THE *FAST-MOVING* AI GOVERNANCE LANDSCAPE

April 2026

protiviti®

Global Business Consulting

Agenda

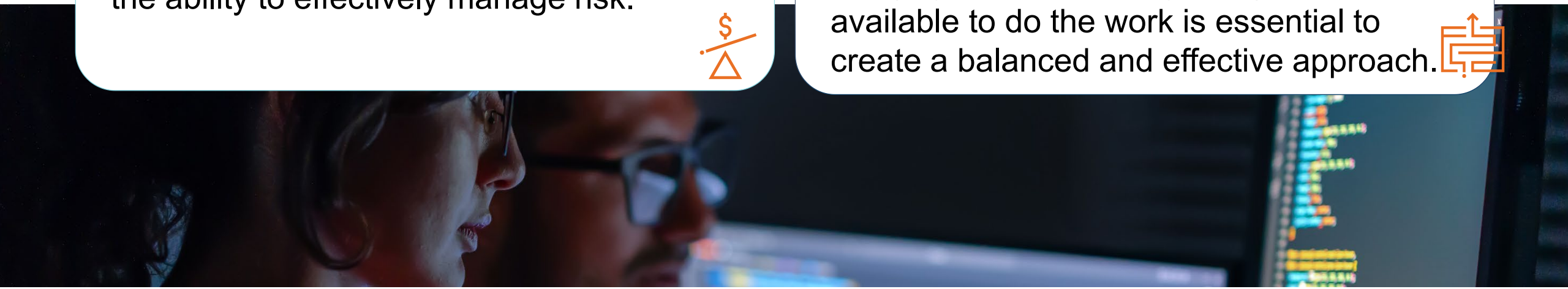
Strategic and Responsible Use of AI

Balance Innovation with Responsibility

Organizations must evaluate opportunities while considering responsible and trustworthy principles. A smart decision that allows an opportunity to move forward is based on considering aspects such as the business model along with risk factors and the ability to effectively manage risk.

Navigate Opportunity and Risk Jointly

An effective AI operating model incorporates careful consideration of opportunities, the ability to measure and monitor realized value, and the need for effective risk management. A multidisciplinary cross-functional team that is highly skilled, formally assigned, and available to do the work is essential to create a balanced and effective approach.



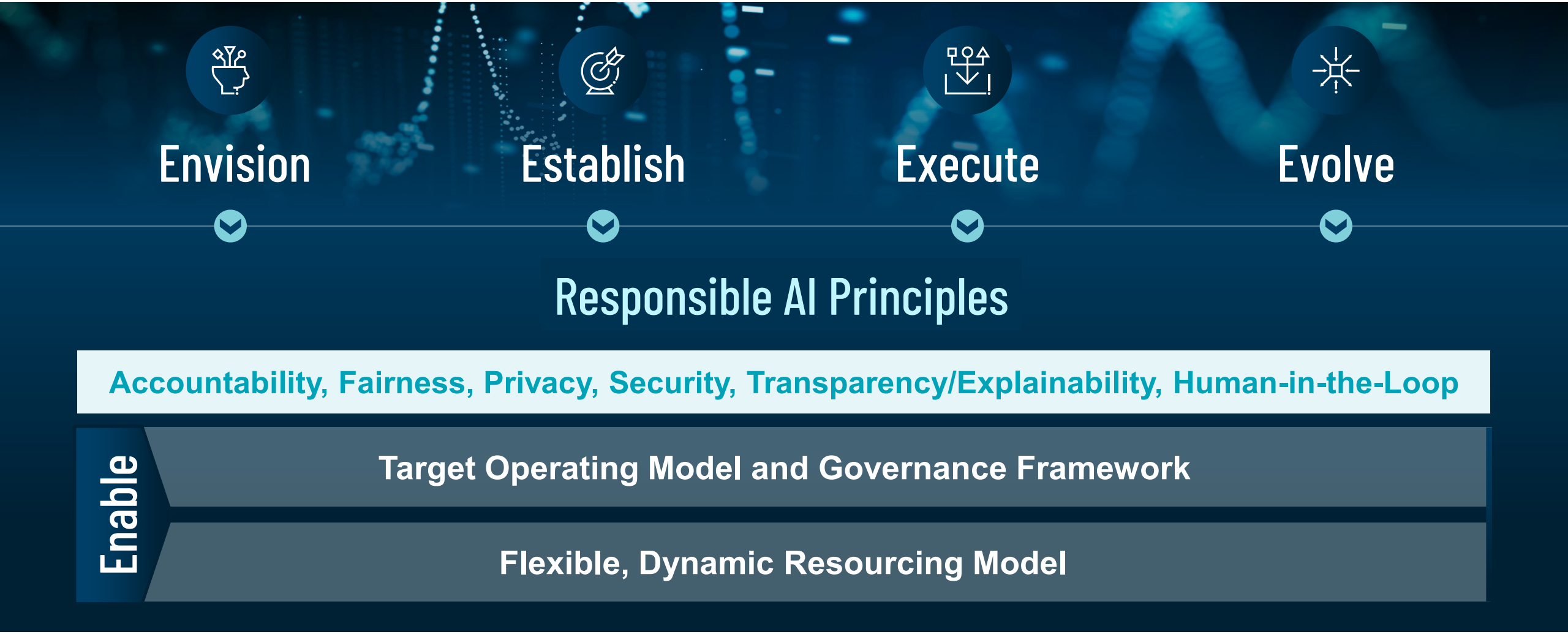
Common AI Challenges and Concerns

Nearly all organizations are experimenting with generative AI, yet 95% of pilot programs fail to deliver clear ROI or measurable impact, with only 5% successfully translating into revenue acceleration or sustained productivity gains.

Source: MIT Technology Review 07/2025

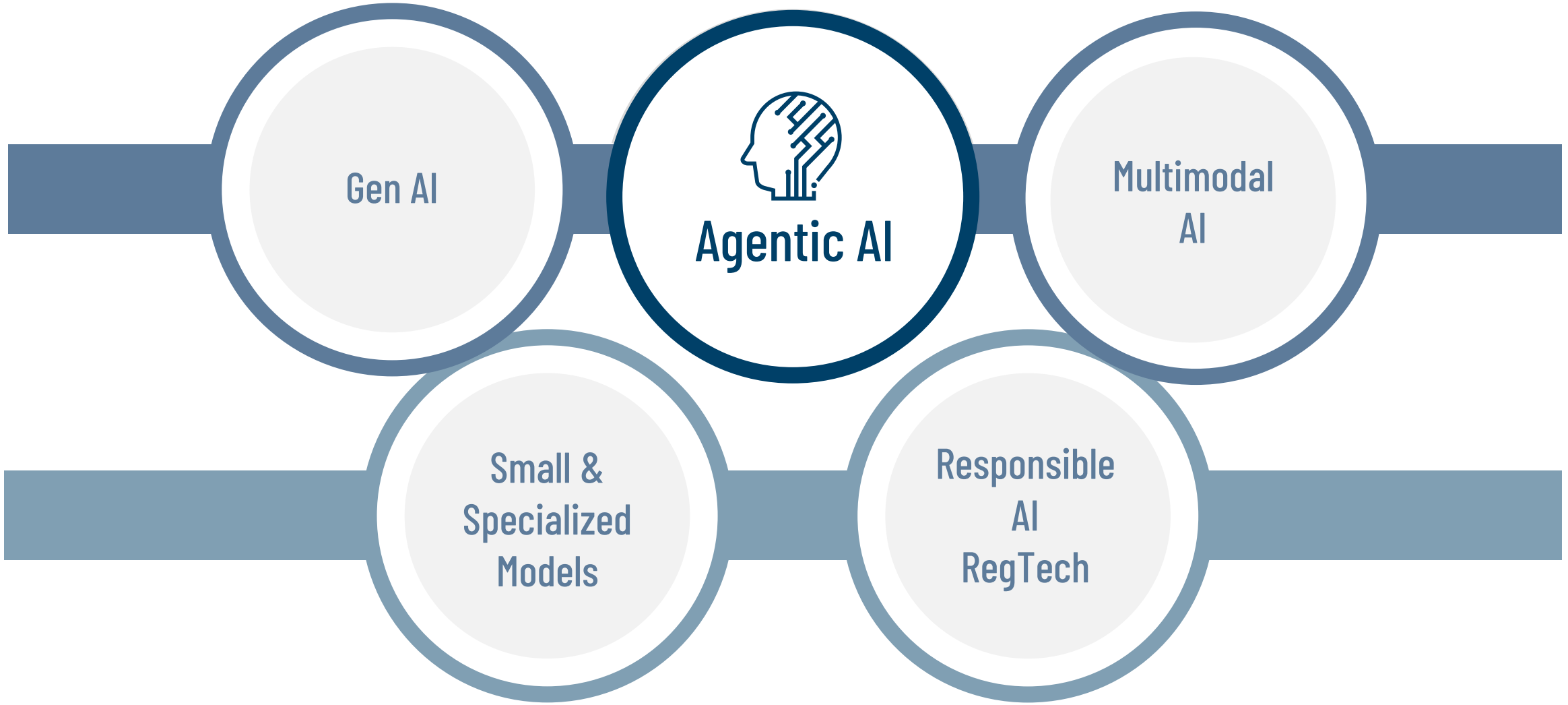
- **Difficulty delivering speed to value & achieving clear ROI**
- **Confusion navigating the rapidly evolving AI technology landscape**
- **Ambiguity in use case selection, prioritization, and resourcing**
- **Lack of trust, transparency, & data security**
- **Uncertainty amid fast-changing regulatory and legal requirements**

Leading Companies Approach AI Strategically, Grounded in Responsibility



protiviti

AI Trends



protiviti

What is Agentic AI?

Agentic AI describes **AI systems** that are designed to **autonomously** make decisions and act, with the ability to pursue complex goals with limited supervision. It brings together the flexible characteristics of LLMs with the accuracy of traditional programming. **This type of AI acts autonomously to achieve a goal** by using technologies like {NLP, ML, RL}... Agentic AI can adapt to different or changing situations and has “agency” to make decisions based on context.

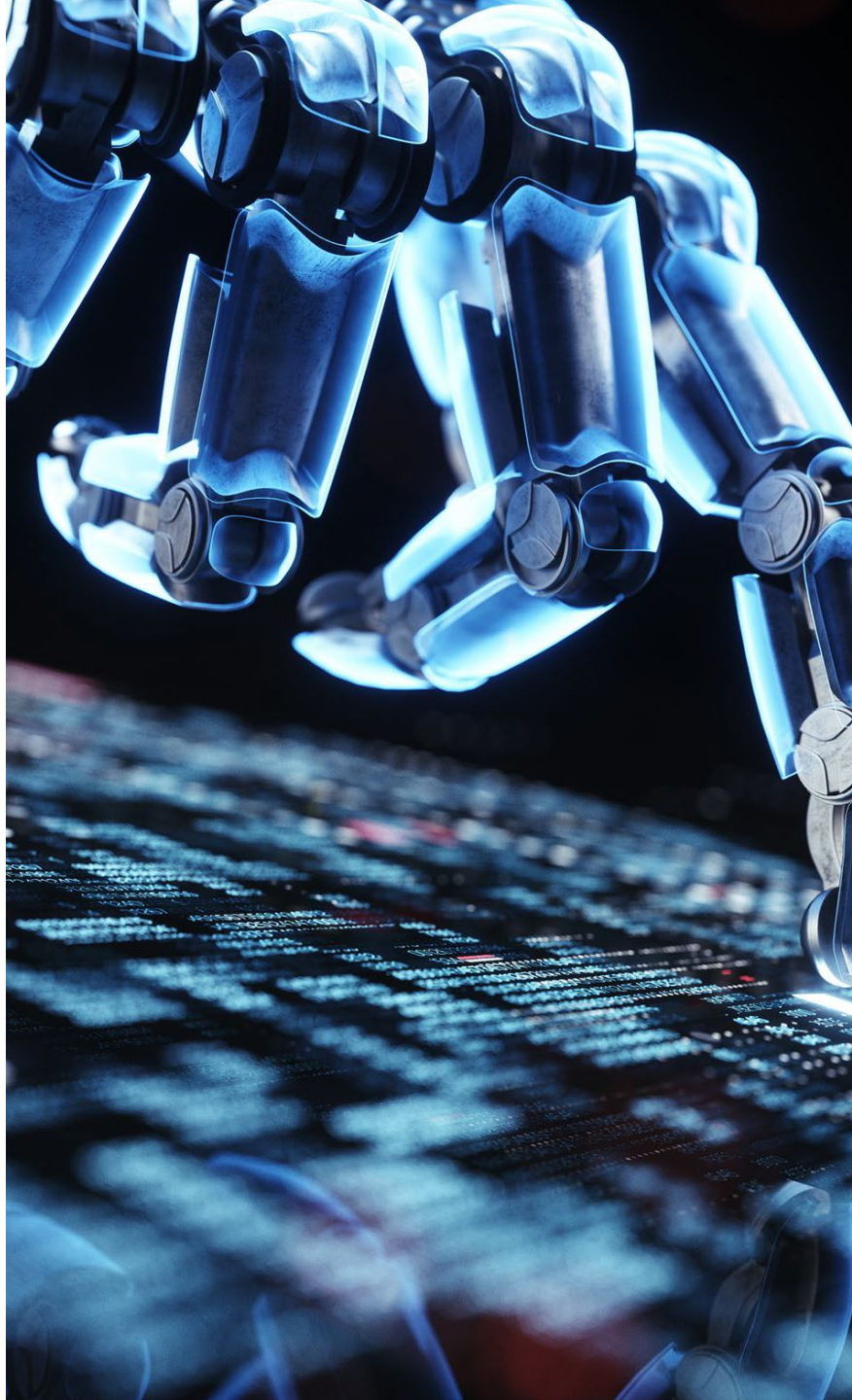
IBM Agentic vs Generative AI

Agentic AI is **proactive and autonomous**. It makes its own decisions to reach goals. A key feature is using external tools to get information beyond their inherent knowledge base. This lets Agentic AI work and solve problems very independently and effectively.

Google - Agentic AI with Gemma

Agentic AI is a **software system** designed to interact with data and tools in a way that requires minimal human intervention. With an emphasis on goal-oriented behavior, agentic AI can accomplish tasks by creating a list of steps and performing them **autonomously**.

RedHat What is Agentic AI



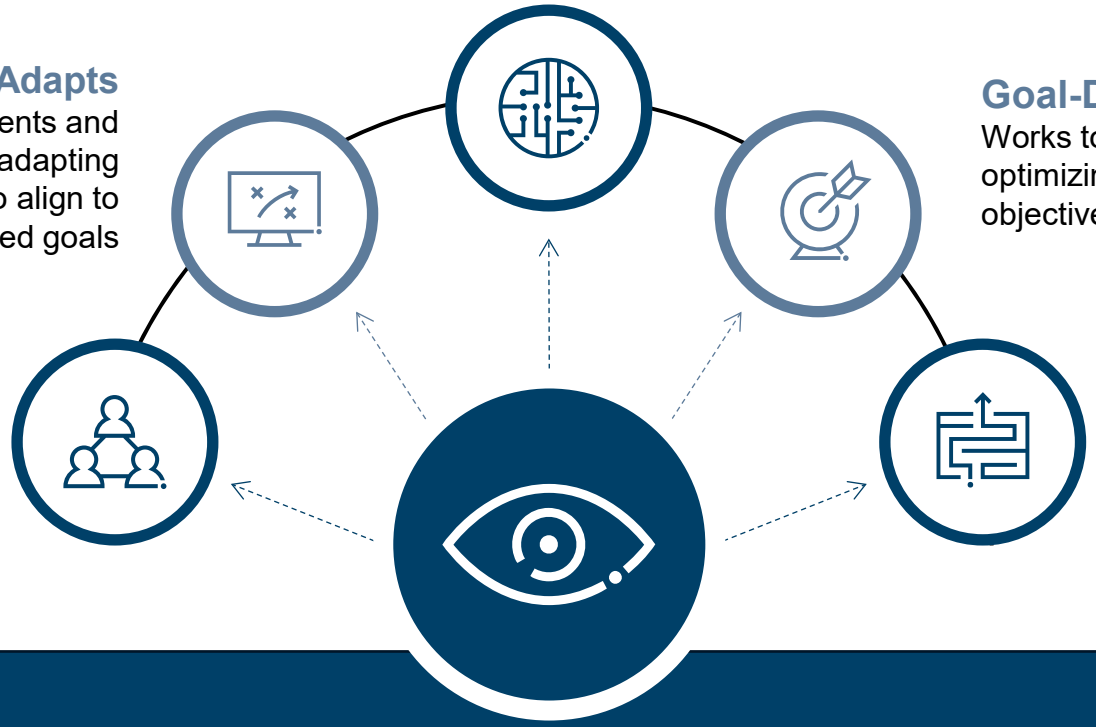
Agentic AI Characteristics

A non-exhaustive overview of the predominant characteristics of Agentic AI

Autonomous
Analyzes, interprets and acts without constant human supervision

Learns & Adapts
Learns from engagements and outcomes, improving and adapting performance over time to align to stated goals

Goal-Driven
Works towards a defined objective, optimizing actions to align to stated objectives



Cooperative
A collection of technologies and models, often with an orchestrator agent

Reasons
Plans its own steps or tasks using techniques such as step-by-step reasoning, formulates strategies over multiple steps and interactions

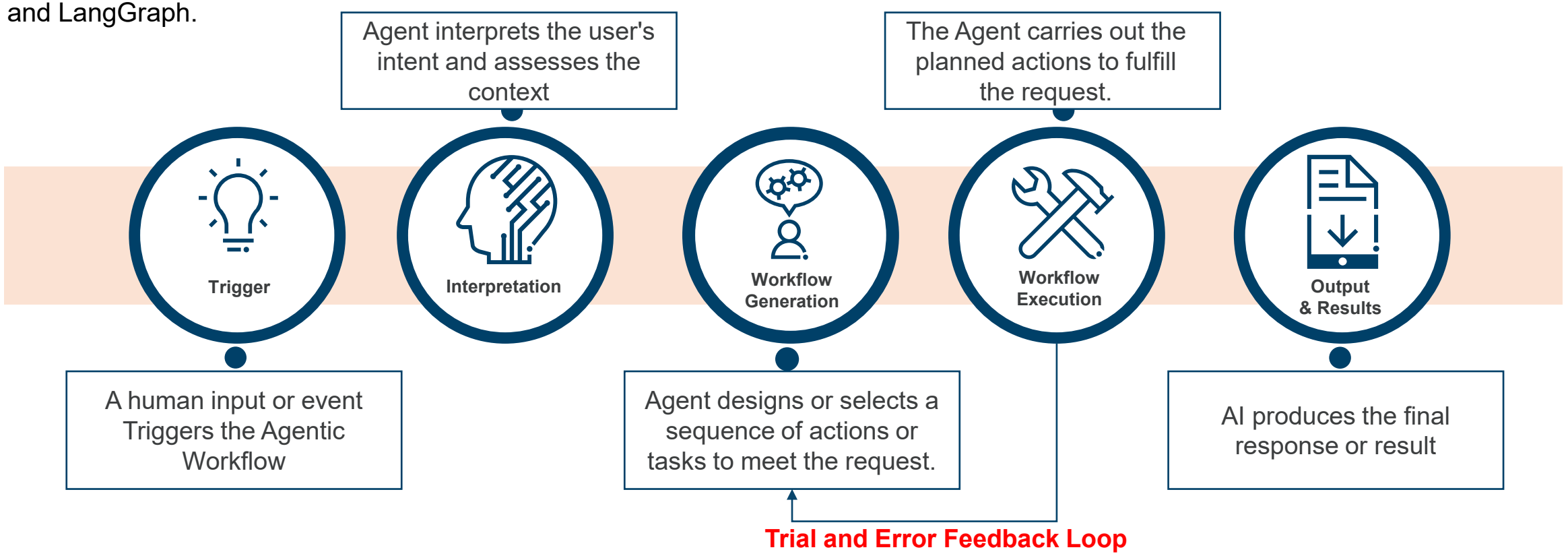
Agentic AI vs. Automation

Agentic AI shifts from predefined, rule-based automation to AI systems that plan, adapt, and act autonomously in complex environments

	"Traditional" Automation	Automation + AI	Autonomous + Agentic
Purpose	Performs a pre-defined action	Follows a list of steps and uses an LLM in at least one step	Develops a plan and executes to accomplish an objective
Autonomy	Low	Moderate	High
Adaptability	None	Learns from past experience	Adapts to real-time feedback and as circumstances change
Decisioning	Limited, follows predefined rules and/or scripts	Advanced, with machine learning algorithms and data analysis	Highly advanced, dynamically adjusting plan to achieve goal
Task Capacity	Repetitive and routine	Complex, requiring reasoning, prediction and problem solving	Dynamic, goal oriented, execution steps may differ
Example	Automates responses to customer inquiries with scripted, pre-defined templates	Interacts with customers through a natural language chatbot, resolves common issues, and routes complex problems to human agents	Facilitates a procurement process proactively - researching vendors, negotiating terms, preparing contracts, involving humans for final approval

Agentic Workflows

Agentic workflows allow individual users to scale their AI capabilities by using agentic tools and framework like CoPilot, AutoGen, and LangGraph.



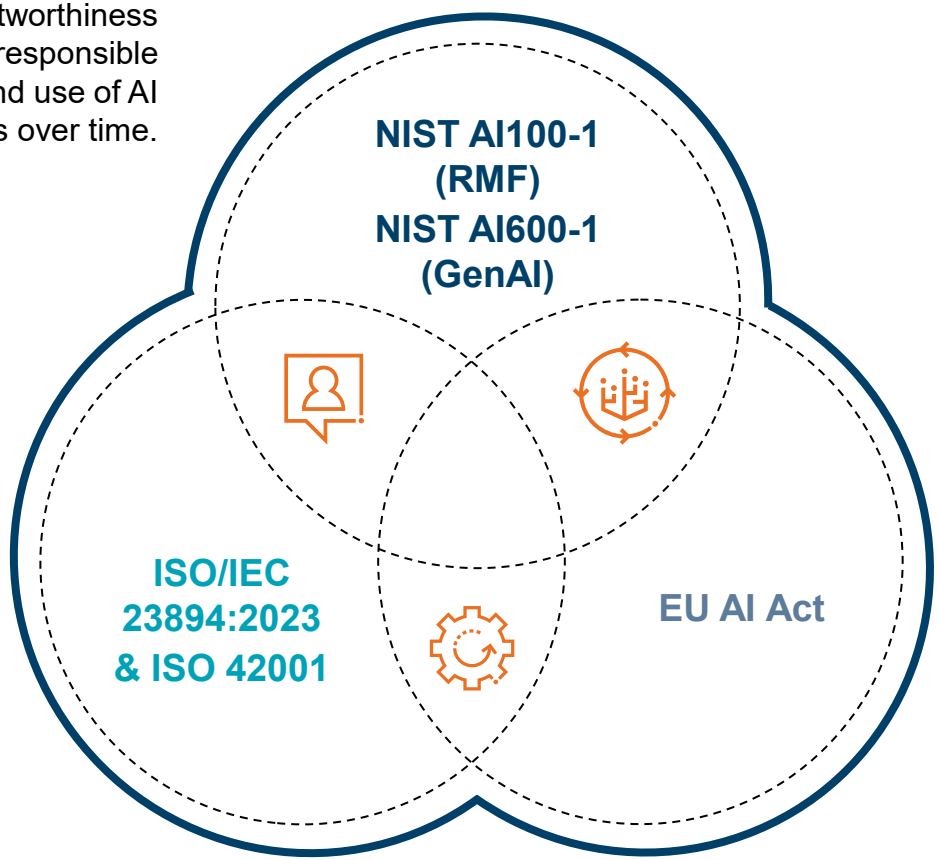
Benefits of Agentic AI

- **Enhanced Autonomy**
- **Improved Problem Solving**
- **Adaptability**
- **Personalization**
- **Scalability**

Emerging Standards for AI Governance

NIST AI Risk Management Framework

is designed to equip organizations and individuals with approaches that increase the trustworthiness of AI systems, and to help foster the responsible design, development, deployment, and use of AI systems over time.



Predominant Themes

Safety, Security & Resilience	**Transparency & Accountability**
Privacy	**Ethics & Fairness**
Validity / Reliability	**Explainability & Interpretability**
Data Quality & Integrity	

ISO/IEC AI Framework

Provides guidance on managing risk associated with the development and use of AI. The document offers strategic guidance to organizations to assist in integrating risk management into significant activities and functions.

European Union AI Act

Focuses primarily on strengthening rules around data quality, transparency, human oversight, and accountability. It also aims to address ethical questions and implementation challenges.

protiviti

NIST AI 600-1 – Extensions for Generative AI

Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile – *July 2024*

- **CBRN Information or Capabilities:** Access to information or abilities related to hazardous materials including chemical, biological, radiological, and nuclear (CBRN) weapons.
- **Confabulation:** Generation of confidently stated but erroneous or false content that can mislead users.
- **Dangerous, Violent, or Hateful Content:** Production and access to harmful content including violent, inciting, radicalizing messages or recommendations for illegal activities.
- **Data Privacy:** Risks relating to unauthorized leakage, use, disclosure, or de-anonymization of sensitive personal data.
- **Environmental Impacts:** Adverse ecological impacts due to high computation resource usage in GAI models training and operation.
- **Harmful Bias and Homogenization:** Amplification of existing biases leading to discrimination or incorrect presumptions; system outputs skewed toward undesired homogeneity.
- **Human-AI Configuration:** Misinterpretations in human-AI interactions leading to inappropriate anthropomorphizing & emotional entanglement
- **Information Integrity:** Deterioration in the veracity of content due to ease in generation and dissemination potentially leading to misinformation campaigns.
- **Information Security:** Enhanced threats from offensive cyber capabilities compromising system availability and data integrity.
- **Intellectual Property:** Unauthorized replication of copyrighted content; exposure of trade secrets; plagiarism issues.
- **Obscene, Degrading, and/or Abusive Content:** Easier creation/accessibility to harmful imagery including synthetic child sexual abuse material (CSAM), nonconsensual intimate images (NCII).
- **Value Chain and Component Integration:** Risks arising from non-transparent integration of third-party components in the AI lifecycle undermining accountability.

Navigating AI Security Risks: OWASP's Top Threats

OWASP

Top Threats for LLM Applications & Generative AI

Prompt Injection	Sensitive Information Disclosure
Supply Chain	Data and Model Poisoning
Improper Output Handling	Excessive Agency
System Prompt Leakage	Vector and Embedding Weaknesses
Misinformation	Unbounded Consumption

Top Threats for Agentic AI

Agent Goal Hijack	Tool Misuse and Exploitation
Identity and Privilege Abuse	Agentic Supply Chain Vulnerabilities
Unexpected Code Execution (RCE)	Memory & Context Poisoning
Insecure Inter-Agent Communication	Cascading Failures
Human-Agent Trust Exploitation	Rogue Agents

Top Threats for Machine Learning (ML) Systems

Input Manipulation Attack	Data Poisoning Attack
Model Inversion Attack	Membership Inference Attack
Model Theft	AI Supply Chain Attacks
Transfer Learning Attack	Model Skewing
Output Integrity Attack	Model Poisoning

protiviti

Identifying Value & Evaluating Readiness of AI

Value Identification

Where should we apply AI?

Key Focus:

Do we understand AI's strengths, value areas, impacts, levers, and how we'll measure results?

Data

Do we have the data and is it ready?

Key Focus:

What data do we need, where is it stored, is it usable, governed, and fit for AI?

Skills

Do we have the talent we need to unlock the value?

Key Focus:

What AI skills do we have, where are they, and do they align with our goals and training plan?

Ecosystem

Where to build/buy/partner?

Key Focus:

Does our value case fit today's solutions, are we in the AI ecosystem, and do we have a build-buy-partner plan?

Experimentation

Do we have a capacity to test & learn quickly?

Key Focus:

Do we have the right tech setup, a prototyping approach, and strong design thinking and agile practices?

Change Management

Do we have an organized plan to execute?

Key Focus:

What is our change readiness, and how will we get buy-in, communicate, and handle feedback?

Enterprise AI Governance Pillars

protiviti

AI Solution (System, Use Case, Model) Lifecycle Example

Below outlines an illustrative AI Governance Lifecycle/Framework with underlying risks, controls, and supporting Governance elements (People, Process, Technology). This is an illustrative framework and is not intended to be exhaustive, but rather to be right-sized and form fit for your organization.

01	02	03	04	05	06	07
Business Need & Context	Data Understanding & Preparation	Solution Design & Development	Testing Evaluation Validation & Verification	Integration & Implementation Planning & Execution	Monitoring & Optimization	Contingency Plans & End-of-Life Management

Status Reporting & Escalation when behavior drifts from plan

Communicate & Educate the strengths & weaknesses of the AI in question, understanding technical details, incorporating controls into AI design, credible challenge

Holistic	Multidimensional	Systematic	Actionable

AI System/Use Case Intake, Tiering, and Risk Assessment Framework

Terms of Reference / Definitions	Structured Intake	AI System, Use Case and Model Inventory	Tiering Matrix (routing mechanism)	AI System, Use Case and Model Risk Assessment	Calculated Residual Risk	Additional Tech/ Human Controls	Finalized Risk Control Profile
Key terms are defined and aligned to organizational risk taxonomy to leave fewer things open to interpretation and remove ambiguity (EU AI Act, ISO, NIST, IAPP, etc. typically leveraged)	System, Use Case, and Model Intake request has structured data fields and limits freeform text entry	Necessary attributes to understand system, use case, models, data, features, risks, and other characteristics required for transparency and explainability	Initial use case risk tier is determined based on information from intake request form and AI risk questionnaire; Model risk tier is determined when development team selects model	System, use case and model risk tiering dictate level of rigor needed for UC Risk Assessment; existing profiles are referenced if applicable; tool or model/use case/system risks are considered	Initial output of System, Use Case, or Model Risk Assessment includes residual risk; risk tier is re-evaluated/ confirmed	If residual risk falls within organizational risk tolerance, it is mitigated by adding additional tech and human controls	Final output of System, Use Case, or Model Risk Assessment is managed inherent and residual risk

AI System, Use Case, and Model Lifecycle Accelerators

Streamlined Intake Process

- Standardized intake uses structured fields to limit open text
- Captures key information upfront for faster stakeholder decisions
- Generates a use-case tier to guide next governance steps

Secure Sandbox Environment for POCs

- Internal and vendor sandboxes provide secure environments for POC testing
- Sandboxes operate with clear guardrails
- POCs in sandboxes are time-bound and tracked

Delegated Roles & Approvals

- Authority and responsibility are distributed by tier across governance and risk bodies
- Roles are clearly defined to streamline decisions and strengthen accountability

Optimized Risk Tiering Methodology

- Each AI use case, system, or model receives a risk tier based on key intake attributes
- Tier defines required activities, approvals, & documentation
- Creates a structured framework

Expedited Path for Lower Risk/ Impact Use Cases

- Lowest tier offers faster approval for low-impact use cases with minimal tollgates
- Maintains proper governance and oversight while speeding implementation

Standardized Risk Control Matrices (RCMs)

- RCMs standardize risks and controls, ensuring consistent detail
- They distinguish model-level and use-case-level risks, so stakeholders assess only what's relevant

Key terms essential to AI governance and lifecycle processes are defined in a comprehensive AI glossary

Exemplary Risk Tiering Attributes

Starred attributes highlights one pattern or subset of tiering attributes that can be chosen

	Attribute	Description
★	**EU AI Act or Organizational 'Prohibitive' or 'high-risk' use of AI**	Whether the AI use case is classified as prohibited/high-risk per the EU AI Act or internal policy
★	**Impact on Core Business Processes**	Degree to which the AI system affects essential business operations or services
	Regulatory Compliance Legal Exposure	Potential for legal or regulatory violations if the AI system fails or is misused
	Reputational Exposure	Risk of negative public perception or media attention resulting from AI-related incidents
	Third Party Risk Rating	Level of risk introduced by external vendors or service providers involved in the AI solution
	Use of Agentic AI	Whether the system utilizes agentic AI, which may present unique risks
	Operational Criticality/Resilience	Importance of the AI system to operational continuity and ability to recover from failures
	Based on Pre-Approved AI Environment	Whether the AI operates in an environment sanctioned by IT and security standards
★	**Information Security Classification**	Sensitivity of data processed (e.g., confidential, restricted, public)
	Impact on Failure	Severity of consequences if the AI system malfunctions or produces incorrect outputs
	End User Role Proficiency	Skill level and expertise of users interacting with the AI system
	Information Barriers	Existence of controls preventing unauthorized data access or leakage
★	**Data Leaving Corporate Network**	Extent to which AI solution transmits data outside the organization's secure network
★	**Target Audience**	Intended recipients of AI outputs (e.g., internal staff, customers, public)
	Target End Users	Specific user groups who directly interact with the AI system (e.g., finance team, sales)

How Can Generative AI be Applied in Internal Audit?

LLMs can drive efficiencies throughout the entire audit life cycle. Below are example use-cases for consideration.

Select your department
Internal Audit v

Today

- **Impactful Presentation Ideas**
- **Audit Committee Preparation**

Previous 7 Days

- **Combative Control Owner**
- **Planning API Audit**
- **Mentoring Audit Staff**

Previous 30 Days

- **Preparing for GAM Conference**

Planning

- Audit Announcement
- Planning & Scoping Memo
- Document Request List
- Work Program Development
- Control Test Plan Development

Fieldwork

- Business Process Flows
- Executive Summary Development
- Process/Control Narratives
- Observations & Recommendations
- Evidence Review Acceleration
- Audit Response Analyzer
- Work Program Completion
- Best Practices & Value Adds
- Control Test Plan Completion
- Policy & Standard Reviewer

Other

- Internal Audit Charter Creation
- Audit Strategy & Roadmap
- Audit Policies & Procedures
- Risk Assessment
- Audit Analytics & Automation
- Stakeholder Communication
- Meeting Notes Cleaner
- Function Research
- Innovation Brainstorming

protiviti

Auditing Artificial Intelligence

- **AI may be envisioned as a large circle with several smaller circles within it**. AI, which is machines carrying out tasks based on algorithms in an "intelligent" manner, is the large circle; other, more specific types of AI, such as machine learning, are represented in the smaller circles. Machine learning is a subset of AI in that it focuses on machines' ability to receive a set of data and learn for themselves, changing their algorithms as needed as they learn more about the information, they are processing.
- **AI does not operate based on a set of predetermined rules**. Predetermined rules are associated with traditional software engineering. However, an excessive number of rules tends to inhibit the technology's ability to learn and adapt to its circumstances. Therefore, AI does not always operate based on a predefined set of rules.

Traditional lag time

AI has permeated many facets of our daily lives, from making loan decisions to powering our home assistants. AI's rise has been accompanied by the **traditional lag time** between early adoption and the establishment of regulatory and compliance frameworks. There is, for example, no mature auditing framework in place detailing AI subprocesses, nor are there any AI-specific regulations, standards or mandates.

1

Definition of AI is frequently debated

The **definition of AI is frequently debated** and the IT world, including auditors, has not reached a common definition or taxonomy on which to specify a set of world-class practices.

2

Complex systems

AI systems and solutions vary widely from each other, and the vast set of existing and emerging technologies foundational to AI architecture give birth to **complex systems**. This complexity points to a high likelihood of uncertainty around the scope of AI within the business. Despite this uncertainty in the business, auditors are well positioned to take on their responsibilities relative to AI.

3

Shortage of qualified resources, e.g., AI experts

The complexity of AI and the **shortage of qualified data scientists** will routinely lead to the outsourcing of AI development projects to one or more third-party resources. A coherent understanding of enterprise AI will be dispersed—and, over time, perhaps even lost—across tiers of AI providers. This will subsequently increase the challenge for the AI auditor.

4

Source: ISACA

IA Engagement in AI

1. AI Governance Committee Participation

IA Role: Providing insight regarding AI initiative alignment with organizational goals, compliance with regulations, and effective risk management.

2. Design/Maturity Focused Assessment

IA Role: Perform assessments to evaluate the design and maturity level of AI systems, including specific lifecycle processes from development to deployment and maintenance.

3. Assurance Engagements

IA Role: Provide assurance on the reliability and integrity of AI systems by assessing effectiveness of the system meet predefined criteria and standards.

4. Consideration for AI in Non-AI Focused Engagements

IA Role: Provide insight into how the use of AI may impact other audit areas. For example, IA may be consulted on the potential risks of utilizing AI as a component of an ongoing Human Resources audit, helping to evaluate how these systems comply with legal and ethical standards, and their effects on data privacy and employee rights.

Examples of AI Audits – Overview

- **Enterprise AI Governance Audit:** Assess org-wide AI strategy, policies, oversight.
- **AI Lifecycle Audit:** Evaluate AI system acquisition and development process and controls across design, training, deployment, monitoring.
- **System/Model-Specific Audit:** Deep dive into a single AI solution or model.
- **Third-Party Risk Audit:** Evaluate processes and controls specific to AI throughout the third-party lifecycle.
- **AI Cybersecurity Audit:** Focus on security controls, threat modeling, and vulnerability assessments for AI systems.

Current AI Usage in Internal Audit

As AI advances, Internal Audit should leverage it for greater efficiency and effectiveness. Here's how other Internal Audit departments are adopting AI, with percentages reflecting usage based on a recent survey.

45%	65%	35%	10%
AI In GRCs	**Copilot**	**Private LLMs**	**AI + Automation**
AI embedded in Audit Management or GRC tools to generate issue, risk wording, and more.	Using Microsoft Copilot for audit use cases within Teams, Word, PowerPoint, and Excel.	Private and secure cloud-based chat applications, akin to ChatGPT, are designed exclusively for corporate use.	Utilizing APIs and agentic AI to facilitate automated usage of AI outside of the chat interface.

Or none	5%

Internal Audit Departments Are Already Seeing AI Benefits

39% of internal auditors are already employing AI with an additional 41% planning to adopt within the next 12 months; **80% of internal auditors plan to be using AI within the next year**.

54% of internal auditors reported that AI will drive efficiency and productivity gains in the next 12 months.

Internal audit departments are beginning to see real value in driving efficiencies across the audit lifecycle. From planning and scoping to reporting, resources are using AI to re-allocate their time to more critical activities.

Planning & Scoping

30%

estimated time savings

- Walkthroughs
- Process / Control Scoping
- Narratives / Process Flows

Fieldwork

20%

estimated time savings

- Evidence Review
- Document Request Lists
- Observation Language Review

Reporting

40%

estimated time savings

- Report Writing
- Drafting Action Plans
- Finding Risk Assessments

Sources: (1) Walters Kluwer (2) Microsoft

Questions?

Richard Kessler

Rich Kessler is a Director at Protiviti within Risk & Compliance and leads Artificial Intelligence Governance and Risk Management. During three-decade career, spent largely in-house at financial services institutions, he's helped clients address challenges in AI & emerging technologies, cyber security and privacy, data and information governance, eDiscovery and investigations, technology strategy, and operational risk management.

https://www.linkedin.com/in/rikessler/

Thank You

We value your feedback! Scan to complete the CPE course evaluation

protiviti®

Appendix

protiviti®

AI Governance & Risk Management Service Offering Overview

Protiviti's AI Governance & Risk Management offering enables clients to transform their AI strategy and use to address trustworthy and responsible AI principles early, often, and always. By improving in-house governance and risk management capabilities, leveraging new and existing channel partners and tools, we drive our clients to improve AI literacy, drive AI transformation, and successfully govern, control, and assure AI responsibly.

About Our Practice

Cross-disciplined / Cross-Capability competency hub **delivering cutting-edge governance and risk management AI assessments, audits, & build-outs** enabling Protiviti to be a leading provider of governance and risk management advisory and audit.

What We Do

We offer a comprehensive suite of approximately **twenty packaged offerings** to define standards, policies, and procedures for trustworthy & responsible AI; implement effective control mechanisms to manage AI risk and ensure compliance; and continuously evaluate, test, and assure AI performance, security, and trustworthiness.

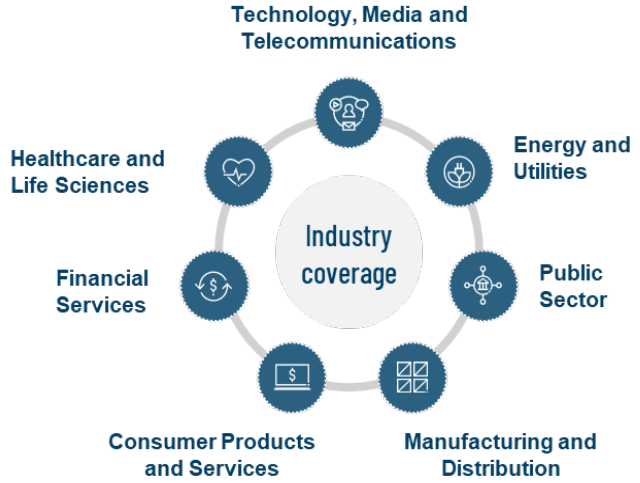
Our Mission

Our mission is to **provide our clients with insight, advisory, and foresight that drives informed decisions and transformative AI application and use cases**, ensuring competitive advantage and sustainable growth.

Client Base

Diverse coverage of clients across industries and geographies: a large number of our clients are serviced across FSI, Healthcare, Hospitality, TMT, CPG, M&D, and Government sectors..

Cross-Industry Coverage



Value Proposition

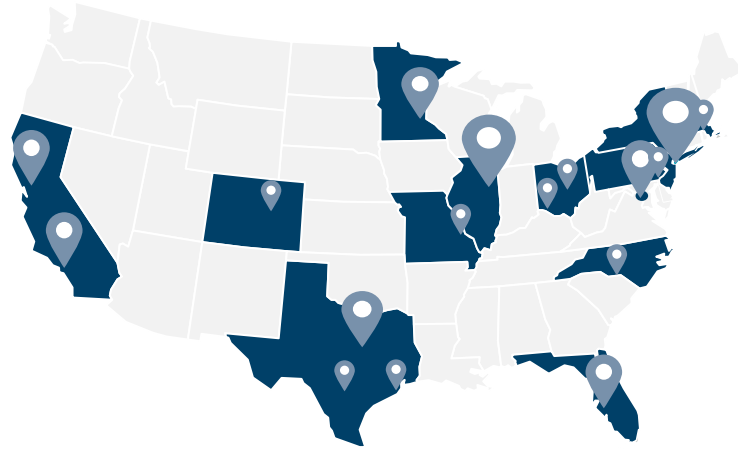
Accelerate decision-making and enhance operational efficiency by keeping pace and monetizing emerging and AI technology.

As a central AI Governance and Risk Management Hub, we offer **differentiated and innovative** solutions for various Geographies / Capabilities / Industries / C-Suite Solution teams.

Promote **collaboration, continuous learning and cultivate a culture of intellectual curiosity** by standing up high performing teams and enabling cross-solution offerings.

100+ Resources Across

16 Major Us Cities



Major Hubs

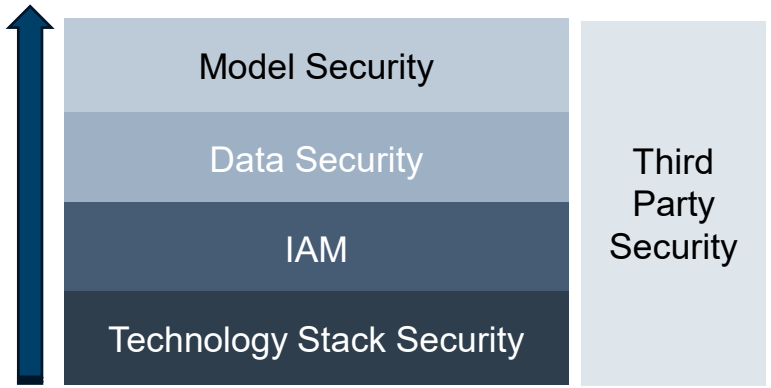
Austin	Cincinnati	Houston	San Francisco
Boston	Columbus	Los Angeles	St. Louis
Charlotte	Dallas	Minneapolis	Tampa
Chicago	Denver	New York	Washington DC

protiviti

How Enterprise Should Approach AI Risks

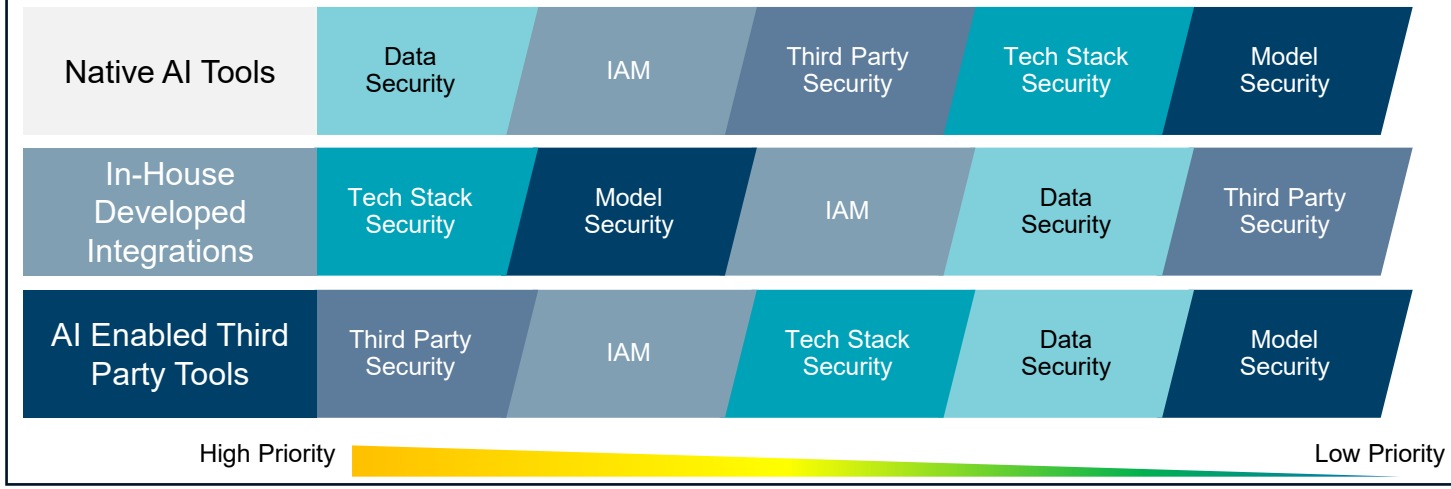
The following considerations provide a foundational framework to help an enterprise design risk ownership, control implementation, and governance processes.

Consideration 1:
AI risks should be viewed as "stacked" layers.



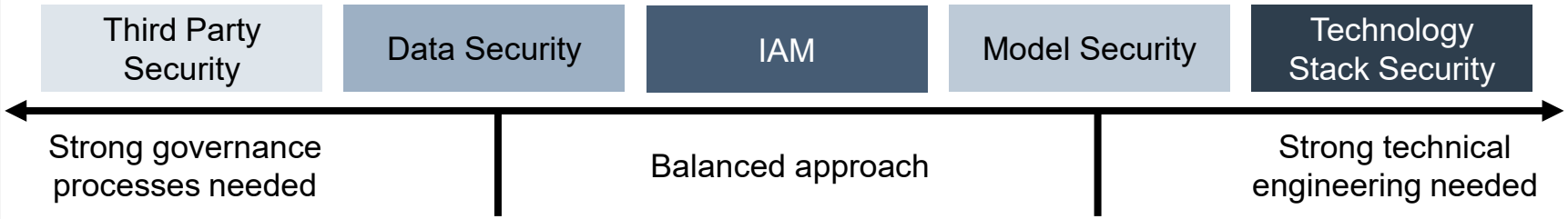
Exposure at a lower layer **cascades upward**.

Consideration 2:
AI risks should be prioritized differently based on the types of AI.



Consideration 3:
AI risks should be viewed by its level of abstraction:

- More abstracted risks require more **governance processes**
- Less abstracted risks require more **technical engineering**



protiviti

Principles of Responsible AI

1	2	3	4	5	6
Transparency and Explainability	**Fairness and Bias Mitigation**	**Accountability**	**Privacy and Data Governance**	**Robustness and Security**	**Human-Centered Design**
Organisations should strive for transparency in their AI systems, making sure they are understandable and explainable. Clear explanations of how AI systems work, **including data sources, algorithms, and decision-making processes**, foster trust and enable users to make informed judgments.	To ensure fairness, organisations should proactively identify and mitigate biases in their AI systems. They should assess and address potential biases in **data collection, model training, and algorithmic decision-making** to prevent unfair outcomes or discrimination based on protected attributes such as race, gender, or ethnicity.	Organisations should establish mechanisms to ensure accountability for the development, deployment, and use of AI systems. This includes clear lines of responsibility, **monitoring and auditing processes, and mechanisms** for addressing potential harms or unintended consequences of AI applications.	Safeguarding user privacy and ensuring responsible data governance is crucial. **Organisations must handle personal and sensitive data with utmost care**, following legal and ethical guidelines. They should implement appropriate measures to **protect data, obtain informed consent,** and comply with relevant data protection regulations.	AI systems should be designed and developed to be robust, resilient, and secure. Organisations must consider **potential vulnerabilities, adversarial attacks**, and potential risks associated with AI deployment. Implementing strong **security measures, continuous monitoring**, and risk assessment processes are essential to maintain system integrity.	Organisations should prioritise human well-being and ensure that AI systems are designed with **human needs and values in mind.** This involves involving diverse perspectives, considering user feedback, and regularly assessing the **social impact and ethical implications of AI** applications.

Microsoft Responsible AI Standard

Envision the Potential, Establish a Plan

Activities

Phase	Input	Strategic	Responsible	Output
Identify	Stakeholder/SME Participation via **Industry Use Case Catalog** and **Standards.**	• Use creative thinking to **find AI opportunities** • Use the **Industry Use Case Catalog** to define them • Build an **actionable AI idea inventory**	• Define **ethical, legal, and compliance requirements** • **Select relevant standards** (EU AI Act, etc.)	• Use Case Inventory • Recommended AI Standards
Prioritize	Use Case Inventory filtered through **AI Prioritization Framework**	• Set **value levers** and assess **technical complexity** • Check organizational readiness • Align tech components • Sequence roadmap for action	• Define use-case **risk schema** (L/M/H) • Do initial **risk ranking** • Gather more details for high-risk cases	• Sized & Prioritized Use Case Backlog • Initial Risk Screening Schema
Act	Prioritized Use Case developed with **Rapid Prototype Methodology**	• **Build and integrate** a prototype using rapid prototyping • **Connect to enterprise data** and demonstrate AI in action	• Expand **use-case details** • Run use-case **risk assessments** • Set guardrails to mitigate risks	• Functional Prototype

Protiviti's AI Capabilities

Value Creation

AI Strategy & Roadmap

Target Operating Model (TOM)

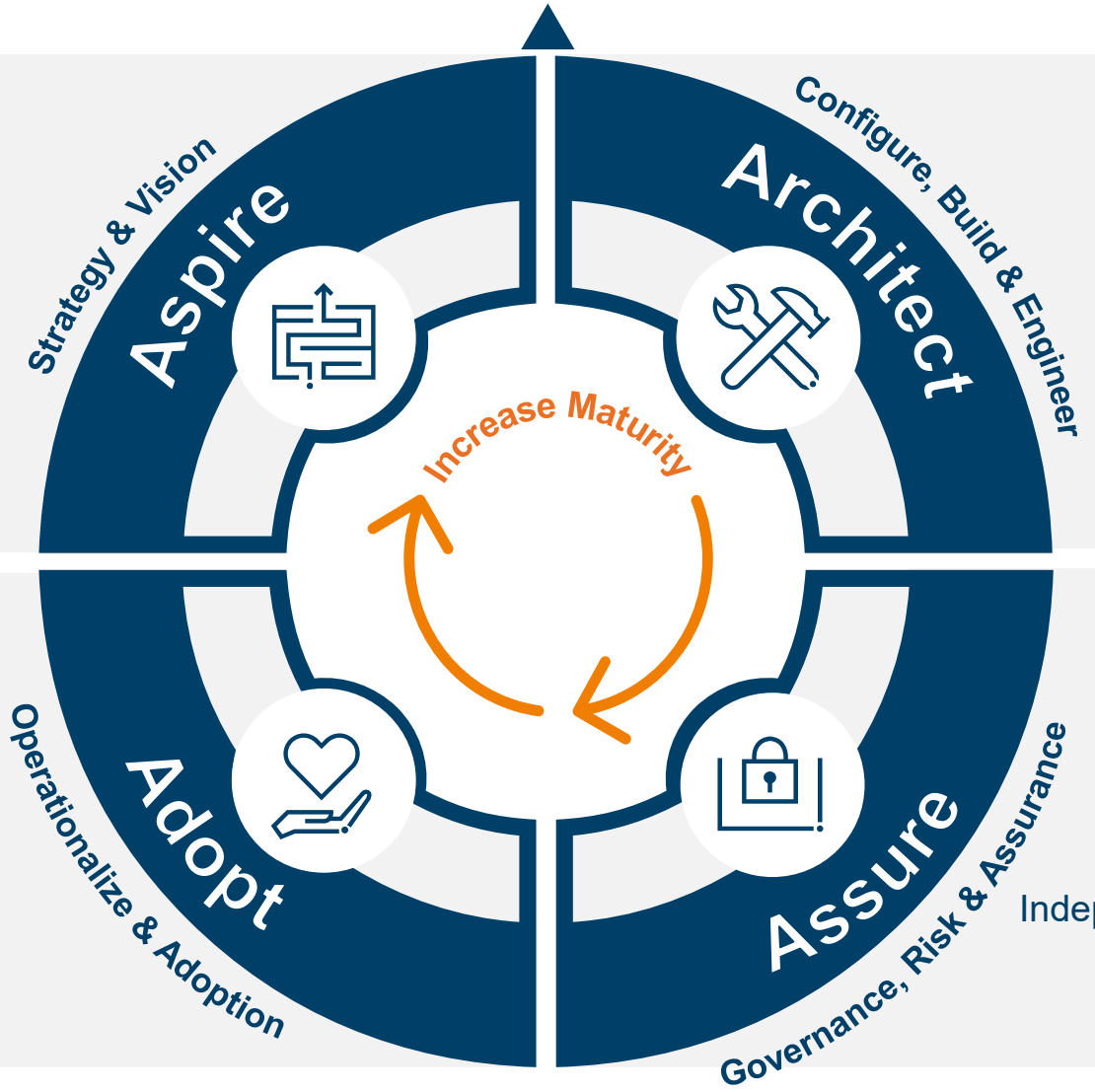
Maturity Assessment

Value Capture

Data Modernization

MLOps/LLMOps Implementation

Configure/Develop Solution



Value Realization

Workforce Transformation

Change Management & Training

Model Monitoring & Maintenance

Value Protection

Responsible AI (RAI) Framework

AI Risk Assessment

Independent Model Assurance & Audit

Protiviti's AI Capability Map

Create to accelerate business outcomes

Govern to build trust and transparency

Ideate + Strategize

Data Strategy
Align + Operationalize Data

AI Strategy
Value-Led AI Transformation

Experience Design
Concept + Design Experience

Center of Excellence
Scale + Operationalize AI

Develop + Deploy

App Modernization
AI-Ready Infrastructure

Data Development
Curate + Prepare Data

Model Development
Build Custom AI-ML Models

AI/GenAI Integration
Incorporate + Extend Models

Configure + Consume

Microsoft
M365 Copilot + Agents
Purview

Salesforce
Agentforce

ServiceNow
Agents + Automation

UiPath
Agents + Automation

Protect

Governance Strategy
Develop a Risk Roadmap

Governance Programs + Operationalization
Manage + Govern Risk

Regulatory Risk Management
Compliance + Reg Readiness

Legal Risk
Identify + Manage Risk

Control

Policies + Procedures
Establish Standards

Data + AI Governance
Inventory + Steward

Control Frameworks
Design + Implement

AI Security
App + Architecture Review

Monitor + Test

Audit & Readiness
Assess Controls

Model Risk
Evaluate Reliability

Red Team
Offensive Security Evaluation

Manage change to maximize adoption

AI Training
Upskill + Reskill Your Team

Executive Education
Inform + Align Leaders

Workforce Realignment
Align to Skills as AI Emerges

Change Management
Embrace + Manage Change

Protiviti's Key Definitions

Specific definitions and distinctions do not have academic and scientific consensus.

Artificial Intelligence ("AI")

Computer systems that mimic human-like thinking.

Machine Learning ("ML")

Algorithms that learn without explicit programming.

Generative AI ("GAI")

AI that creates new content (text, code, images, etc.).

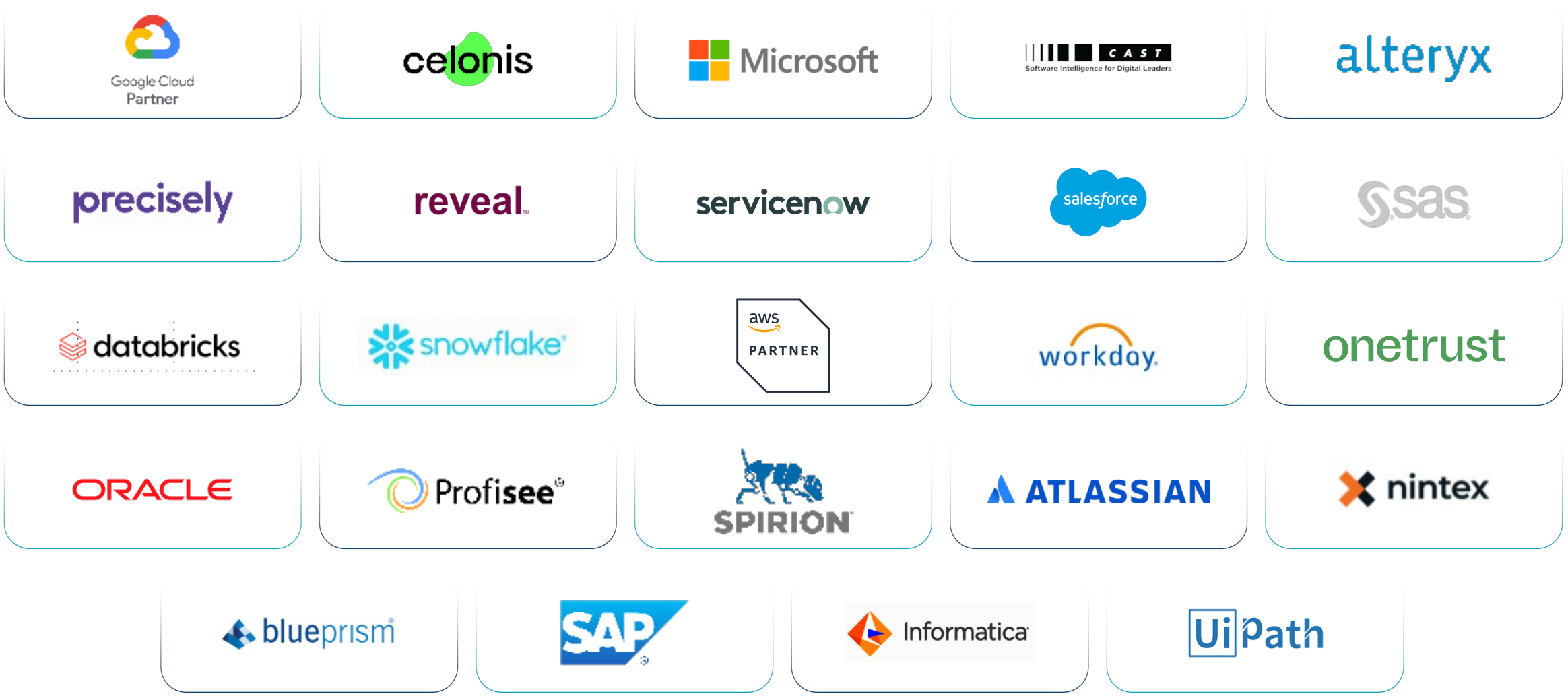
Large Language Models ("LLMs")

Generative models that produce text using massive data and parameters.

Chat GPT

An OpenAI LLM designed for conversation.

AI Partners


Google Cloud Partner
celonis
Microsoft
CAST
Software Intelligence for Digital Leaders
alteryx
precisely
reveal
servicenow
salesforce
sas
databricks
snowflake
aws PARTNER
workday.
onetrust
ORACLE
Profisee
SPIRION
ATLASSIAN
nintex
blueprism
SAP
Informatica
UiPath

Microsoft Partner Credentials

Microsoft
INNER CIRCLE
FOR MICROSOFT AI BUSINESS SOLUTIONS
25 | 26

Elite Partner

Microsoft Security

Microsoft Solutions Partner
Data & AI
Azure

Specialist
Data Warehouse Migration
Analytics
Infra and Database Migration

Microsoft Solutions Partner
Security

Specialist
Copilot
Threat Protection
Cloud Security
Identity and Access Management
Data Security

Microsoft Solutions Partner
Modern Work

Specialist
Adoption and Change Management
Teamwork Deployment
Modernize Endpoints
Copilot

Prioritized Tier Partner

Copilot

Microsoft Solutions Partner
Business Applications

Specialist
Low Code Application Development
Intelligent Automation
Copilot

Microsoft Solutions Partner
Digital & App Innovation
Azure

Specialist
Low Code Application Development

Microsoft Solutions Partner
Infrastructure
Azure

Specialist
Infra and Database Migration
Azure Virtual Desktop

Microsoft
Microsoft Partner
Finalist
2024 Partner of the Year
Compliance Award

protiviti

Global Data, Analytics & AI Presence

Protiviti has data, analytics & AI core offerings around the world supported by regional and global delivery centers

The Americas

1. United States
2. Argentina*
3. Brazil*
4. Canada
5. Chile*
6. Colombia*
7. Mexico*
8. Peru*
9. Venezuela*

Europe/Middle East/Africa

10. France
11. Germany
12. Italy
13. The Netherlands
14. Switzerland
15. United Kingdom
16. Bahrain*
17. Kuwait*
18. Oman*
19. Qatar*
20. United Arab Emirates*
21. Saudi Arabia*
22. Egypt*
23. South Africa*
24. Hungary

Asia-Pacific

25. Australia
26. China
27. India*
28. Japan
29. Singapore

Key:

*Protiviti Member Firm

- Regional Delivery Center(s)
- Global Delivery Center
- AI Studio(s)

Regional Delivery Centers

- In-country/region hub for client service delivery
- Flexible option for projects requiring onshore capabilities
- Centralized delivery capability focusing on standardized and scalable service offerings
- Innovative service offerings and solution exploration focusing on automation and emerging technologies
- Large pool of fungible resources with ability to scale up or down as required by your project needs

Global Delivery Centers

- Global hub for digital & innovation development and service delivery
- Specialized talent pool that can be scaled and customized for evolving client needs
- Bring global best practices to help our clients maximize technology investments.
- 24/7 support where needed
- Optimal blend of expertise and pricing
- Expertise in emerging technologies to help our clients manage costs and enable growth

protiviti

Why We are the Right Partner

Your journey, is our journey – We are with you every step of the way to ensure that you receive a 5-star experience

11,000+ employees	85+ offices	25+ countries	Agile and personalized support

Experience

AI is a multi-disciplinary, cross-functional effort. We bring both breadth of expertise as well as depth in each discipline. Our teams include:

- Technologists with 10+ Years of AI Expertise
- Data + Analytics Consultants
- Digital Strategists
- Legal, Compliance, Risk Experts
- Industry Executives

We understand the implementation and regulatory issues faced by global institutions and we have deep, practical experience addressing these challenges.

Partnerships

Success with AI is scaled through partnership, with each vendor providing domain and industry specific capabilities. We maintain a robust ecosystem of 60+ partners which enables us to support your build/buy/borrow approach to AI solutioning.

Our experience with AI is recognized through our Microsoft Specialization in as AI and Machine Learning.

These partnerships and our proven accelerators enable our teams to efficiently deliver and tailor solutions to your unique needs.

People

Our award-winning talent & culture is what we are known for and comprises top talent to serve our clients. Protiviti has also been recognized with an Excellence in AI Consulting Award.

Leveraging our parent company, Robert Half, Protiviti offers a blend of consulting and staffing solutions, allowing us to provide project-based resources at all levels.

Our unique expertise and blended staffing models enable us to provide powerful insights and practical solutions.

Protiviti consulting expertise + **Best in class ecosystem** + **Blended delivery models** = **Client value**

protiviti

PRO Modeling Services

Protiviti has conducted model development, validation, and audit activities for various models, including Artificial Intelligence & Machine Learning, across a variety of risk segments, subject to the same validation standards as specified in many regulatory requirements for Model Risk Management.
Protiviti's agile model development and insight validation methodology, shown below, directly accommodates Basel III, OCC 2011-12, rR 11-7, SR 21-8 and other regulations.

Process

Governance & Oversight

- Defined roles & responsibilities
- Management objectives
- Organisation structure
- Independence of development, validation & audit groups
- Issue resolution & escalation procedures

Model Environment

- Complete model inventory & linkages
- Comprehensive documentation
- Change control mgmt. for model maintenance & updates
- Model risk classification & control requirements
- Revalidation triggers & frequency

Machine Learning specific activities

Data & assumptions

Data Collection & Quality

- Review data collection & scrubbing processes
- Ensure data quality completeness, coverage, correctness & relevance
- Ensure data integrity during entry & system transfer
- Contingency, proxy use, imputation & backfilling procedures
- Review ongoing data extraction for reporting
- Data updating process & controls
- **Data labelling & sampling processes**
- **Train/Test split assessment**
- **Feature engineering**

Assumptions & Limitations

- Determine applicability & impact of assumptions
- Adequacy of documentation
- Justification of proxies & simplifications
- Review proxies & approximations
- Risk allocation & boundary decisions
- Appropriateness of time horizons
- Assumptions updating process & controls
- Determine & assess model limitations

Analytics

Conceptual Soundness

- Model rationale, intended use & domain of applicability
- Review theory, methodology & conceptual soundness
- Determine appropriateness of statistical tools
- Determine stability of parameter values
- Review analytics & mathematics
- Compatibility with other models used
- Review distribution fitting routines & use of correlations
- **Review choice of architecture, hyper-parameters, optimizers, regularization & activation functions**

Outcomes Analysis

- Benchmarking against other models & industry practice
- Error checking developer test results
- Performance testing
- Scenario/stress testing
- Back testing
- Convergence & stability testing
- Fragility & sensitivity testing
- Use out of sample data to determine model accuracy
- Comparison to actual behaviours
- **Interpretability**
- **Ensemble vs. individual model attribution**
- **Bias-Variance analysis**

Output

Ongoing Monitoring

- Ongoing monitoring program
- Analysis of overrides & overlays
- Performance threshold
- **Dynamic model calibration**
- **Additional model performance metrics**

Process Verification & Reporting

- Implementation testing
- Management risk acceptance
- User acceptance testing (UAT)
- Validating controls on model/computer code
- Timely & actionable reporting
- Output verification process & controls
- **Production readiness**

Effective Challenge to Model Development

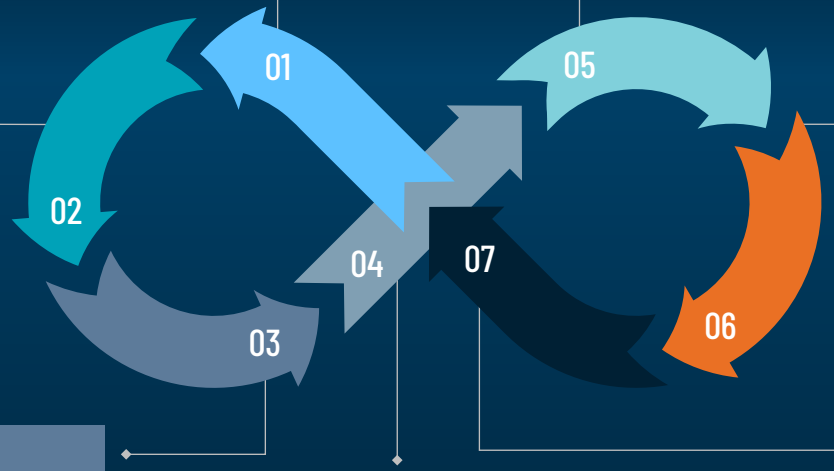
Risk Management and Compliance AI Use Cases

1. Frameworks, Methodologies, Governance Docs

- Standard Operating Procedure (SOP) Creator
- Risk Policy Creator
- Risk Policy Alignment and Benchmarking
- Document Comparison Accelerator (Policy vs Standard vs Procedure)
- Control to Control Framework Mapping

2. Risk Data Model & Technology

- Process Taxonomy Development
- Risk Taxonomy Development
- Control Taxonomy Development
- Taxonomy Benchmarking
- Risk KRI & KPI Development



3. Risk/Control Identification & Management

- Regulatory Extraction, Parsing, & Translation
- Risk Statement Development
- Risk & Control Rationalization
- Risk & Control Mapping Tool
- Regulatory Mapping & Comparative Analysis
- Process to RCSA Presumptive Mapping

4. Risk Assessment

- Risk & Controls Transformation
- RCSA: Effective Challenge Reporting Support
- RCSA: Inherent Risk Rationale Generation
- RCSA: Excel Add-in to support all risk & control AI tools
- Enterprise Risk Assessment Automated Tool

5. Monitoring & Testing

- Control Testing Walkthrough Preparation & Summarization
- Test Step Development (Control-and Outcomes-Based)
- Test Script Question Development
- Test Attribute Development
- Export Control Compliance

6. Issue & Change Management

- Emerging Issues Identification / Classification
- Issue documentation and risk rating
- Root cause tagging
- Issue duplicates identification & remediation clustering
- Issue Prioritization & Resource Optimization

7. Credible / Effective Challenge

- Credible Challenge & QA / QC
- Automated comparison of outcomes to P&Ps & Methodologies

protiviti

AI Related Lawsuits

Numerous lawsuits have been brought against generative AI companies regarding copyright and misuse. These lawsuits highlight pivotal issues and concerns such as licensing and copyright protections, and, more broadly, transparency and accountability of AI and their implications for creative industries.

GitHub, Microsoft and OpenAI

A class-action suit was filed against these companies involving GitHub's Copilot tool, which predictively generates code based on what the programmer has already written. The plaintiffs allege that Copilot copies and **republishes code from GitHub without abiding by the requirements of GitHub's open-source license**, such as failing to provide attribution.

Open AI and Microsoft

The New York Times is suing OpenAI for **copyright infringement.** The case, filed December 2023, alleges that millions of New York Times articles were used to train and develop OpenAI's chatbot and other technology, which now competes with the news organization as a source of reliable information.

Meta and Open AI

Sarah Silverman's lawsuit against Meta and OpenAI alleged copyright infringement and said ChatGPT and Large Language Model Meta AI (Llama) were **trained on illegally acquired data sets** with her work contained. The suit alleges the books were acquired from shadow libraries, such as Library Genesis, Z-Library and Bibliotek, where the books can be torrented.

Google

A class-action lawsuit is being brought against Google for alleged **misuse of personal information and copyright infringement.** Some of the data specified in the lawsuit includes photos from dating websites, Spotify playlists, TikTok videos and books used to train Bard.

Stability AI, Midjourney and DeviantArt

A complaint against these AI image generator providers was filed in January 2023. The plaintiffs alleged the systems directly **infringe on plaintiffs' copyrights** by training on works created by the plaintiffs and **creating unauthorized derivative works**.

OpenAI

Filed in June 2023, Authors Paul Tremblay and Mona Awad are suing OpenAI for allegedly **infringing on authors' copyrights**. The complaint estimated that more than 300,000 books were copied in OpenAI's training data.

Anthropic

A $3.1 billion lawsuit alleges that Anthropic used **pirated music to train its AI models,** highlighting the financial and legal risks of using unlicensed materials and driving discussions on fair compensation for rights holders.

Perplexity AI

Dow Jones and The New York Post accuse Perplexity AI of **incorporating copyrighted news content** into its outputs without consent, underscoring regulatory concerns around AI's reuse of journalistic work.

Claude (Anthropic)

In United States v. Heppner, the court ruled that AI-**generated documents used for legal defense were not protected by privilege,** illustrating the risks of using public AI tools in sensitive workflows and prompting a reassessment of AI compliance policies.

Richard Kessler

Director
AI Governance &
Risk Management

Tampa, FL & New York, NY

CONTACT

P: +1 862.225.4510
richard.kessler@protiviti.com

AREAS OF EXPERTISE

- AI & Emerging Tech Governance
- Operational Resilience & AI Governance Audits
- Data & Information Governance
- Infonomics & Data Asset Valuation
- Operational Resilience
- Operational Risk Management
- eDiscovery & Investigations
- Technology & Data Architecture
- Regulatory Compliance
- Data Privacy and Cybersecurity
- Third-Party Risk Management

INDUSTRY EXPERTISE

- Financial Services
- Consumer Products & Services
- Healthcare & Pharmaceutical
- Aerospace & Automotive
- Telecommunications
- Technology

EDUCATION

- B.S. Studies – Computer Engineering, Polytechnic NYU

PROFESSIONAL MEMBERSHIPS & CERTIFICATIONS

- Information Privacy Technologist (CIPT)
- InfoGov ANZ International Council

PROFESSIONAL EXPERIENCE

Rich is a Director in the Risk & Compliance Analytics practice based in Tampa and New York City and leads Protiviti's AI Governance practice. He has over 30 years of business experience, including 25 years in financial services, 7 in global advisory services across multiple industries, and three years as an entrepreneur in data & analytics and eDiscovery. Rich's focus areas include artificial intelligence governance, operational resilience, cyber resilience, business resilience, third-party risk, and technology risk management.

Before Protiviti and during the COVID-19 pandemic, Rich co-founded and built eDiscovery and data & analytics start-ups. Prior to his start-up experience, as part of a cybersecurity strategy and governance advisory practice, Rich worked on devising, managing, and delivering large-scale, multi-disciplinary data and information risk engagements. While in-house at a multi-national FSI, he envisioned, created, managed, and evolved the global information governance function, beginning with oversight of policies, guidelines, and standards, evolving into the organization's global data & information risk compliance controller. As controller, he worked to enhance and build out all three lines of defense to define and mature effective challenge processes, controls, analytics, and reporting across lines of business and supporting functions.

Previously Rich served in U.S. and global roles at large financial services institutions (FSIs).

MAJOR PROJECTS

- AI Governance Implementation – Created a comprehensive operating model and framework to assess and mitigate risks in agentic, predictive, and generative models and use cases, resulting in the development, deployment and continuous improvement of a tailored AI Governance system focused on governance as enablement.
- AI Governance Audits – conducted AI governance audits at a large US bank and several healthcare organizations, comparing existing policies, practices, and procedures associated with the AI use case lifecycle, compliance and risk management with NIST, ISO, and EU AI Act requirements; provided strategic recommendations for improvement
- AI Standard, and Controls design - conducted a thorough analysis of a large, multinational organization's existing information security and technology standards and controls. Developed an AI governance standard and revised and net new controls to mitigate AI risk, tailored to the client and its industry, incorporating leading practices risk management and governance principles, compliance requirements, and responsible AI design principles.
- AI Use Case Lifecycle Risk Control – Developed an end-to-end process for assessing and mitigating risk aligned to NIST, ISO, responsible AI principles and other standards to accelerate deployment of revenue-generating AI solutions.
- Regulatory Change Risk Remediation - Assisted a secondary mortgage market FSI with implementing their data and information risk program to remediate major risk items and to comply with significant anticipated regulatory changes. Orchestrated a multi-practice, multidisciplinary advisory approach as well as an internal program integration at the client to address 'all things data' holistically, including emerging technologies, operational risk, information governance, data governance, and business requirements for data assets. Mitigated major risk items within required timeframes.
- Data and Information Risk Program - Managed a multidisciplinary engagement for a large U.S. FSI to analyze policies, procedures, governance, tools, data catalogs, and related environmental components for consolidation and improvement, focusing on open risk items and regulatory requirements.
- Sensitive Data Management Innovation - For a large U.S. FSI, pioneered unique data scorecard approaches to data valuation, quality, and risk management, supporting the FSI's enterprise-sensitive data management function.

Face the Future with Confidence®

protiviti®
Global Business Consulting