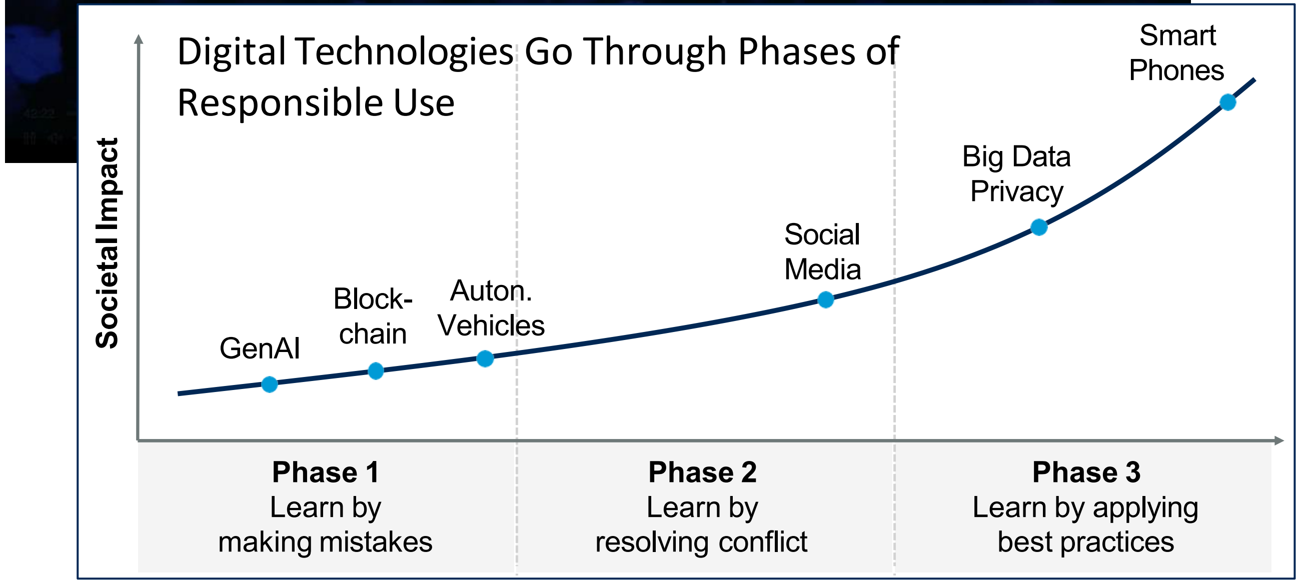
Source: Predicts 2022: Generative AI Is Poised to Revolutionize Digital Product Development 11 January 2022 - ID G00757883
By Brent Stewart, Van Baker, Joachim Herschmann

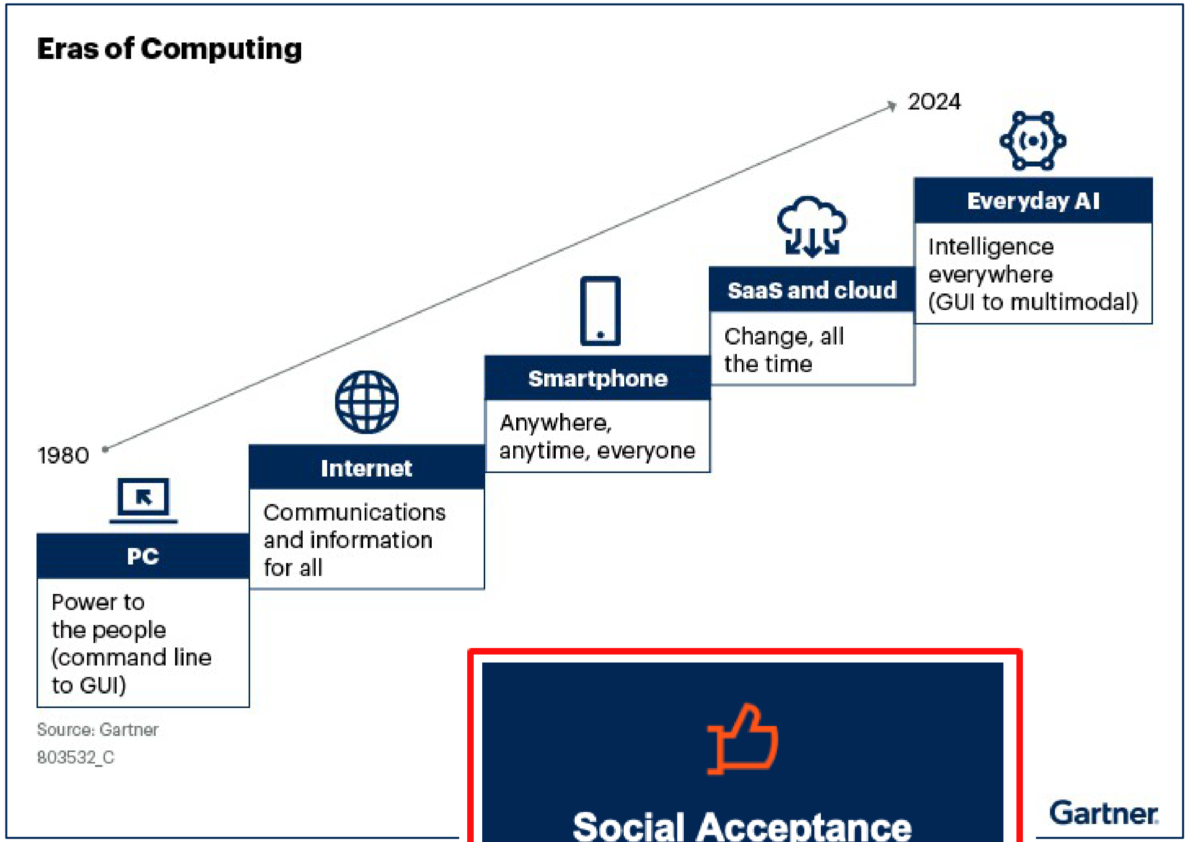
This is a Business Transformation, Not Technology



The Hype Cycle for GenAI







Eras of Computing

1980

2024

PC
Power to the people (command line to GUI)

Internet
Communications and information for all

Smartphone
Anywhere, anytime, everyone

SaaS and cloud
Change, all the time

Everyday AI
Intelligence everywhere (GUI to multimodal)

Source: Gartner
803532_C

Gartner

Social Acceptance

ChatGPT offers immediate benefit, with little effort.
It helps professionals write speeches, students write essays, and executives write strategies.

GenAI Opportunity Radar- Use Cases

Internal

Back Office

- Improving Productivity

Core Capabilities

- Enhancing Operational Efficiency

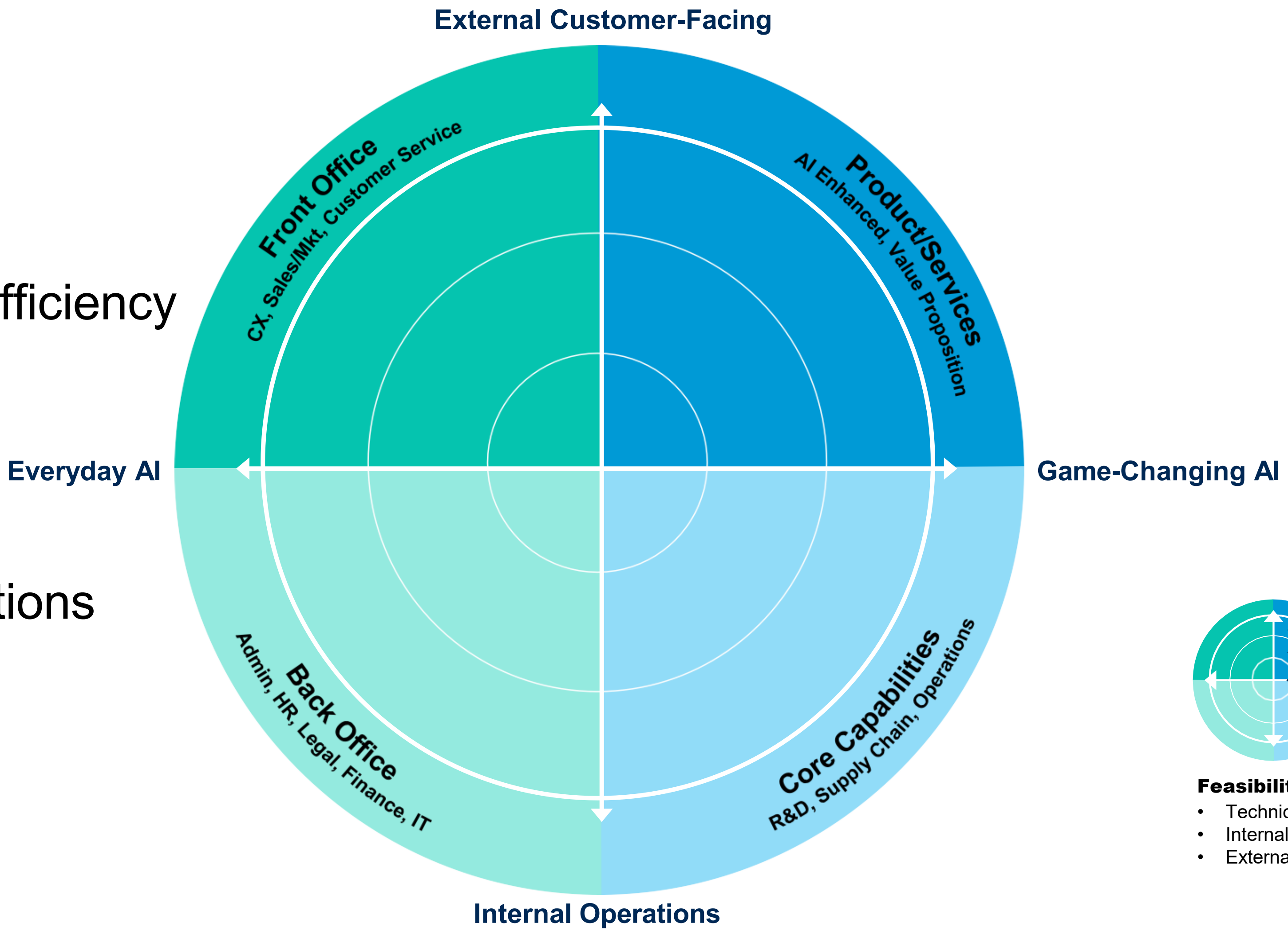
External Customer-Facing

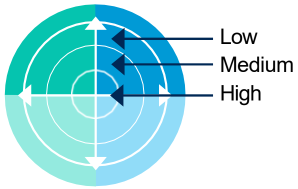
Front Office

- Resident-Centric Applications

New Products/Services

- Community Well-Being



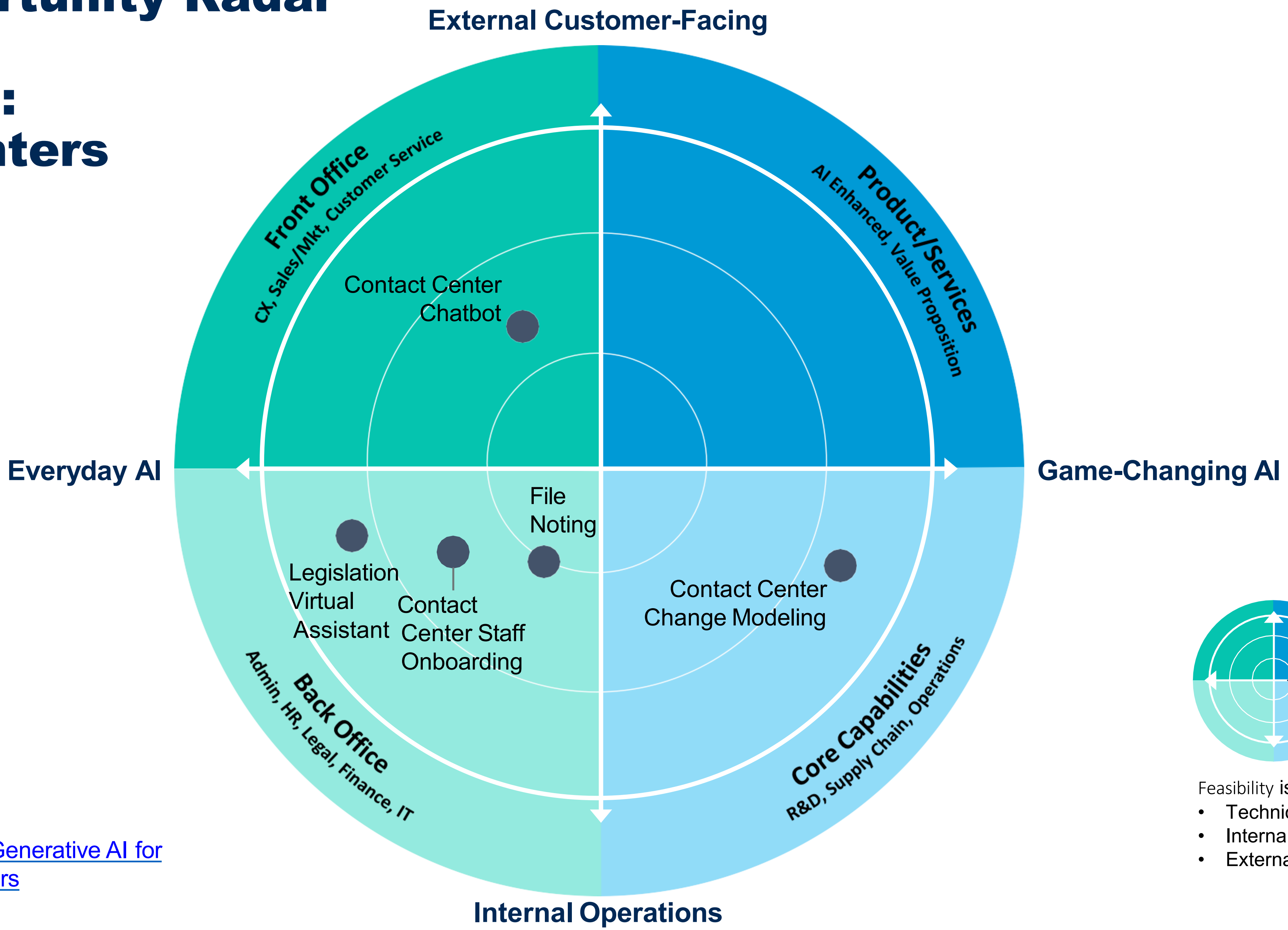


Feasibility is combination of

- Technical Feasibility
- Internal Readiness
- External Readiness

GenAI Opportunity Radar

Government: Contact Centers



External Customer-Facing

Everyday AI

Game-Changing AI

Internal Operations

Front Office
CX, Sales/Mkt, Customer Service

Product/Services
AI Enhanced, Value Proposition

Back Office
Admin, HR, Legal, Finance, IT

Core Capabilities
R&D, Supply Chain, Operations

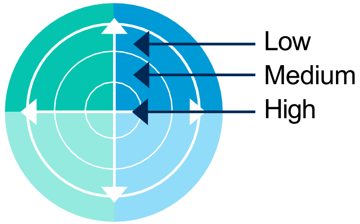
Contact Center Chatbot

File Noting

Legislation Virtual Assistant

Contact Center Staff Onboarding

Contact Center Change Modeling



Low

Medium

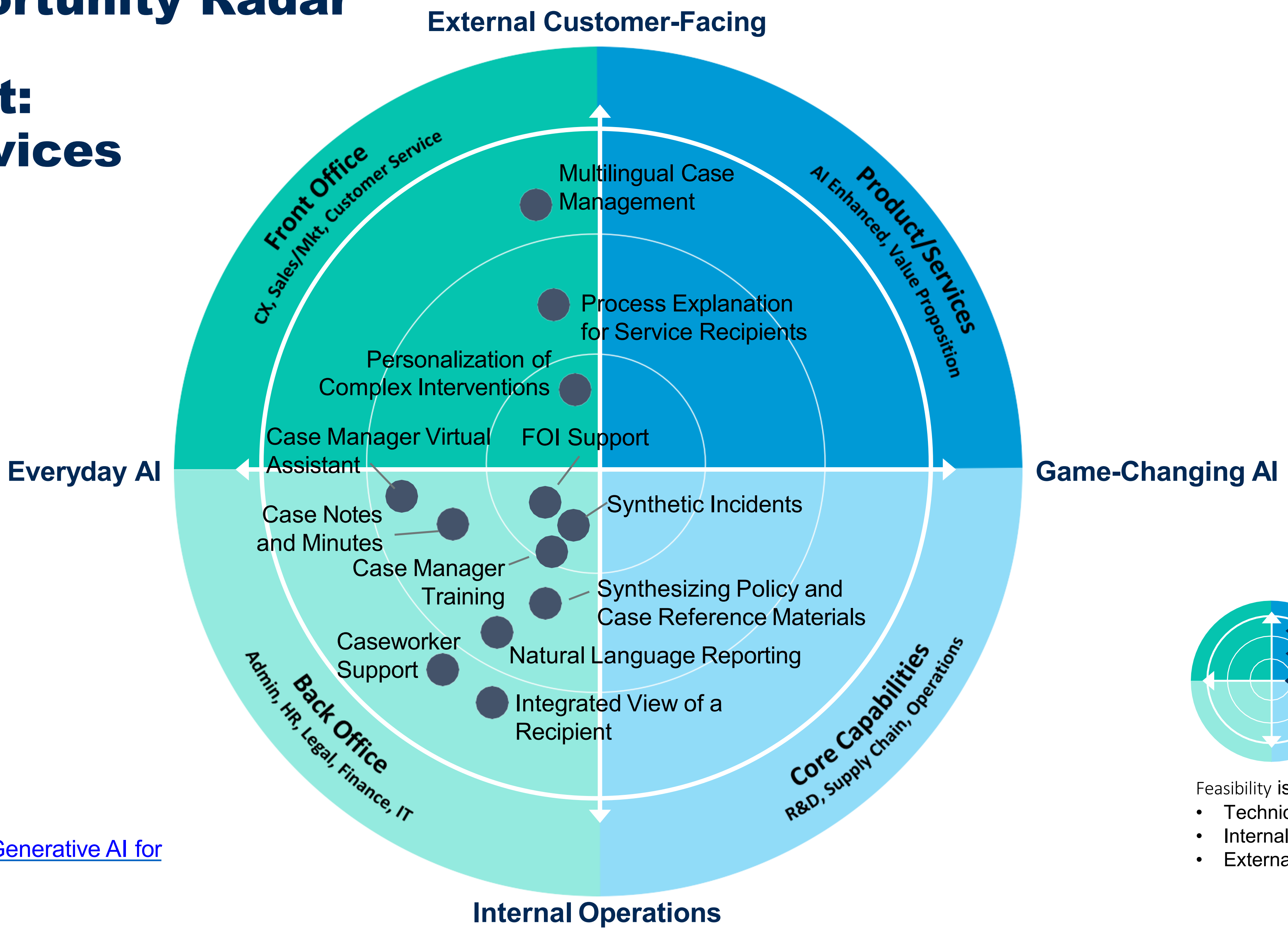
High

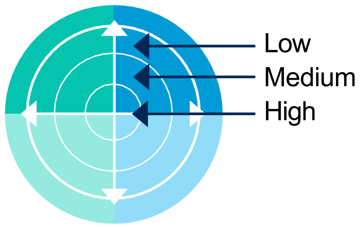
Feasibility is combination of
- Technical Feasibility
- Internal Readiness
- External Readiness

Source: [Use-Case Prism: Generative AI for Government Contact Centers]

GenAI Opportunity Radar

Government: Human Services


External Customer-Facing
Everyday AI
Game-Changing AI
Internal Operations
Front Office
CX, Sales/Mkt, Customer Service
Product/Services
AI Enhanced, Value Proposition
Back Office
Admin, HR, Legal, Finance, IT
Core Capabilities
R&D, Supply Chain, Operations
Multilingual Case Management
Process Explanation for Service Recipients
Personalization of Complex Interventions
Case Manager Virtual Assistant
FOI Support
Synthetic Incidents
Case Notes and Minutes
Case Manager Training
Synthesizing Policy and Case Reference Materials
Caseworker Support
Natural Language Reporting
Integrated View of a Recipient



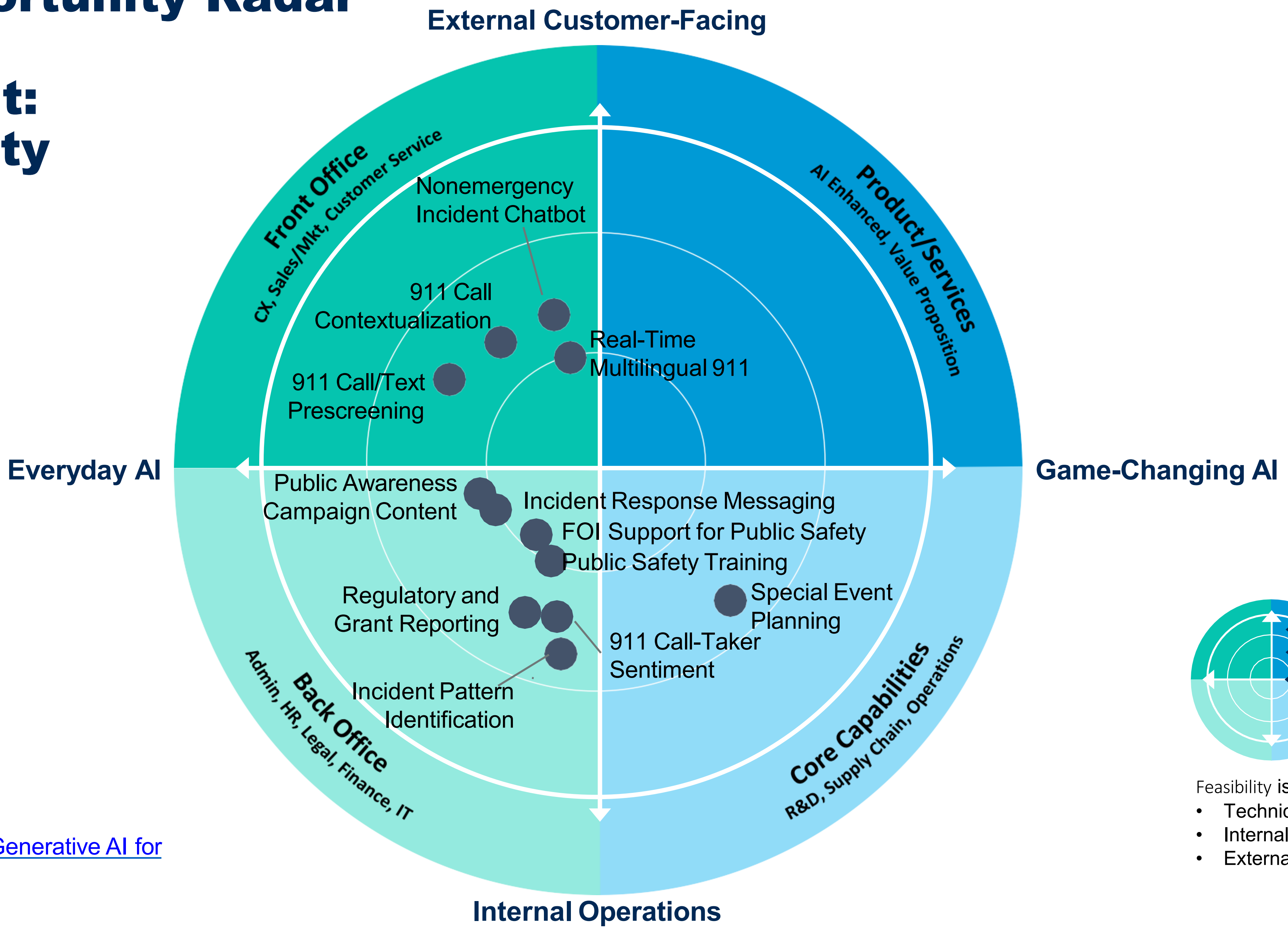
Feasibility is combination of

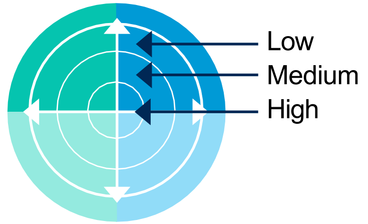
- Technical Feasibility
- Internal Readiness
- External Readiness

Source: Use-Case Prism: Generative AI for Human Services

GenAI Opportunity Radar

Government: Public Safety


External Customer-Facing
Everyday AI
Game-Changing AI
Internal Operations
Front Office
CX, Sales/Mkt, Customer Service
Product/Services
AI Enhanced, Value Proposition
Back Office
Admin, HR, Legal, Finance, IT
Core Capabilities
R&D, Supply Chain, Operations
Nonemergency Incident Chatbot
911 Call Contextualization
Real-Time Multilingual 911
911 Call/Text Prescreening
Public Awareness Campaign Content
Incident Response Messaging
FOI Support for Public Safety
Public Safety Training
Special Event Planning
Regulatory and Grant Reporting
911 Call-Taker Sentiment
Incident Pattern Identification



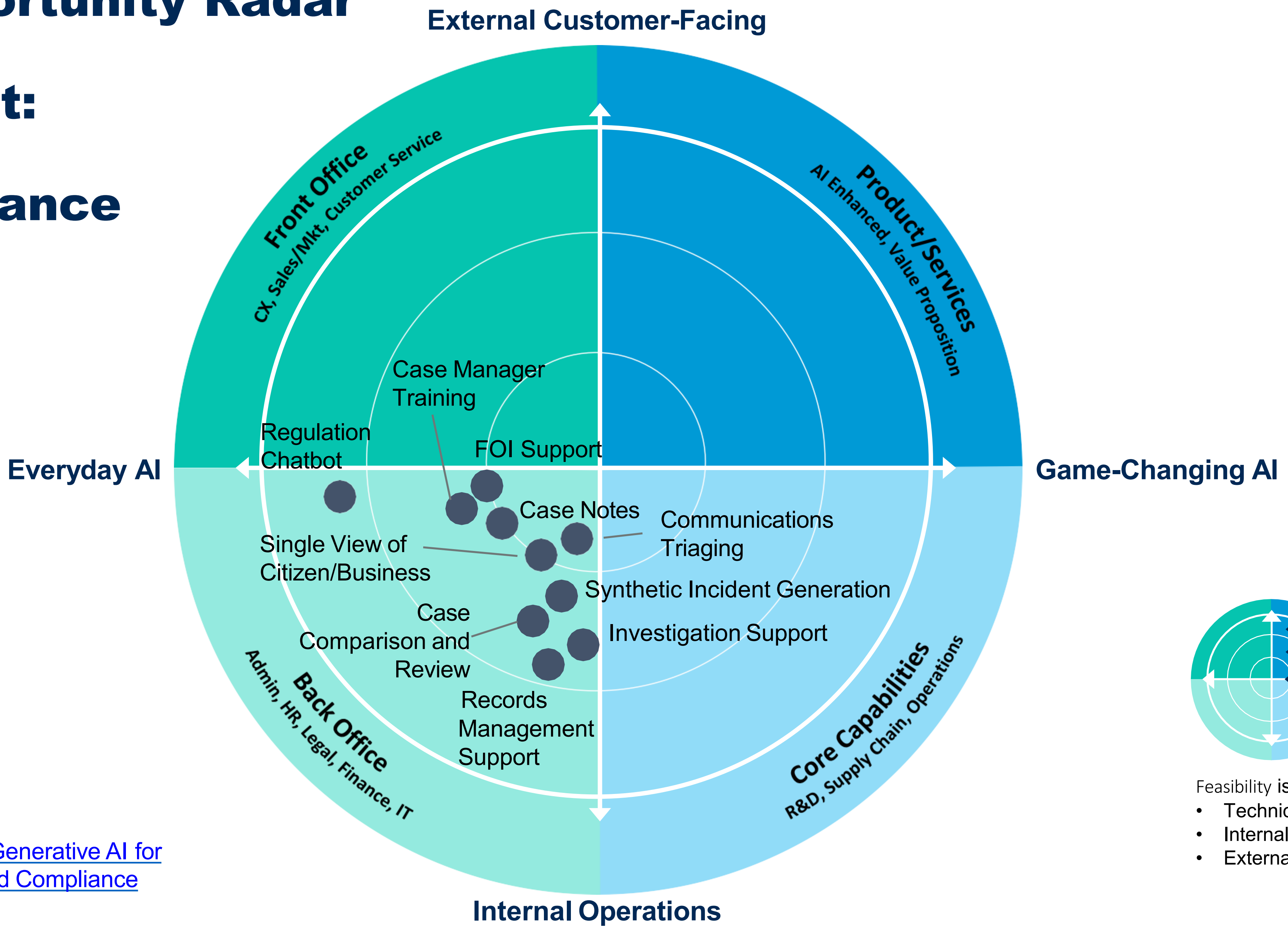
Feasibility is combination of

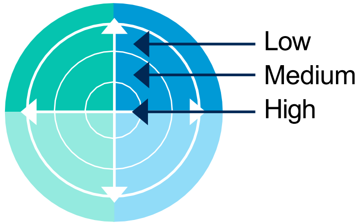
- Technical Feasibility
- Internal Readiness
- External Readiness

Source: Use-Case Prism: Generative AI for Public Safety

GenAI Opportunity Radar

Government: Regulatory and Compliance


External Customer-Facing
Front Office
CX, Sales/Mkt, Customer Service
Product/Services
AI Enhanced, Value Proposition
Everyday AI
Game-Changing AI
Back Office
Admin, HR, Legal, Finance, IT
Core Capabilities
R&D, Supply Chain, Operations
Internal Operations
Case Manager Training
Regulation Chatbot
FOI Support
Case Notes
Communications Triaging
Single View of Citizen/Business
Synthetic Incident Generation
Case Comparison and Review
Investigation Support
Records Management Support



Feasibility is combination of

- Technical Feasibility
- Internal Readiness
- External Readiness

Source: Use-Case Prism: Generative AI for Government Regulatory and Compliance

Real Use Cases Being Prototyped

From Peers at other Cities

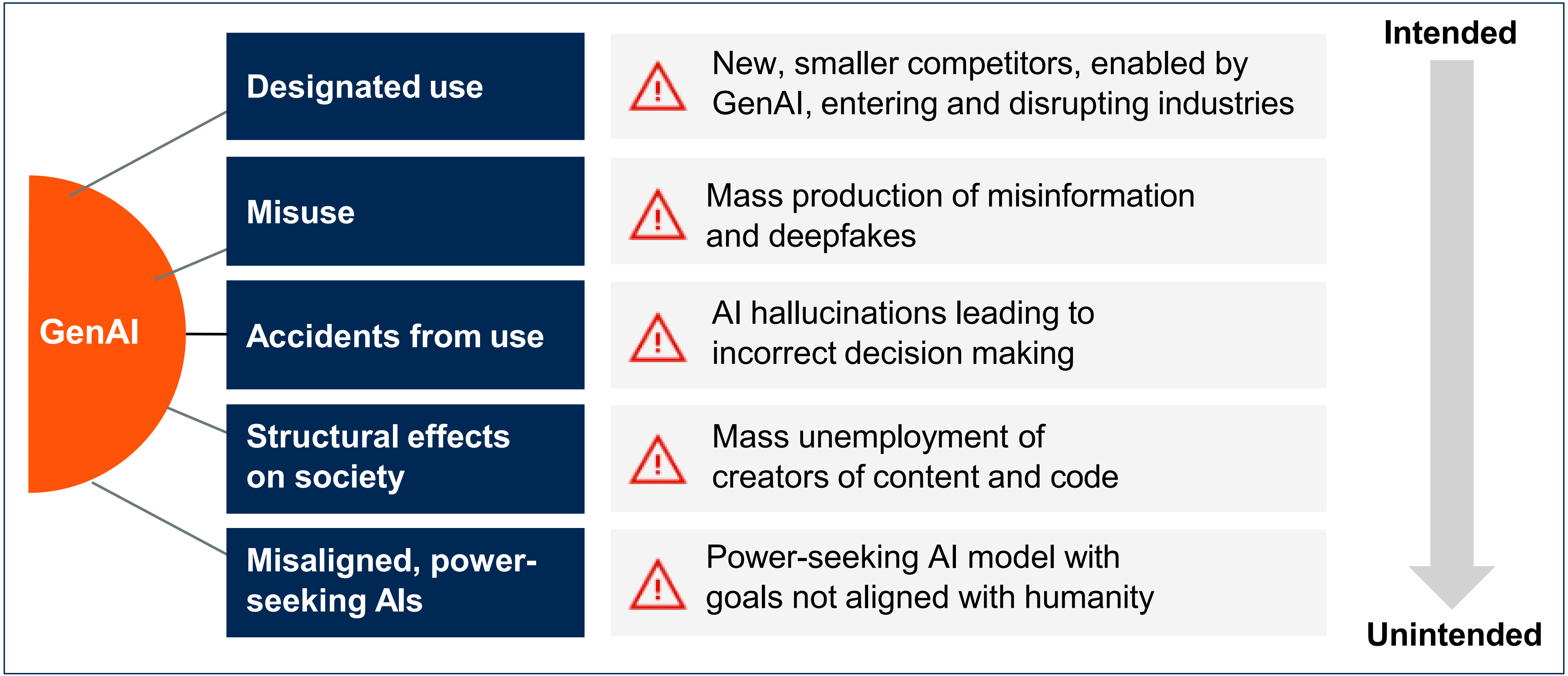
- **Bulk OCR** for environmental Health reports
- **Object detection** for road safety, graffiti, illegal dumping, lived-in vehicles/encampment, etc.
- **Capture meeting notes** in Zoom, Teams, Council meeting minutes
- **Chatbots for websites**
- **Translation services** to provide Spanish language
- **Automated sewer video** observations/inspections
- **Training software** for 911 dispatchers
- **Above ground inventory** for street and traffic infrastructure assets
- **Location intelligence** and customer visitation for economic development
- **Traffic signal** adaptive models
- **Sensor leak detection** for our water utilities

What are We Doing?

- **Talkin' Broadway-** chatbot information about bond construction on lower Broadway Corridor.
- **Language Translation** Town hall and community meetings as well as resident facing digital communications.
- **One City Chat-** chatbot across multiple San Antonio public agencies for resident inquiries. (Azure AI)
- **LiDAR Sensing-** computer vision to classify roadway usage including pedestrians, vehicles, and bicycles.
- **Contract Intelligence-** customized information about contracts to users across the procurement workflow.
- **Microsoft CoPilot-** included in MS Office 365 government cloud. (Summer 2024)
- **COSA Virtual Assistant-** employees can ask questions about employee benefits, leave, HR policies, etc.
- **SWMD Safety-** a digital event recorder that detects distracted or risky driving behavior.
- **COSA IT Held Service Desk-** users can request technical help from ITSD directly in an AI chatbot.

Generative AI Creates Many Kinds of Risks

Should CIO's Allow the Use of Generative AI at Work?



GenAI

Intended

Unintended

- **Designated use** — ⚠ New, smaller competitors, enabled by GenAI, entering and disrupting industries
- **Misuse** — ⚠ Mass production of misinformation and deepfakes
- **Accidents from use** — ⚠ AI hallucinations leading to incorrect decision making
- **Structural effects on society** — ⚠ Mass unemployment of creators of content and code
- **Misaligned, power-seeking AIs** — ⚠ Power-seeking AI model with goals not aligned with humanity

Source: Gartner

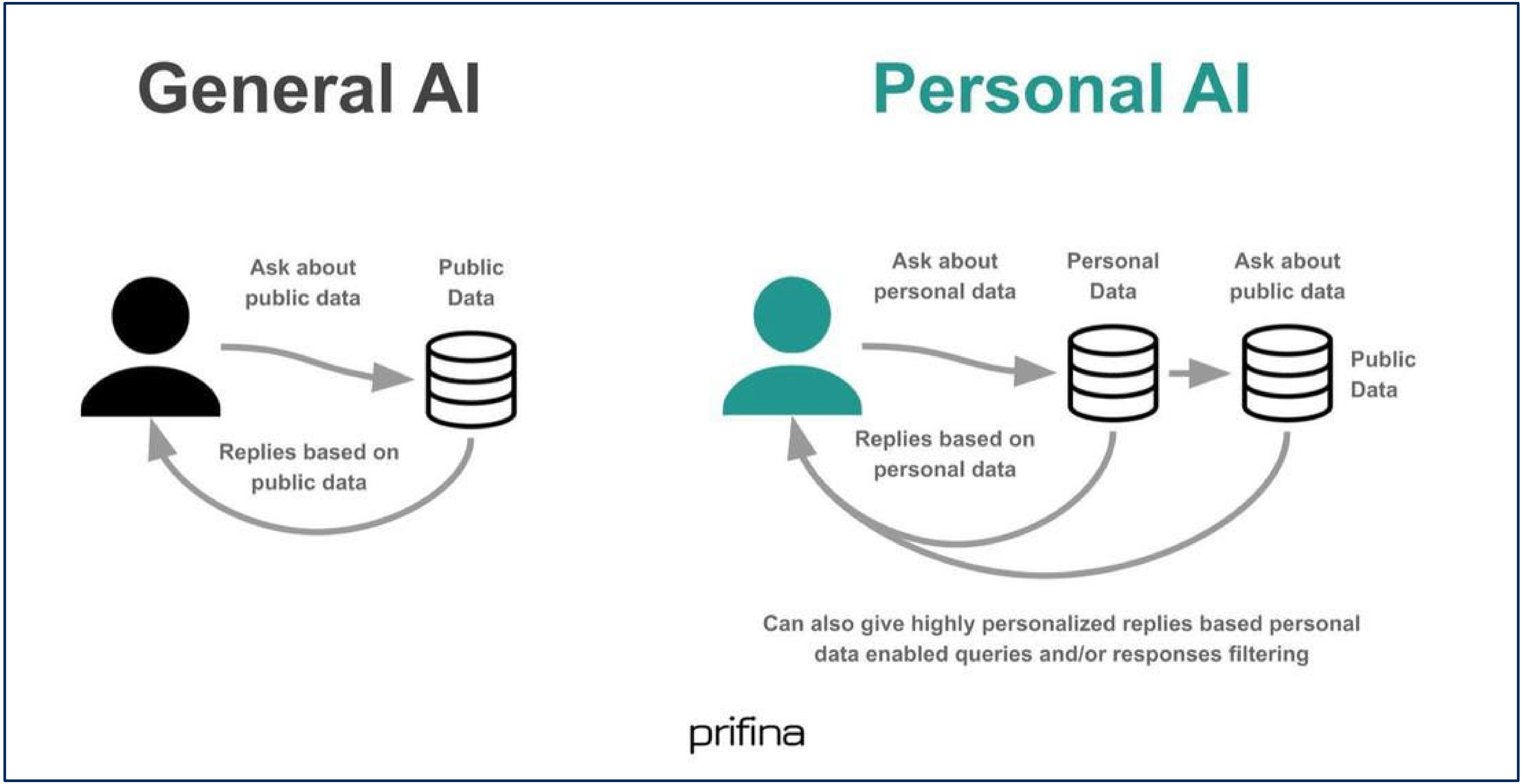
ChatGPT Real Risks Today

> **“Ethical decisions masquerade as IT decisions all the time.”**

Intellectual Property	Data Privacy	Cyber Concerns
• Information entered into ChatGPT can become part of its training set. • Any proprietary, sensitive or confidential information entered as prompts could be used in outputs for other users. • Amazon warned employees against ChatGPT when it generated code similar to internal Amazon code.[1]	• OpenAI may share ChatGPT user information with third parties without prior notice.[2] • These third parties may include vendors or service providers, affiliates, and other users. • However, it is possible to request OpenAI to delete your data.	• Personal or sensitive information stored by OpenAI could be accessed by hackers. • Hackers can also use “prompt injection,” or use prompts that can manipulate ChatGPT to give away information it shouldn’t.[3] • ChatGPT can also be tricked into writing malware or ransomware codes.

Source: [1] Amazon Warns Employees to Beware of ChatGPT, Gizmodo; [2] Privacy Policy, OpenAI; [3] Microsoft’s Bing Chatbot AI Is Susceptible to Several Types of “Prompt Injection” Attacks, TechSpot

Public vs Private Models



Can also give highly personalized replies based personal data enabled queries and/or responses filtering

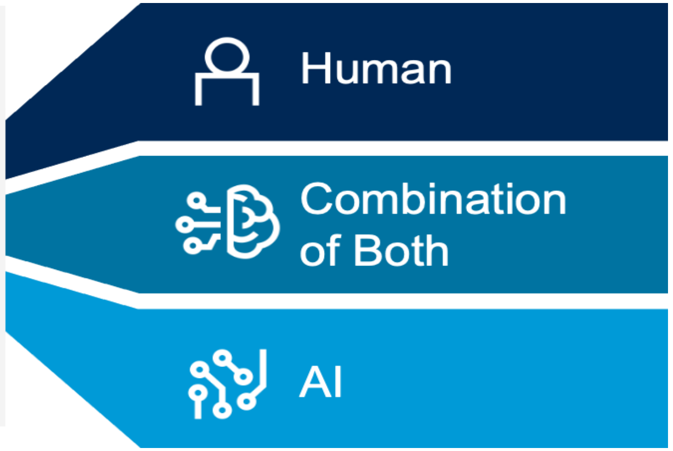
Even in an AI World, It’s All About the People

By 2025:

“80% of the workforce will be able to eliminate 10% of their tasks”

“20% of the workforce will be able to eliminate 50% of their tasks”

Gartner predicts that every knowledge job will be scrutinized and separated into **individual activities and tasks**.

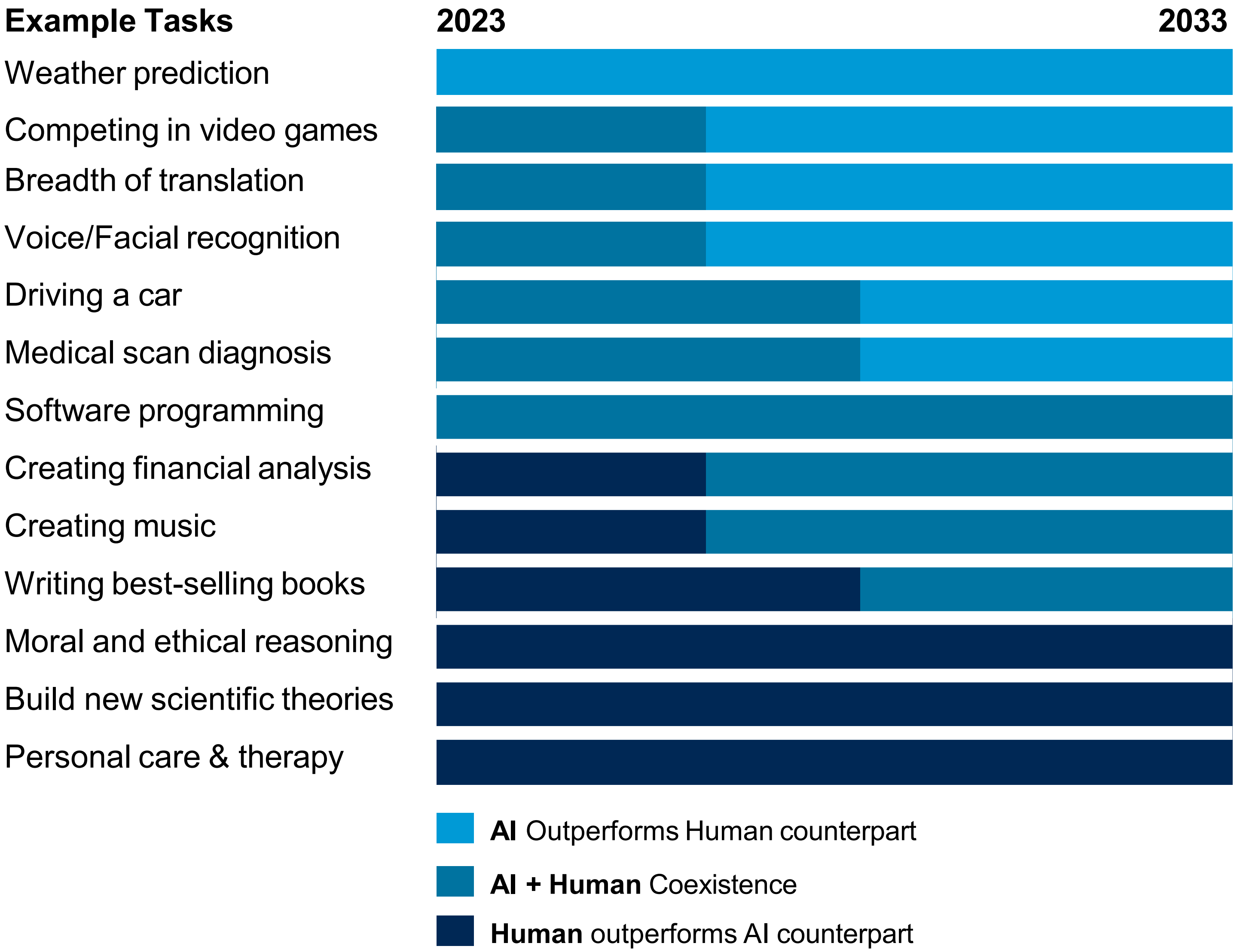


The most common impact for the next decade will **not** be the **replacement of workers**. It will be the **augmentation of jobs** with AI.

Democratization of Work and Redistribution of Workload

Source: Gartner

AI Outperforms People in Some Tasks, but Not All



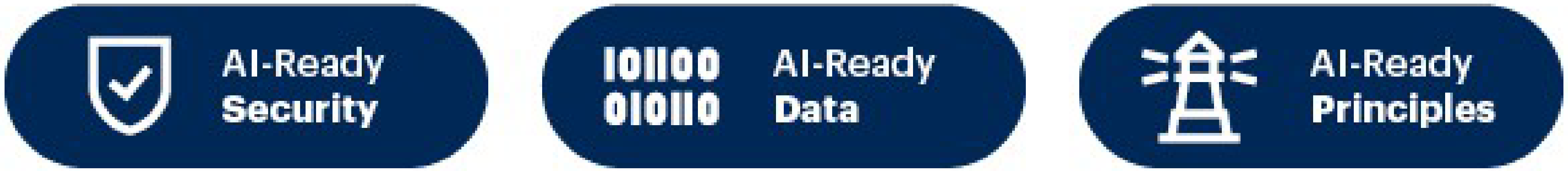
By 2026

Despite all the advancements in AI, the global **jobs impact will be neutral-** there will not be net decrease or increase.

More than **100 million** people will engage **robocolleagues** (synthetic virtual colleagues) to contribute to enterprise work.

What Can We Do to Become “AI-Ready”

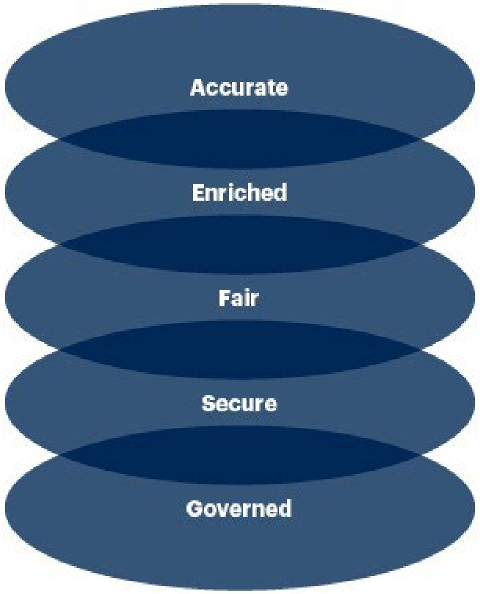
Establish Three Pillars to Become AI-Ready



Source: Gartner
799922_C

“If your data isn’t ready for AI, you’re not ready for AI.”

Five Criteria for AI-Ready Data

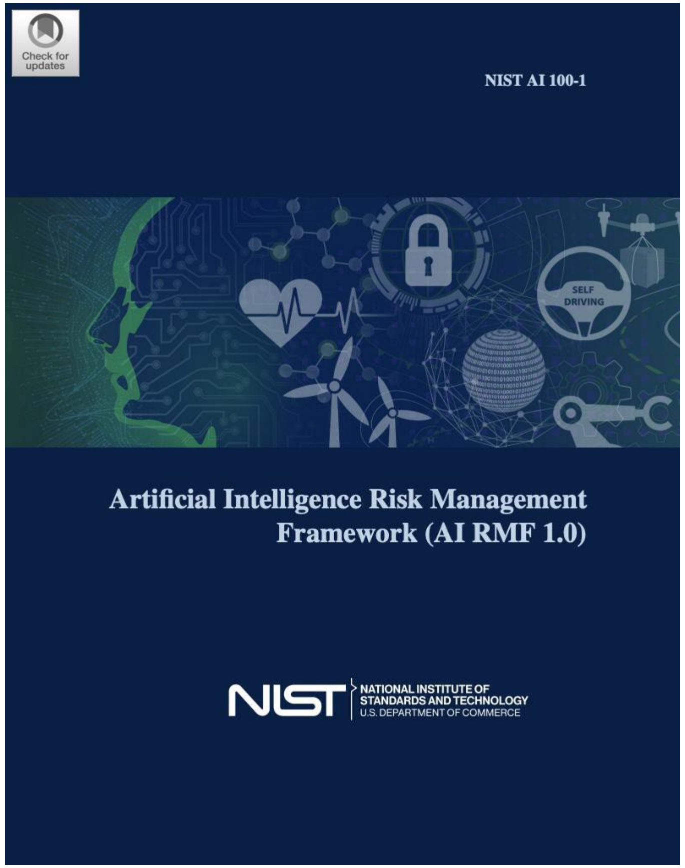


Source: Gartner
799922_C

Data + Rules + Tags

Risk Management Framework

NIST AI 100-1 is a set of standards and practices developed by the National Institute of Standards and Technology (NIST) for evaluating, maintaining, and improving the trustworthiness of AI systems

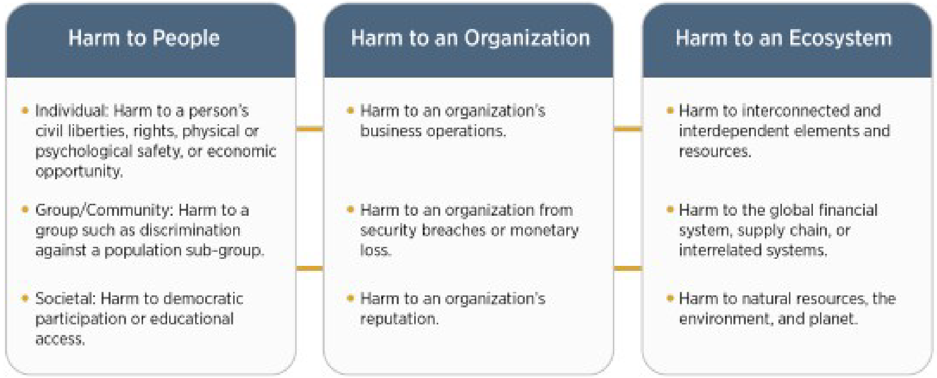


Check for updates

NIST AI 100-1

Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE



Harm to People

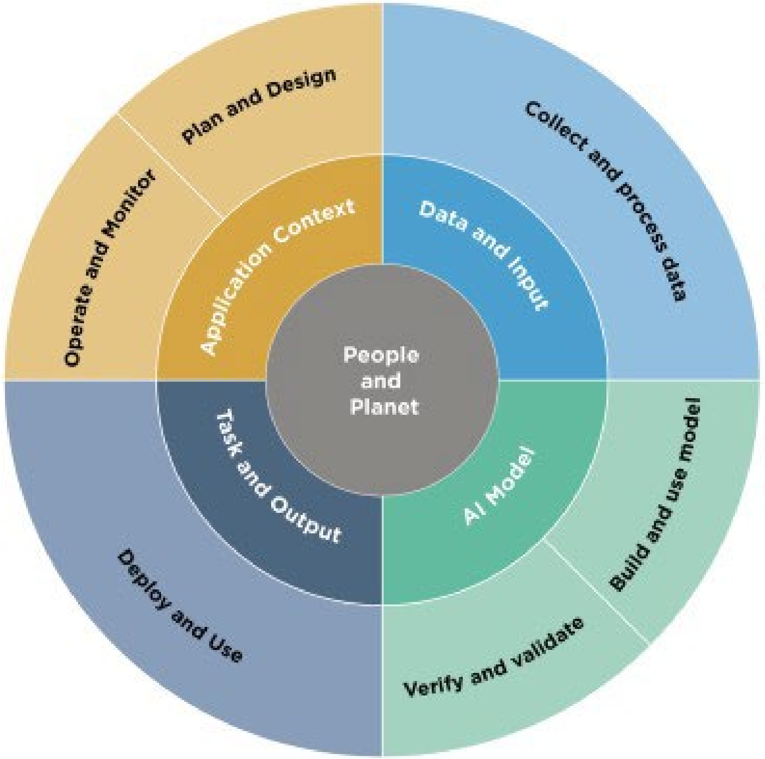
- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.



Industry Guiding Principles

Human-Centered Design

Developed and deployed so that AI powered services are elevated for their impact on the public.

Privacy

Preserved by safeguarding (PII) and sensitive data from unauthorized access, disclosure, and manipulation.

Equity

Systems support equitable outcomes for everyone. Bias is effectively managed with the intention of reducing harm.

Effectiveness

Systems are reliable, meet objectives, and deliver precise and dependable outcomes for which they are deployed.

Security and Safety

Systems maintain confidentiality, integrity, and availability through safeguards that prevent unauthorized access/use.

Transparency

Purpose and use is proactively communicated, understandable, documented, and disclosed to the public.

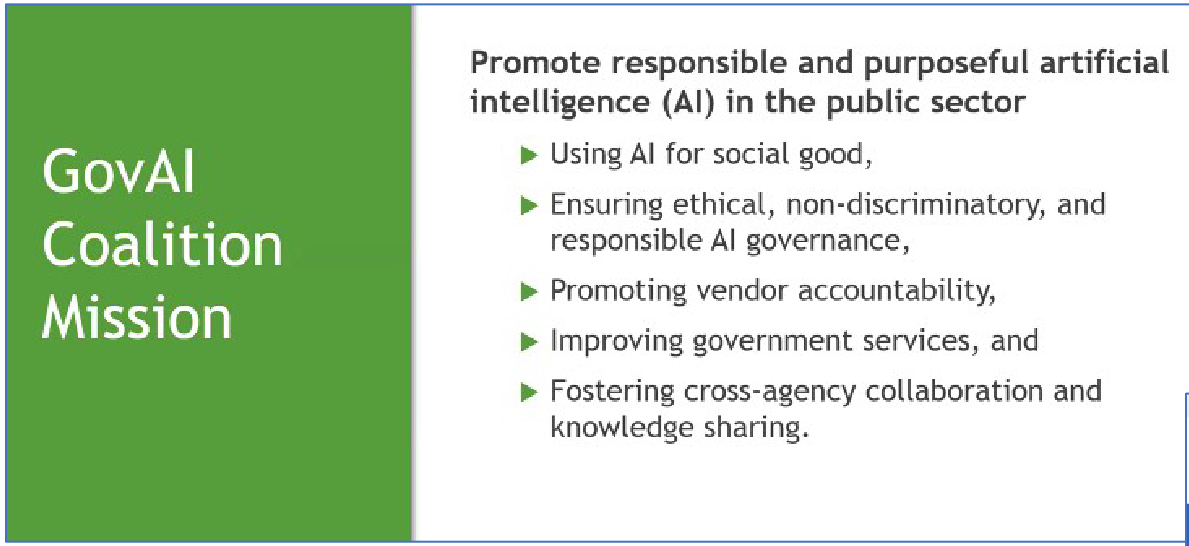
Accountability

Govern deployment, maintenance and human oversight ensures adherence to relevant laws and regulations.

Workforce Empowerment

Staff use AI in their roles; education, training, collaboration that promote participation and opportunity.

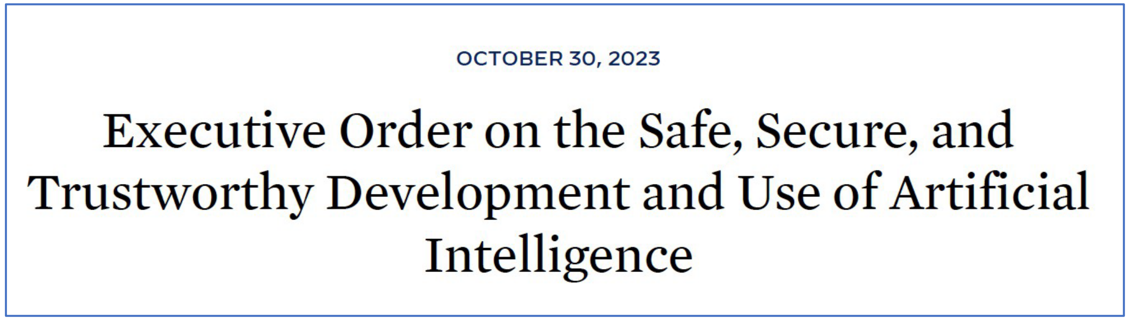
Agency Collaboration



GovAI Coalition Mission

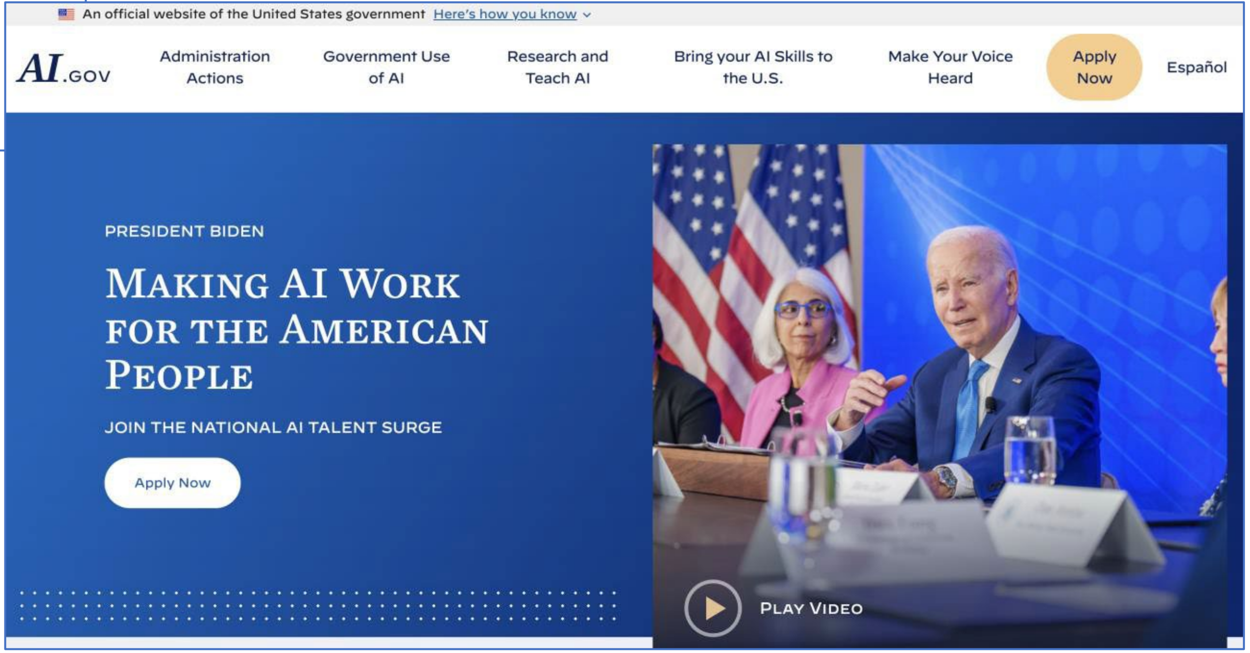
Promote responsible and purposeful artificial intelligence (AI) in the public sector

- Using AI for social good,
- Ensuring ethical, non-discriminatory, and responsible AI governance,
- Promoting vendor accountability,
- Improving government services, and
- Fostering cross-agency collaboration and knowledge sharing.



OCTOBER 30, 2023

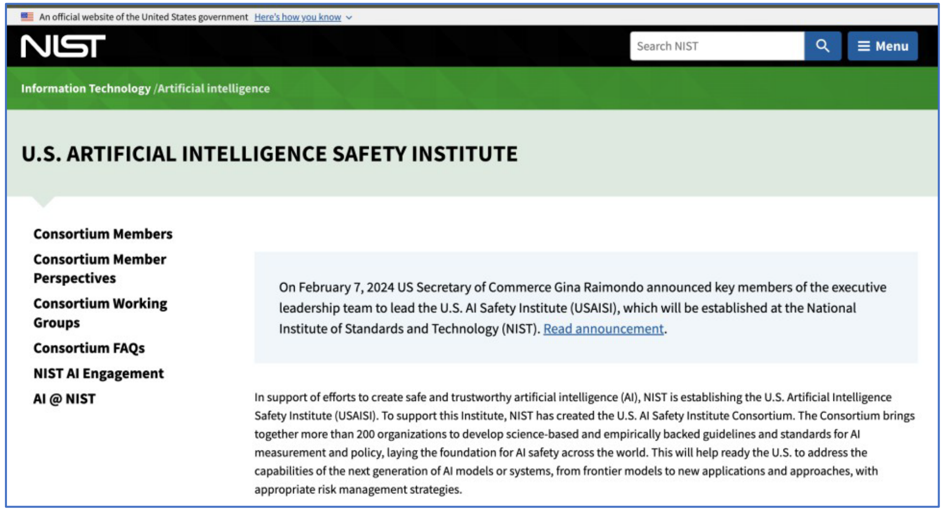
Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence



PRESIDENT BIDEN

MAKING AI WORK FOR THE AMERICAN PEOPLE

JOIN THE NATIONAL AI TALENT SURGE



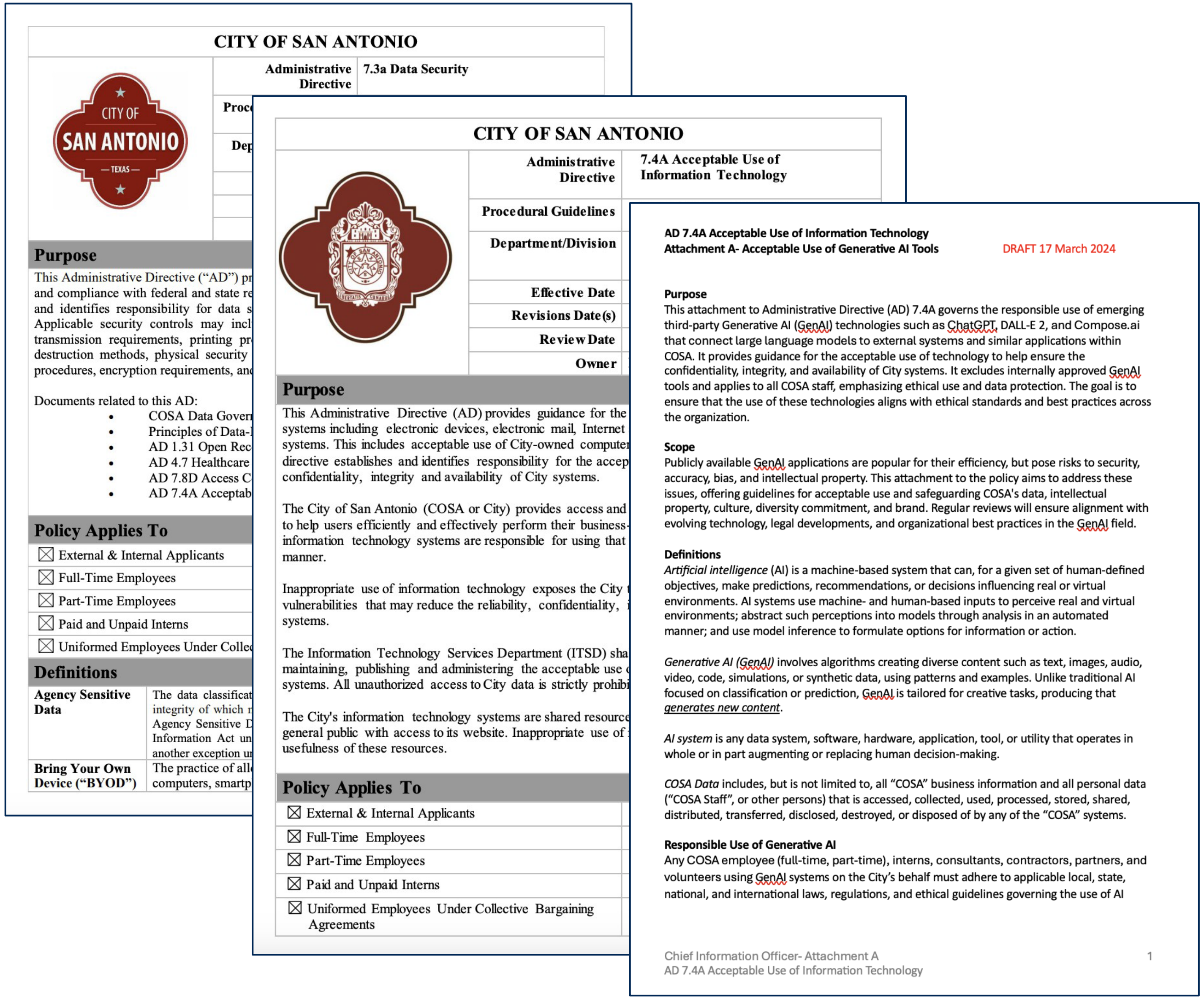
An official website of the United States government Here's how you know
NIST
Search NIST
Menu
Information Technology /Artificial intelligence
Consortium Members
Consortium Member Perspectives
Consortium Working Groups
Consortium FAQs
NIST AI Engagement
AI @ NIST

U.S. ARTIFICIAL INTELLIGENCE SAFETY INSTITUTE

On February 7, 2024 US Secretary of Commerce Gina Raimondo announced key members of the executive leadership team to lead the U.S. AI Safety Institute (USAISI), which will be established at the National Institute of Standards and Technology (NIST). Read announcement.

In support of efforts to create safe and trustworthy artificial intelligence (AI), NIST is establishing the U.S. Artificial Intelligence Safety Institute (USAISI). To support this Institute, NIST has created the U.S. AI Safety Institute Consortium. The Consortium brings together more than 200 organizations to develop science-based and empirically backed guidelines and standards for AI measurement and policy, laying the foundation for AI safety across the world. This will help ready the U.S. to address the capabilities of the next generation of AI models or systems, from frontier models to new applications and approaches, with appropriate risk management strategies.

COSA Policies and Standards



CITY OF SAN ANTONIO

Administrative Directive	7.3a Data Security
Proc	
Dep	

Purpose

This Administrative Directive ("AD") pr
and compliance with federal and state re
and identifies responsibility for data s
Applicable security controls may incl
transmission requirements, printing pr
destruction methods, physical security
procedures, encryption requirements, an

Documents related to this AD:

- COSA Data Gover
- Principles of Data-
- AD 1.31 Open Rec
- AD 4.7 Healthcare
- AD 7.8D Access C
- AD 7.4A Acceptab

Policy Applies To

☒ External & Internal Applicants
☒ Full-Time Employees
☒ Part-Time Employees
☒ Paid and Unpaid Interns
☒ Uniformed Employees Under Collec

Definitions

Agency Sensitive Data	The data classificat integrity of which r Agency Sensitive D Information Act un another exception u
Bring Your Own Device ("BYOD")	The practice of all computers, smartp

CITY OF SAN ANTONIO

Administrative Directive	7.4A Acceptable Use of Information Technology
Procedural Guidelines	
Department/Division	
Effective Date	
Revisions Date(s)	
Review Date	
Owner	

Purpose

This Administrative Directive (AD) provides guidance for the
systems including electronic devices, electronic mail, Internet
systems. This includes acceptable use of City-owned computer
directive establishes and identifies responsibility for the accep
confidentiality, integrity and availability of City systems.

The City of San Antonio (COSA or City) provides access and
to help users efficiently and effectively perform their business
information technology systems are responsible for using that
manner.

Inappropriate use of information technology exposes the City
vulnerabilities that may reduce the reliability, confidentiality,
systems.

The Information Technology Services Department (ITSD) sha
maintaining, publishing and administering the acceptable use
systems. All unauthorized access to City data is strictly prohibi

The City's information technology systems are shared resource
general public with access to its website. Inappropriate use of
usefulness of these resources.

Policy Applies To

☒ External & Internal Applicants
☒ Full-Time Employees
☒ Part-Time Employees
☒ Paid and Unpaid Interns
☒ Uniformed Employees Under Collective Bargaining Agreements

AD 7.4A Acceptable Use of Information Technology
Attachment A- Acceptable Use of Generative AI Tools DRAFT 17 March 2024

Purpose
This attachment to Administrative Directive (AD) 7.4A governs the responsible use of emerging third-party Generative AI (GenAI) technologies such as ChatGPT, DALL-E 2, and Compose.ai that connect large language models to external systems and similar applications within COSA. It provides guidance for the acceptable use of technology to help ensure the confidentiality, integrity, and availability of City systems. It excludes internally approved GenAI tools and applies to all COSA staff, emphasizing ethical use and data protection. The goal is to ensure that the use of these technologies aligns with ethical standards and best practices across the organization.

Scope
Publicly available GenAI applications are popular for their efficiency, but pose risks to security, accuracy, bias, and intellectual property. This attachment to the policy aims to address these issues, offering guidelines for acceptable use and safeguarding COSA's data, intellectual property, culture, diversity commitment, and brand. Regular reviews will ensure alignment with evolving technology, legal developments, and organizational best practices in the GenAI field.

Definitions
Artificial intelligence (AI) is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments. AI systems use machine- and human-based inputs to perceive real and virtual environments; abstract such perceptions into models through analysis in an automated manner; and use model inference to formulate options for information or action.

Generative AI (GenAI) involves algorithms creating diverse content such as text, images, audio, video, code, simulations, or synthetic data, using patterns and examples. Unlike traditional AI focused on classification or prediction, GenAI is tailored for creative tasks, producing that *generates new content*.

AI system is any data system, software, hardware, application, tool, or utility that operates in whole or in part augmenting or replacing human decision-making.

COSA Data includes, but is not limited to, all "COSA" business information and all personal data ("COSA Staff", or other persons) that is accessed, collected, used, processed, stored, shared, distributed, transferred, disclosed, destroyed, or disposed of by any of the "COSA" systems.

Responsible Use of Generative AI
Any COSA employee (full-time, part-time), interns, consultants, contractors, partners, and volunteers using GenAI systems on the City's behalf must adhere to applicable local, state, national, and international laws, regulations, and ethical guidelines governing the use of AI

Chief Information Officer- Attachment A 1
AD 7.4A Acceptable Use of Information Technology

- COSA CIO Position Statement; Artificial Intelligence (AI) Standards (Jan 8, 2024)
- AD 7.4a Acceptable Use of Informaton Technology
- Attachment A- Acceptable Use of Generative AI Tools (Feb 2024)
- AD 7.3a Data Security
- AD 7.12 Data Governance
- COSA Ethics Training

COSA Roles and Responsibilities

Chief Information Officer (CIO)/ Chief AI Officer (CAIO)

- Directs COSA technology resources, policies, projects, services, and coordinates same with other COSA departments.
- Actively ensures the AI system is used in accordance with this policy and other policies.
- Oversee enterprise digital privacy practices, data processing practices, and responsible usage of technology in compliance with the COSA Administrative Directives.
- Oversee the privacy practices of AI systems used by or on behalf of COSA departments.
- Notify COSA departments when an update to this policy or the [AI Policy Manual, or applicable policy] is released.

Chief Security Officer (CSO)/Chief Information Security Officer (CISO)

- Ensure AI systems are used in accordance with the COSA Information and System Security Policy.
- Oversee enterprise security infrastructure, cybersecurity operations, updating security policies, procedures, standards, guidelines, and monitoring policy compliance.

COSA Departments:

- Follows policy and updates to policy and shall check compliance with these documents at least annually.

City Attorney's Office (CAO):

- Advises of any legal issues or risks associated with AI systems usage by or on behalf of COSA departments.

City Manager's Office (CMO):

- At discretion, inspect usage of AI systems or alter/cease its or partner's usage on behalf of the department.

Finance Department (CFO,DCFO)- Purchasing Office (CPO):

- Oversee procurement of AI systems; require vendors to comply with COSA policy through contractual agreements.

How Does GenAI Change a Typical AI Strategy?

	Current AI Strategy		Updated AI Strategy
Vision	AI automating tasks	▶	Generative AI augmenting people in their work
Roadmap	Three-year outlook, business innovation	▶	One-year outlook, business criticality
Use Cases	Predictive analytics, automating tasks	▶	Generating artifacts (text, video, audio, code & data) and simulating decisions
Governance	Fragmented or part of data and analytics	▶	Clear business responsibility, ethics-focused
Talent	AI center of excellence	▶	Educating everyone on responsible use of GenAI

Source: Gartner

Updated Transformation Strategy

Vision	• Embrace that Generative AI Augments, not Replaces People. • Focus on Making Residents Lives Better. • Approach: People. Policy. Process. Data. Then Technology.
Roadmap	• One-year Outlook, Business Criticality. • Business Purpose. Pain. Resident and Employee Needs. • Controlled Private Large Language Models with Standards and Governance.
Use Cases	• Find High Value Business Use Cases that Are Best for AI; Resident and Back Office. • Generating Artifacts (text, video, audio, code & data) and Simulating Decisions. • Focus on Transforming Operations and Augmenting Workers.
Governance	• Business is Responsible. CIO Guided. Ethics Focused- Double Down on Ethics. • Set AI Principles Aligned with Current Data Governance, Acceptable Use Policies. • Understand and Mitigate the Risks and Potential Harms Early.
Talent	• Educate Everyone on Definitions and Responsible Use of AI and GenAI. • Be Security and Data AI-Ready. • Focus on Employee Upskilling vs Replacement.

Emerging Use of Artificial Intelligence (AI) Technologies

CITY OF
SAN ANTONIO
TEXAS

Council B Session
15 May 2024

Craig Hopkins
Chief Information Officer/ IT Director