ENTERPRISE ARTIFICIAL INTELLIGENCE

Building Trusted AI with Secure Data

Shannon Bell
David Fraser
Tom Jenkins

ENTERPRISE ARTIFICIAL INTELLIGENCE

Building Trusted AI with Secure Data

By Shannon Bell, David Fraser, and Tom Jenkins

First publication, November 2025

Published by

Open Text Corporation

275 Frank Tompa Drive

Waterloo, Ontario, Canada

N2L 0A1

(519) 888-7111

info@opentext.com | www.opentext.com

Foreword

James Arroyo OBE
Former Director for Data, British Foreign and Commonwealth Office and Director of The Ditchley Foundation*

We stand at a pivotal juncture in history—a time when the world's technological systems are converging, raising questions of power, trust, sovereignty and governance. Artificial Intelligence is redefining how decisions are made, how organizations operate, and how societies function. Yet progress in AI cannot be measured solely by technical capability. We must combine advances with policy clarity, ethical discipline, and a renewed understanding of what sovereignty means in the digital age.

This book, *Enterprise Artificial Intelligence: Building Trusted AI with Secure Data* addresses both the challenge and opportunity presented by AI. It recognizes that the next decade will not only be defined by who builds the largest models, but by who governs and uses data most effectively. Data is both the fuel and the foundation of modern intelligence systems. Much like energy or currency, it requires regulation, stewardship, and, above all, trust. The future of AI depends on how we manage the privacy, provenance, and sovereignty of that data. This will become critical as individuals, institutions, and enterprises move to add their own personal, proprietary and sovereign data to AI systems.

When I served as Director for Data at the UK's Foreign and Commonwealth Office, our task was not simply to digitize the institution and define the policies that would make digital transformation sustainable for decades to come. We had to ask difficult questions: *Who owns the data we rely on? Where does it reside? How is it shared, stored, and secured? How long should it be retained?* Those same questions now confront every enterprise, every government, and every citizen as AI systems become more autonomous and pervasive. AI's powers of inference mean that every atom of data can potentially bring insights in aggregate combination and that is game changing.

In conversation with leaders from technology, government, and civil society, it is becoming clear that **sovereign data policy is not a technical debate—it is a question of national and economic security**. In a world where the majority of data is locked behind organizational and governmental firewalls, sovereignty extends beyond mere compliance. It is about control, accountability, and the ability to act with confidence in a world of algorithmic decision-making.

* James Arroyo's views do not necessarily represent those of the Ditchley Foundation.

This book makes a compelling case for that philosophy. It argues that trusted data and responsible AI are two sides of the same coin, and that to build AI that is fair, explainable, and safe, we must ensure the data it learns from is well governed, contextual, and sovereign. Without privacy and data stewardship, AI risks undermining the very institutions it seeks to empower. Without innovation, governance risks becoming a hinderance that hinders progress. The task before us is to align trust and innovation so that one strengthens the other.

As you read, you'll see how the landscape of enterprise computing is being rebuilt from the inside out. Hyperscale infrastructure, sovereign clouds, and AI-driven systems are forming the backbone of the digital economy's industrial grid. But real advantage will belong to those who treat data not as a neutral commodity but as a constitutional principle—something to be protected, respected, and deployed responsibly.

The book's call to action is one I can warmly endorse: to move fast but to govern faster; to innovate boldly, but with purpose; to ensure that every digital advance strengthens public trust rather than erodes it. That is the essence of leadership in this new era of AI.

In the years ahead, the nations and enterprises that will win, by embedding AI in society and encouraging widespread and deep adoption, will be those that understand a simple but profound truth: **AI without trusted, sovereign, and well governed data is power without responsibility and perhaps legitimacy.** But when innovation and governance move in step—when privacy, accountability, and ethics are embedded in design—we can create not just intelligent systems, but intelligent societies.

The cognitive computing era is here—a time where trust is the foundation, and innovation is the engine. Its success will depend not on machines alone, but on our shared ability to define the principles that govern them. *Enterprise Artificial Intelligence: Building Trusted AI with Secure Data* offers a roadmap for that journey and an invitation to shape the future responsibly, together.

About the Authors

Shannon Bell

Shannon Bell is the Executive Vice President, Chief Digital Officer, and Chief Information Officer for OpenText, responsible for the company's IT and digital systems, data platforms, networks and communications, commercial and corporate cloud operations, as well as its security and compliance. She is an accomplished IT leader with over 25 years of international experience in technology transformation and large-scale integrations. Prior to OpenText, she held a senior leadership role at Rogers Communications, spearheading the technology integration of the Shaw acquisition. Her career has included roles at Amdocs, NewStep Networks, MetaSolv Software, Axiom Systems, and Newbridge Networks. Shannon holds an MBA from the University of Surrey and undergraduate degree from Carleton University.

David Fraser

Major-General (Ret.) David Fraser has served as a director of OpenText since September 2018. One of the most decorated generals in Canadian Armed Forces history, he is a recipient of the Order of Military Merit, among others. In 2006, he was the commander of the Multinational Brigade for Regional Command South in Afghanistan and led Operation Medusa, the largest combat engagement of Canadian Armed Forces in more than fifty years. General Fraser also served as the Commandant of the Canadian Forces Staff College. After his retirement from the military, he served as an executive with three different corporations, among them Blue Goose Pure Foods, and has experience leadership on both the battlefield and in the boardroom. David co-authored *The Anticipant Organization*, a survival guide for leading organizations in a world of constant disruption, with Tom Jenkins and Mark J. Barrenechea.

Tom Jenkins

One of Canada's leading experts on innovation and digital technologies, Tom Jenkins is the Chair of OpenText Corporation, the largest software and cloud company in Canadian history and one of the most successful internet companies in the world. Tom has served or continues to serve on the boards of OpenText Corporation, Manulife Financial, Thomson Reuters, TransAlta Corporation, BMC Corporation, and Slater Steel. He also served as the Chair of the National Research Council of Canada. He received his commission as an officer in the Canadian Armed Forces and as the Honorary Colonel of an infantry regiment and a fighter squadron in the Canadian Armed Forces. He was the 10th Chancellor of the University of Waterloo, and he was inducted as a Companion into the Canadian Business Hall of Fame. Tom is a recipient of the Federal Republic of German Order of Merit (Knight's Cross), and he is an Officer of the Order of Canada. Tom has authored many business books on digital innovation and co-authored *Ingenious: How Canadian Innovators Made the World Smarter, Smaller, Kinder, Safer, Healthier, Wealthier, and Happier,* with David Johnston, the former Governor General of Canada.

Acknowledgements

The authors would like to thank the following people for their time, energy, and insight:

Michael Acedo, DeeDee Andrews, James Arroyo, Savinay Berry, Lev Dranikov, Paul Duggan, Joe Dwyer, Adam Hennessy, Bita Houshmand Rabiee, Michelle Kelly, Anupam Khazanchi, Edward Kiledjian, Mark L'Heureux, Stephen Ludlow, James McGourlay, Sandy Ono, Sunnie Rothenburger, Scott Schultz, along with Elizabeth Chestney-Hanson, editor, and Stephen Ksiadz and Kevin Sy, for layout and design.

Contents

Foreword 3
About the Authors 5
Introduction 8

Chapter One
The Evolution of Enterprise Data 15

Chapter Two
The Rise of Enterprise Artificial Intelligence 35

Chapter Three
The Intersection of Data and Artificial Intelligence 54

Chapter Four
Making it Secure—The Importance of Cybersecurity 67

Chapter Five
Data Governance—The Foundation of Trusted Enterprise AI 83

Chapter Six
The Governance of EAI 100

Chapter Seven
The Architecture of Sovereign EAI Implementations 115

Chapter Eight
Putting Agentic AI to Work 132

Chapter Nine
The Management of EAI Applications 149

Chapter Ten
The Creation of AGI from Agentic AI 164

Chapter Eleven
The Future of EAI and Operations Management 176

Appendicies
Endnotes 192
Glossary 196
Works Cited 206
Index 212

Introduction

Welcome to the Cognitive Computing Era

We're living through another major turning point in technology—the beginning of the Cognitive Computing Era, driven by the rise of Enterprise Artificial Intelligence (EAI). What started as a digital revolution has evolved into something far more dynamic: a world where data doesn't just inform decisions; it influences technology to interpret, learn, and act.

Over the past few decades, the ground beneath the IT industry has shifted. The COVID-19 pandemic forced entire economies to digitize almost overnight. Cloud adoption, remote work, and automation leapt forward in months instead of years. The result? A completely re-wired business landscape where digital infrastructure isn't just an operational layer—it's the heartbeat of the organization.

Not long ago, enterprise IT meant makeshift servers running in overheated closets, where one bad line of code could crash an entire system. Today, those fragile setups have been replaced by hyperscale infrastructure—global, resilient, and endlessly scalable. On top of that backbone, a new intelligence has emerged. Agentic Artificial Intelligence (AI) can reason, adapt, and respond in real time. Work that once took teams of developers, marketers, or analysts can now be orchestrated instantly across millions of users.

Classic Enterprise Applications Are Transforming

This is the new inflection point: the convergence of hyperscale computing and agentic AI. Hyperscalers and sovereign clouds have become the industrial grid of the digital economy—the power that runs everything else. Layer AI on top, and you get a nervous system for modern business, one that doesn't just store and process data but anticipates and acts on it. For enterprises, this isn't just another wave of innovation; it's a complete redefinition of how work, value, and intelligence flow.

Classic enterprise applications are changing fast to keep pace. Hyperscalers like Amazon Web Services, Google Cloud, and Microsoft Azure are moving in on the traditional B2B stronghold, offering powerful, low-cost cloud services that rewrite the rules of the game. For years, what kept those systems safe were the things that made them hard to copy—their complex workflows, their custom interfaces, and their mountains of historical data locked deep in archives. But that's exactly where the new pressure is building.

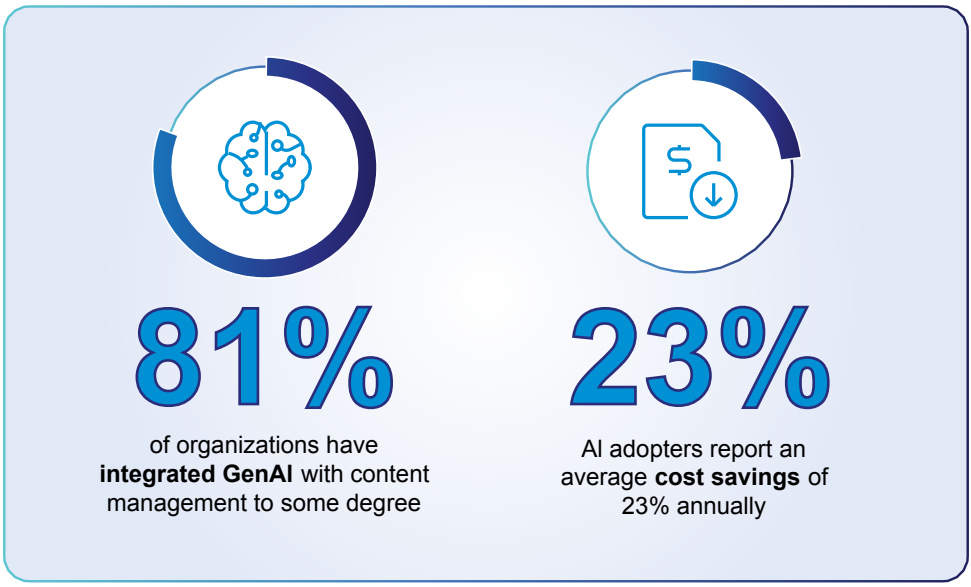
Those old defenses aren't holding the way they used to. The user interfaces and configuration tools that once felt unique can now be replicated in minutes. And the data sitting quietly in archives—the years of transactions, interactions, and records—has become the fuel that every AI model wants to learn from. Agentic AI doesn't just compete with enterprise systems; it learns from them, imitates them, and, in many cases, outpaces them.

The real advantage now isn't in building taller walls; it's in building smarter foundations. What makes an enterprise resilient today isn't the size of its software stack, but how well it governs, protects, and activates the data inside it. That's where real intelligence—and real differentiation—begins.

Leaders advancing cognitive computing must balance trust and innovation, recognizing that secure, well-managed data underpins trust, while AI drives progress and innovation. Trusted data ensures confidence, reliability, and compliance as AI unlocks new solutions and efficiencies. Without strong data governance, rapid AI advancement can compromise privacy and security; but without innovation, progress stalls.

In this era, trust and innovation must be in sync—aligning robust data practices with bold AI initiatives enables organizations to responsibly harness transformative technologies, ensuring every advancement is anchored in public trust and ethical standards.

Simply put, only trusted data can power truly trustworthy and effective AI.



Early Adopters Are Already Benefiting from the Adoption of Integrated AI[1]

The next decade will belong to the organizations that understand this shift. The ones that treat data not as a byproduct of business, but as its operating system. The ones that know data can't be powerful unless it's also trusted, governed, and secure. AI will transform every industry, but only if it's built on a foundation strong enough to carry it.

Consider this: In May 2025, Salesforce announced it would acquire Informatica for approximately US $8 billion—a signal event that tells us exactly where the battle lines of enterprise software are shifting. *Why did this deal make sense?* While Salesforce relied on

external systems for their critical data, their data integration capabilities were weak. And they wanted to close the data-integration gap so that AI could run on governed, contextual information.

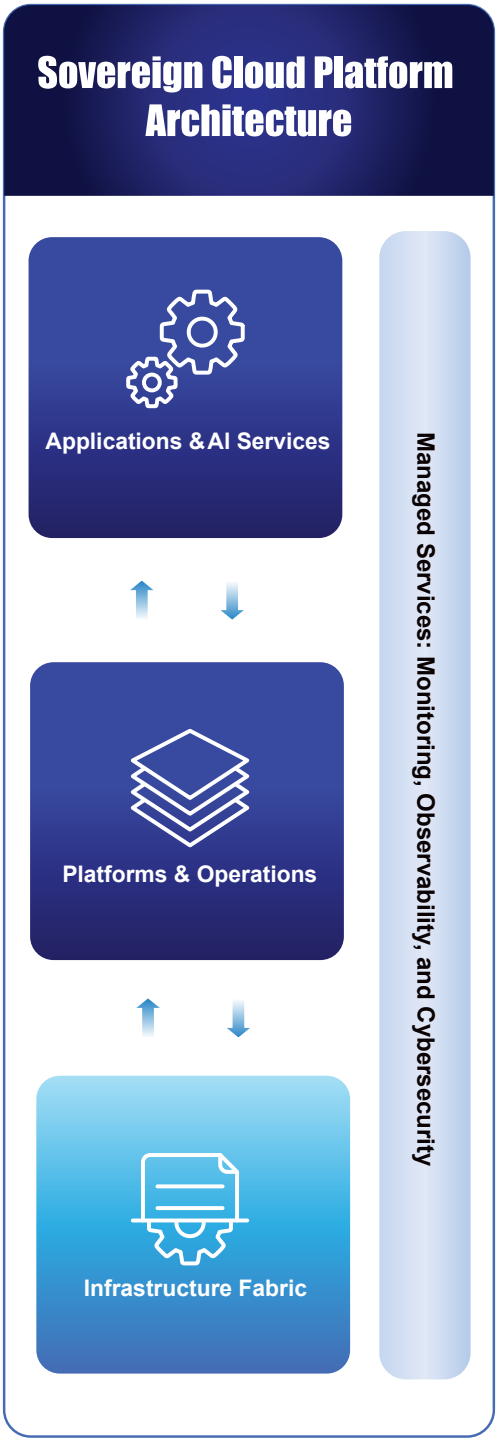
Salesforce recognized that the future of AI depends on access to secure, structured, and unstructured data—the kind of data that lives deep within organizations, not out in the open web. This is especially true for the training of *agentic AI* systems, which are expected to become the cornerstone of global enterprise productivity in the decade ahead. But here's the challenge: most of the world's valuable information doesn't exist on public data sources. It sits inside corporations, governments, and institutions—governed, protected, and often, regulated by law.

Public chatbots like ChatGPT, Claude, and Perplexity have already trained on nearly everything that's freely available—Reddit posts, Wikipedia pages, and other open repositories. As they reach the limits of that content and attempt to learn from more specialized information, they collide with copyright, privacy, and data ownership boundaries. This is *proprietary data*—the information organizations have sovereignty over—and it's increasingly governed by strict privacy and security regulations, from municipal and federal frameworks to global standards set by the UN and NATO.

In reality, more than 90 percent of the world's data sits behind corporate and government firewalls.[2] It's not just hard to reach; it's protected by design. Gaining access requires permission, compliance, and governance. This is where Enterprise Information Management comes in: document and records management systems, workflows, and rules engines that control who can see what, when, and why. For enterprise agentic AI to evolve responsibly, it will need to learn not just from information, but within the guardrails of trust that systems like these provide.

When a company trains or fine-tunes its Large or Small Language Model on data it doesn't have the right to use, it's basically teaching the machine someone else's homework—and that never ends well. If that data turns out to be proprietary, the fallout isn't a quick fix; it's a full reset. The organization that owns it can demand the AI be "untrained," which in today's world means starting from scratch. You can't just pluck out one bad data source—you have to roll the whole thing back to where the mistake began. That can cost millions of dollars and months of lost time. In some cases, it can take a promising AI program right off the board. In short, when it comes to governing data to train effective AI models, organizations need to measure twice and cut once. That's why understanding data sovereignty has become mission critical.

Every organization holds something too valuable to lose: its institutional knowledge and data, the "keys to the castle." It's what makes your business yours. Hand that over to the wrong system or the wrong partner, and you risk watching your own information come back to you, re-packaged and re-sold. Governments see that risk too, which is why they're racing to set guardrails. New AI and data protection laws are on the horizon—and they'll make General Data Protection Regulation (GDPR) look like the opening act. They'll reshape how companies store, share, and train on data, especially when personal or sensitive information is in play.



Organizations Require Sovereign Data

To get AI-ready, organizations need to understand the three kinds of datasets that fuel intelligent systems and manage them responsibly:

1. Human-generated content we create every day: documents, emails, presentations, images, videos, and conversations, or what we call the living record of how an organization thinks.
2. Machine-generated content: log files, alerts, and telemetry from IT systems, networks, and security tools—the constant hum of how an organization operates.
3. Data that flows between organizations: transactions, supplier exchanges, and B2B integrations. This is the connective tissue that keeps the economy running.

Agentic enterprise AI needs all three datasets to function with real business context. The shift ahead is from *content in context* to *AI in context*—where intelligence doesn't just process data; it understands relationships, intent, and value in order to effectively take action and learn. And just like the information it learns from, AI itself must be secure, governed, and compliant. Those aren't just technical standards; they're the foundation of trust that determines whether AI can be safely put to work inside the enterprise.

The real question isn't *whether* you'll share your data; it's *how* you'll stay in control of it.

True sovereignty means knowing where your data lives, who's accessing it, and how it's being used—not once, but continuously. You need secure ways to bring Generative AI (GenAI) inside, where your information already lives—inside your governed, secure systems. Let your people chat with their content: find it, summarize it, and build on it without ever breaking governance rules. And transform analytics into something you can simply ask about in plain language. And safely introduce other products that carry that same intelligence into cybersecurity, application management, and beyond.

With secure, governed, sovereign data, you don't have to hand over your crown jewels to innovate. You can use AI confidently. Because in the era of responsible intelligence, the smartest organizations aren't the ones who feed AI the most data. They're the ones who know which data they can trust.

The Path Forward: A Call to Leadership

As we've discussed, the next era of innovation won't be led by those who move the fastest, but by those who move the most responsibly. It is the intersection of trust and innovation.

Every executive decision, every line of code, every AI model now carries a moral dimension—because information has power, and how that power is used will define the decade ahead.

This is the moment when leaders in enterprise, government, and industry will be required to treat their data and information not just as a resource, but as a responsibility. To strengthen data foundations, to embed governance into design, and to make security the default, not the exception. The future of AI depends not only on how much we can automate, but on how deeply we can trust the systems—and the data—we build it on.

Across sectors, we see the same challenge emerging: the need to transform at speed without sacrificing control. The organizations that succeed will be those that combine the courage to innovate with the discipline to govern. They'll be the ones that protect privacy as fiercely as they pursue insight, that make transparency a competitive advantage, and that build Enterprise AI capable not just of reasoning—but of earning trust.

This is where readiness meets responsibility. Where digital ambition becomes accountable intelligence. And where the most transformative technologies are also guided by principle.

Just as trusted data forms the bedrock and AI innovation lights the path forward, the chapters ahead will unpack data frameworks, AI governance models, and key considerations for both sovereign and non-sovereign data architectures. At the end of each chapter, you'll find a "Fast Five Download" to distill the essentials for quick reference, ensuring you're prepared to build, govern, and innovate with confidence.

The decade of responsible intelligence has begun. Together, we can build it—securely, ethically, and for the greater good.

Chapter One

The Evolution of Enterprise Data

Not long ago, enterprise data was treated like an attic box—filled with old records, reports, and compliance paperwork. It was something you stored, not something you lived with. You climbed up to the attic only when you needed to check a number, prove a point, or satisfy an auditor. But today, data lives on the main floor. It's awake, wired, and running the business in real time. It informs every decision, powers every transaction, and, if placed out on the street—or made public—it can reveal more than you ever intended.

But keep this data private and protected, and it will drive your competitive edge.

Artificial intelligence doesn't exist apart from data—it *is* data, remembered, organized, and activated in motion. The enterprise is the same old house, but with the attic emptied and the brain downstairs. That's why the privacy and security laws that govern data must now be used to govern AI. As we move into the Cognitive Era and AI develops at faster rates, organizations and agencies will be required to treat information as a managed asset across its lifecycle, not a passive archive.

This chapter breaks down enterprise data—what it is, how it's used, and how it can be optimized with an AI engine and governed by an Enterprise Information Management (EIM) platform in the cloud. We'll explore AI as the intelligence layer of your enterprise's information fabric, embedded into content services and analytics and stitched together by your operational business processes.

The Hidden Web

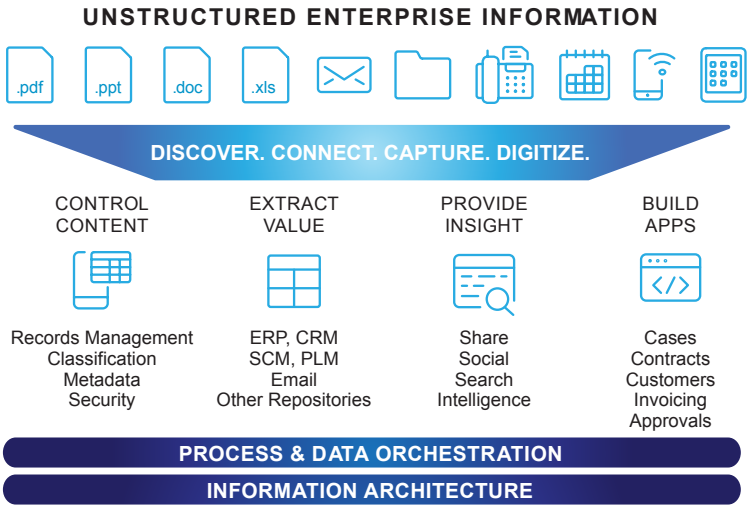
The Real Landscape: 10 Parts Private, 1 Part Public

Most of the world's useful enterprise information lives behind the firewall. IDC reports that an organization's unstructured content—emails, reports, documents, images, recordings—makes up almost 90 percent of all data.[3] This private data vastly outweighs the public web content that fuels today's generative AI. Yet much of it remains unmanaged, fragmented, or trapped across silos.

That imbalance matters. The ratio of private to public data is roughly 10 to 1, which means the vast majority of the world's intelligence potential is hidden from public models. The real competitive advantage sits inside the enterprise—in contracts, design files, invoices, maintenance logs, clinical notes, and correspondence—provided it's governed, connected, and trusted.

Enterprise Information Management was designed for exactly this challenge. EIM unifies, secures, and operationalizes enterprise data so it can be used responsibly and strategically. Managing information well means knowing where it lives, who owns it, who can see it, and when it changes.

But not all data is created equal. Structured data—numbers in a database—can be sorted, queried, and reported with ease. Unstructured data—words, images, video, voice—resists that order. It requires indexing, context, and classification. That's why the technologies that manage numbers and the technologies that manage words must differ.



Unstructured Enterprise Information

To understand the value of unstructured data, consider the scale of what sits beneath every business record. One employee might appear as a row in an HR database—but is also linked to thousands of documents: resumes, contracts, pay slips, correspondence, and performance reviews. An asset—whether an aircraft engine or a power turbine—might exist as a single record in an Enterprise Resource Planning (ERP) system, but it's surrounded by a dense web of manuals, quality reports, inspections, and maintenance logs.

Together, structured and unstructured information form the deep or hidden web of the enterprise—the data that's invisible to public search but vital to daily operations. Every digital artifact contributes to this hidden layer: every email, report, draft, image, and chat thread. As mobile and collaboration technologies have moved inside the enterprise, the variety and velocity of content has exploded. EIM evolved to capture, classify, and govern this complexity—to make sure that what's created is also understood, retrievable, and compliant.

But while EIM brought order to enterprise information, AI is now exposing its next frontier. Generative models, trained mostly on public data, can write, summarize, and predict—but they can't act within a business. They lack the governed, permissioned, internal data that powers real decisions. Without it, AI can't perform agentic tasks like approving invoices, scheduling maintenance, or interpreting engineering drawings.

To move beyond this plateau, AI needs what information management has offered for decades: a framework of secure, compliant, permissioned enterprise data. Only then can an AI operate responsibly inside the firewall, not just imitate intelligence from the outside.

Managing this data means knowing where it lives, who owns it, who can see it, and when it changes. These fundamentals of EIM—permissions, metadata, and lifecycle control—are what make enterprise information trustworthy. These functions must now be applied to AI.

Where to start? Let's take a look at where enterprise information lives.

Where the Data Lives: Types of Enterprise Information

Every organization produces information for a handful of reasons: to record operations, enable communication, preserve knowledge, comply with regulations, and deliver value to customers. What began as structured recordkeeping—transactions, invoices, and inventory ledgers on mainframes—expanded into a web of communication and collaboration: emails, shared documents, and digital workspaces.

Today, these information streams can be understood as three broad classes of enterprise data that matter differently for AI: human-generated content, machine-generated data, and transactional or business-network data. Each has its own structure, governance requirements, and role in AI model training. Together, they form the foundation for agentic intelligence inside the enterprise.

Human-Generated Content: The Language of the Enterprise

Human-generated content includes documents, emails, scans, multimedia, case notes, and other forms of communication. It is rich in meaning and nuance but inherently unstructured. This is the content management domain—where information carries personal, contextual, and often sensitive data that demands careful classification, metadata tagging, and lifecycle management.

These materials contain the policy, precedent, and language that define how a business operates. Training AI on such content requires de-identification and strict governance, but the payoff is significant: this is where intent, business rules, and institutional knowledge live. When properly managed, unstructured content becomes the foundation for Retrieval-Augmented Generation (RAG), prompt libraries, and natural language reasoning—capabilities that allow agentic AI to act with understanding, not just automation.

Machine-Generated Data: The Enterprise Nervous System

Machine-generated data comes from the systems that power the organization—logs, telemetry, performance metrics, and monitoring streams. It's high in volume, velocity, and structure, and it tells the story of what the enterprise is doing in real time. This is the domain of observability and operational awareness, where every event and anomaly leaves a trace.

Machine data provides the causal signals AI needs to act intelligently on infrastructure, detecting patterns, predicting failures, or recommending corrective actions before users notice. Its challenges lie in scale, retention cost, and the need to map raw signals to business context. When combined with policy and human content, this data enables an AI agent to respond autonomously while maintaining auditability and compliance.

Transactional and Business-Network Data: The Source of Truth

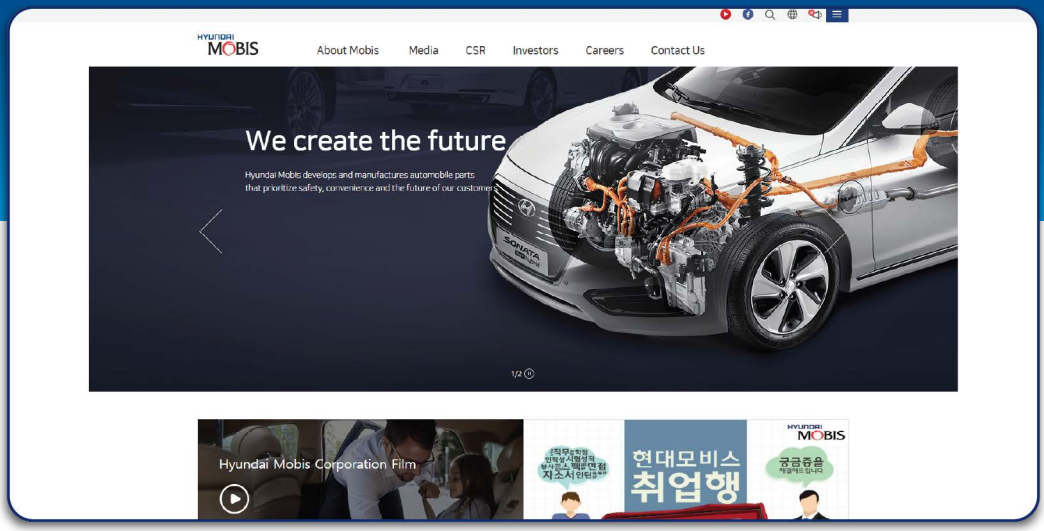
Transactional data—purchase orders, invoices, shipping notices, and other structured messages—represents the legal and economic truth of business operations. These records define the obligations between companies and are essential for compliance, taxation, and audit. Because they follow well-defined schemas and carry high semantic precision, they provide a reliable foundation for reasoning without ambiguity.

For agentic AI, transactional data is what anchors decisions in fact. It enables agents to reconcile financial records, forecast cash flow, and identify exceptions in complex supply chains without fabricating results. Integrating this structured information with the unstructured and operational layers creates a full view of the enterprise: what's happening, why it's happening, and what to do next.

In the following feature, MOBIS, a car manufacturer, created a parts production system designed to ensure quality and savings throughout the supply chain—informed by analytics and business intelligence.

Case Study

MOBIS



MOBIS

Headquartered in Seoul, South Korea, with subsidiaries in approximately 40 countries worldwide, MOBIS manages the supply chain for automobile industry heavyweights Hyundai Motor Company and Kia Motors. The company created a parts production system designed to ensure quality and savings throughout the supply chain—from purchasing and inventory to sales and logistics—helping its clients stand out in the competitive automobile industry. MOBIS Parts Australia Pty Ltd. (MPAU) is the automotive supplier's Australian subsidiary.

The automotive industry has ongoing competitive challenges, with other brands coming up with new products, new sales strategies, and new pricing methodologies. As a result, MPAU has to ensure that they have adequate systems and technologies in place to keep products competitive and operations agile. To react responsively to changing demands or competitors' offerings, the company needed a new business intelligence system that would support real-time inventory and dealer network reporting, monitor sales performance and pricing offers from vendors, and offer analytical capabilities to predict future sales and inventory requirements.

> *From a logistics side, we are able to get clear visibility on business operations by integrating information from the back end to the front end of the BI system, allowing us to analyze the information coming from the back-end system.*
>
> IT MANAGER, MPAU

After testing several systems, MPAU ultimately chose an Analytics Suite based on its robust functionality, as well as its ease of use. The latter was a key factor to ensure end users would take to the system naturally to deepen distributor engagement by integrating seamlessly and intuitively into the day-to-day operations of approximately 140 to 160 users and dealers. The solution was able to integrate with data sources throughout the MPAU operations and dealer network with dashboards that offered each department, from inventory and warehousing through to sales and logistics, a snapshot into their daily activities.

Analytics capabilities give the company competitive advantage, with the ability to not only view historical sales and inventory but to forecast future needs as well. Now, instead of relying on a cumbersome reporting process and inaccurate predictions, users can compare historical data to current sales information in real time and project future sales. The result is a more efficient business environment with informed decision-making that allows users to access and interact with data more reliably and the company to operate with greater agility in a competitive market.

When Information Types Work Together

As illustrated in the above case study, the real power of enterprise data emerges when different types of information converge. When human knowledge, machine telemetry, and business transactions are governed, connected, and contextualized, they form the living architecture of an intelligent enterprise.

Consider a finance shared-services group using an AI assistant to reconcile mismatched purchase orders and invoices. The assistant analyzes invoice images and OCR (Optical Character Recognition) output (in simpler terms, human-generated content), then checks them against ERP transaction records (transactional data), and reviews system logs showing when invoices were received or approved (machine data). With a unified layer of metadata—capturing document lineage, access rights, and timestamps—the AI assistant can generate a defensible recommendation that reduces cycle time and preserves audit integrity.

In another example, a legal department agent preparing litigation hold letters draws from policy documents and prior communications (human-generated content), uses filing timelines and case metadata (transactional data), and verifies server access logs to confirm custodianship (machine data). The result is a draft that's both accurate and compliant, produced in minutes instead of days. The same principle plays out at scale in real organizations, as illustrated in the following case study.

Case Study

An Independent Energy Company

An independent energy company, which is also a state-run public service, serves more than 150,000 customers. The company needed a way to manage growing volumes of information while maintaining compliance across multiple regulatory regimes. “As a high-performance company, we need to ensure that the right information is in the right place at the right time so we can make the right decision,” explains the Corporate Records Manager at the company. “To do this we have to incorporate compliance mandates, overcome information organization challenges, and constantly improve business processes.”

By extending Enterprise Information Management with AI-driven search and automation, the company can now locate and act on information faster than ever. Intelligent retrieval surfaces both structured and unstructured content—emails, spreadsheets, reports, and PDFs—within one secure environment. AI summarization helps employees interpret large sets of engineering data and regulatory records, while machine learning models flag retention issues and automate compliance checks. The company now manages compliance and performance in tandem, using AI to make governance more proactive and less manual.

EIM and enterprise AI together allow the energy company to balance regulatory obligations with operational agility—turning information governance into an engine for insight rather than a constraint. These examples, from automated finance reconciliation to enterprise-wide energy management, illustrate the same truth: AI and automation deliver value not from any single dataset, but from the relationships between them. When data is unified, trusted, and contextualized, it becomes more than information—it becomes intelligence.

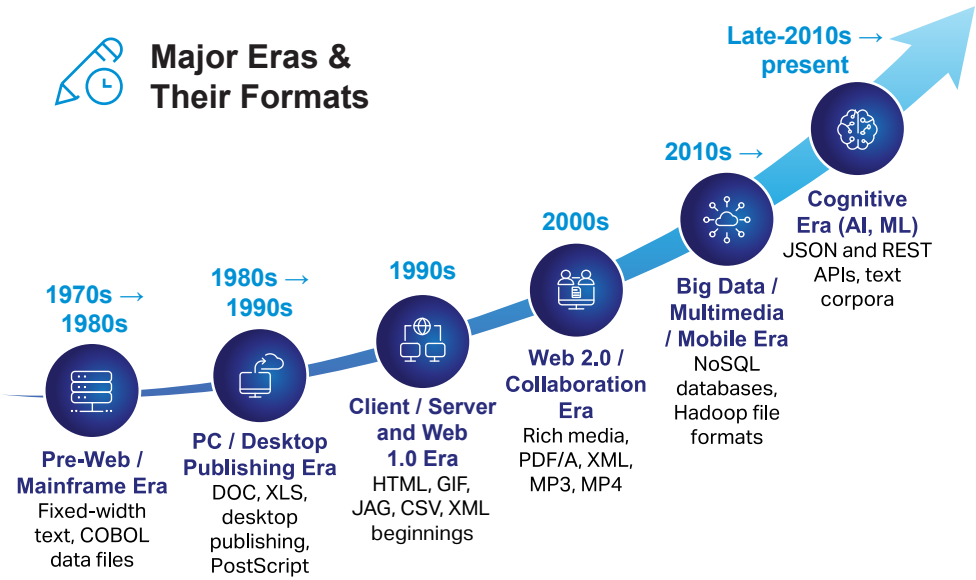
Every organization's digital story begins with its formats. The files, records, and containers we use to store information reflect the technologies and priorities of their time—from punched cards and print spool files to APIs built in JavaScript Object Notation (JSON) and AI-ready datasets. Looking back across fifty years of enterprise information reveals a simple truth: every leap in computing created a corresponding leap in content.

The Pre-Web / Mainframe Era (1970s–1980s)

The first generation of enterprise data lived inside the mainframe. It was structured, rigid, and optimized for machine efficiency. Fixed-width text records, COBOL (Common Business Oriented Language) data files, and indexed ISAM (Indexed Sequential Access Method) formats replaced handwritten ledgers and paper journals. Storage was scarce, so every byte counted.

Batch processing dominated, and the focus was on throughput rather than interaction. Systems were designed to "process overnight," producing printed reports and spool files the next morning. Encoding schemes like EBCDIC (Extended Binary Coded Decimal Interchange Code) kept everything proprietary and tightly coupled to the hardware that produced it.

These early systems established the foundation for structured data discipline. They introduced schema control, versioned record formats, and the beginnings of what would become metadata—the idea that each field had meaning. The mainframe's rigidity forced organizations to think of data as an asset long before the term "data governance" existed.



Major Eras and the Formats They Produced

The PC and Desktop Publishing Era (1980s–1990s)

The arrival of the personal computer brought liberation, along with fragmentation. Suddenly, employees could create content independently of the mainframe. WordPerfect and early Microsoft Word® documents, spreadsheet files, and desktop publishing outputs proliferated across offices and floppy disks.

Information creation shifted from corporate centers to individual desktops. Reports, memos, and presentations multiplied in new digital formats like DOC, XLS, and PostScript. For the first time, documents were visual, editable, and printable at scale.

This democratization of content fueled productivity but fractured control. Data that once lived in centralized systems was now scattered across hard drives and file shares. This era marked the birth of the "content explosion" that would eventually drive demand for enterprise-wide content management systems.

Client/Server and Web 1.0 (1990s)

As organizations networked their systems, information began to move online. The rise of the web introduced HTML pages, GIF and JPG images, and early XML for structured exchange. Internal intranets mirrored public websites, and the challenge shifted from creation to discovery.

Client/server architectures allowed employees to share databases and applications, while browsers made it possible to publish information universally. The need for indexing and search sparked the first metadata models and document management systems. This brought about the "search revolution," which was characterized by information's need for lifecycle thinking—creation, storage, retrieval, and disposal.

Web 1.0 turned corporate knowledge into something dynamic, connected, and increasingly complex. It also laid the groundwork for governance: once you find data, you need to decide who else should access it.

Web 2.0 and the Collaboration Era (2000s)

The early 2000s introduced a more social and participatory web. Rich media, PDF/A archival standards, XML and JSON formats, and multimedia encodings like MP3 and MP4 became common currency.

User-generated content and collaboration tools entered the enterprise. Email archives, portals, and wikis joined traditional records systems. Content management evolved to handle persistent, shareable documents that crossed departmental and even organizational lines.

This was also the era when regulatory pressure met digital scale. The Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), and other compliance regimes forced companies to prove not only what they knew, but when and how they knew it. This convergence of regulation and collaboration cemented the need for records management, version control, and policy-driven archiving—core pillars of modern EIM.

The Big Data, Multimedia, and Mobile Era (2010s →)

By the 2010s, information had outgrown documents. Streams, telemetry, and time-series data flowed from mobile devices, sensors, and apps. New analytic file formats—Avro, Parquet, ORC (Optimized Row Columnar)—optimized for scale and speed became standard in data lakes and cloud warehouses.

Video, voice, and large image repositories expanded exponentially as smartphones and digital experiences became the norm. Object storage and content delivery networks redefined the concept of "file," turning everything into an addressable blob with metadata wrappers.

This proliferation of data gave rise to the "hidden web," the vast universe of unstructured content behind the firewall. It was both an opportunity and a liability for the enterprise; an opportunity to mine with analytics and apply AI training but risky in terms of cost and compliance.

The Cognitive Era (Late 2010s → Present)

Today's content landscape is fluid, interconnected, and multimodal. Data moves not just between people and systems, but between machines. APIs—especially REST (Representational State Transfer) and GraphQL—interconnect microservices. Application-specific bundles (containers, notebooks, structured logs) represent new hybrid document types.

This era is defined by interoperability and automation. Information is both consumed and produced by AI, machine learning, and digital agents. Tokenized text corpora, embedded metadata, and semantic tagging enable retrieval-augmented generation and contextual reasoning.

Where earlier eras optimized for format efficiency, today's focus is meaning. The modern enterprise must unify structured and unstructured data across every modality—voice, image, text, and transaction—into governed ecosystems that support both analytics and intelligent action.

In the Cognitive Era, formats aren't static; they're interfaces between human intent and machine understanding. The same lifecycle that once applied to documents—capture, manage, process, search, archive—now extends to knowledge itself.

Across each era, the theme remains consistent: technology changes, but the need for trust and context endures. From COBOL reports to cloud APIs, every new format redefines not just how data is stored, but how it's governed, shared, and understood. The lesson is simple: information management evolves with the medium. What began as control over files has become control over intelligence. The formats of the past were about legibility; the formats of the future are about learning.

Why Governance Comes First

Enterprise Information Management has always been about that trust. It organizes the information estate across capture, manage, process, search, and archive—tying content lifecycle directly to the business processes that create it. Done well, governance improves insight, reduces risk, and lowers compliance costs. It's not an add-on to AI strategy; it' the precondition.

Discover how UBS has centralized its information in an EIM platform to govern its information and comply with regulations in the case study below.

Case Study

UBS

Certification Process at UBS

In response to the compliance requirements posed by Sections 302 and 906 of the Sarbanes-Oxley Act, UBS, one of the world's leading financial institutions, implemented an internal certification process for financial reports, in which senior executives formally certify their financial figures and processes using a 'subconfirmation' process.

During the internal certification process, appropriate persons are notified via email when their input is required and are then granted personalized access to the relevant documents on the UBS intranet. All relevant processes are archived and tracked in a log file. The CEO and Group Controller—generally the CFO—issue a final certification for the Security Exchange Commission only when all internal processes have been completed.

The UBS corporate governance portal enables the company's business managers worldwide to collaborate in developing internal and external business reports. Relevant departments have access to a complete overview and status of the certification processes at all times. All related processes have been automated and simplified, expediting the certification process.

Mapping EIM to AI: Internet, Intranet, and Extranet

EIM provides a useful mental model for understanding AI maturity. Just as information moves from public to private domains, AI evolves from broad generalization to contextual intelligence.

- **Internet = Generative AI**
  The outermost layer represents public knowledge—open data and generalized language models that are excellent for ideation, first drafts, and exploration. Generative AI works much like the internet itself: vast, connected, and creative, but limited by a lack of organizational context or precision.
- **Intranet = Agentic AI**
  The middle layer mirrors an organization's internal network. Here, data is private, permissioned, and workflow-aware. Agentic AI can reason over internal systems, act on approved workflows, and make bounded decisions under governance controls. This is where AI stops merely describing and starts doing—automating tasks, augmenting staff, and enforcing policy through action.
- **Extranet = Artificial General Intelligence (AGI)**
  The innermost layer represents the future frontier, where AI collaborates safely across organizations and systems. Like an extranet connecting trusted partners, AGI would reason fluidly across boundaries—sharing insights while maintaining trust and compliance between entities.

As AI moves inward—from public to private to shared domains—its context, accuracy, and value increase. But so too does the need for governance. The deeper the intelligence operates within your organization's core data, the greater the responsibility to secure, audit, and align it with human and regulatory boundaries.

By the Numbers: The Energy Cost of Training AI

- Training a foundational model like GPT-3 consumed approximately **1,287 MWh** of electricity, emitting around **502 metric tons** of CO2–roughly equivalent to the annual emissions of 112 gasoline-powered cars.
- In 2024, a study found that up to **30%** of the power used during large language-model training runs is wasted through inefficient scheduling and hardware usage, meaning the same outcome could be achieved with significantly less energy.
- Projections indicate that AI training demand could consume **eight terawatt-hours (TWh)** in 2024 and reach **652 TWh** by 2030, representing an over **80-fold increase** in electricity use in just six years.

Data Quality and the Physics of Learning

"Garbage in, garbage out" has never been more relevant. The accuracy of any AI model depends on the quality of the data it consumes. In statistical terms, more data improves probability—*if* that data is relevant, consistent, and clean. Modern machine learning doesn't simply add volume; it learns to assign weight to the signals that matter most through repeated training and feedback. Over time, the system develops a sense of what's meaningful and what's noise—much like a human learning through experience.

When those inputs are incomplete, inconsistent, or poorly governed, the model fills the gaps on its own. That's when hallucinations happen: confident, convincing answers that are entirely wrong. As model complexity increases, so does the risk of these errors. The antidote is curation—grounding AI in governed, high-integrity data.

There's also a cost-to-quality ratio at play. The better the data, the less energy and time a model wastes in training and inference. As AI models grow larger and compute demands rise, the physics of learning becomes a matter of efficiency as much as accuracy. Well-curated data reduces redundancy, minimizes reprocessing, and reduces the deployment footprint of AI operations. The new figure of merit lies in the balance between data quality, training time, and energy consumption—a reminder that better governance isn't just safer; it's smarter and more sustainable.

Why AI Must Follow Data's Rules

Traditional software processed data and moved on. AI doesn't. It remembers. Every piece of information it encounters becomes part of its internal landscape, shaping how it reasons, responds, and behaves in the future. That memory makes AI different—and it makes governance essential.

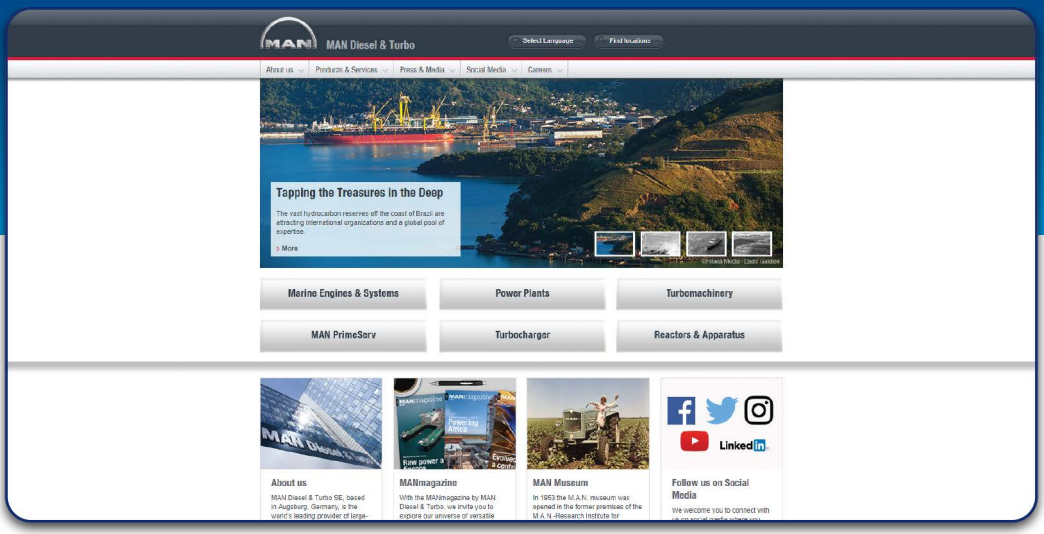
If data has always required rules, AI now extends those rules to a new frontier. The same lifecycle that governs enterprise information—capture, manage, process, search, and archive or dispose—must now apply to intelligent systems. We have to decide what a model is allowed to learn, what it should retain, what it must forget, and how its knowledge can be verified or audited over time.

Without those boundaries, memory becomes liability. Uncontrolled accumulation turns information into risk; disciplined lifecycle management turns it into insight and value. Governance isn't just about protecting data anymore—it's about teaching intelligence how to remember responsibly.

In the following case study, we explore how MAN Diesel & Turbo is using EIM as its foundation for governance and to achieve compliance.

Case Study

MAN Diesel & Turbo



MAN Diesel & Turbo

MAN Diesel & Turbo, headquartered in Augsburg, Germany, is the world's leading manufacturer of large-bore diesel engines and turbomachinery. The company employs around 14,900 staff at more than 100 international sites, primarily in Germany, Denmark, France, Switzerland, the Czech Republic, India, and China.

Diesel engines in container freighters or luxury liners are some of the largest products in the world and among those with the longest lifespan. They have to function for decades and be regularly maintained. One of the world's leading manufacturers in this field, MAN Diesel & Turbo, needs to keep important technical documents for a minimum of 30 years and sometimes indefinitely. The company was looking for an information management solution to ensure high-quality maintenance and successfully refute any claims for liability arising from alleged construction faults.

To help achieve compliance, MAN Diesel & Turbo turned to records management capabilities contained within an extended EIM solution, along with Application Governance & Archiving (AGA). The combined solutions bring together diverse applications to preserve information in context. Approximately 1,000 service staff in Germany and Denmark use it to archive over 4,000 process-related transaction files every day. In many service processes, paper-based transactions are now a thing of the past as existing paper files are being digitized.

MAN Diesel & Turbo is saving valuable time spent on searches and maintaining paper archives along with the large number of their digital archives. The integrated solution is also reducing maintenance requirements through the replacement of legacy systems, enabling the company to modernize its infrastructure, digitally transform key processes, and comply with regulations.

AI's Plateau on Data—and How to Move Beyond It

By 2026, more than 80 percent of enterprises will be using generative AI models or APIs in production.[4] That scale of adoption raises the stakes on governance. Spending on AI governance tools is expected to more than quadruple by 2030 as organizations work to manage risk, permissions, lineage, and model oversight while moving from experimentation to full integration.[5]

Enterprise use of generative AI is now mainstream, but much of that activity still sits on top of public data and generic models—great for content, limited for action. In 2024, 65 percent of organizations regularly used GenAI, a share that has continued to rise into 2025, yet many remain stuck at "good demos" rather than operational impact.[6] The gap isn't enthusiasm; it's data. To work for your business, AI needs governed access to private, permissioned information so it can reason in context and execute workflows safely.

Experience shows that scale without strong foundations rarely delivers results. Companies with mature data and AI capabilities consistently outperform their peers.[7] Those that "break away" do so because they treat data strategy and governance as first principles—not afterthoughts. In practical terms, that means bringing private content under control, enforcing access permissions, and applying policy-rich metadata so models can retrieve relevant information, act within guardrails, and demonstrate accountability.

When AI operates inside the firewall—connected to your governed data estate—it stops guessing and starts working. Instead of offering general answers, it can take informed, accountable action. It can resolve an invoice exception by referencing the purchase order, vendor terms, and approval history. It can draft and route a policy update that automatically respects permissions, retention schedules, and regulatory requirements. It can answer a support case in natural language using approved knowledge and record that interaction in the system of record.

Each of these capabilities depends on the same EIM backbone that reduces fragmentation, governs access, and connects unstructured information to the business processes that rely on it. To oversimplify—an EIM platform provides order. It governs information across systems, silos, and geographies. AI provides context. It learns from that governed data to deliver insights, automation, and decision support.

In the Cognitive Era, AI will unlock the next generation of information management. The implication is straightforward: without private, permissioned data—and the governance to use it responsibly—generative AI hits a ceiling. It can summarize the internet, but it can't approve an invoice, schedule a repair, or resolve a customer exception inside your systems. The way forward lies in enterprise data that is cataloged, classified, and access-controlled, supported by auditable pipelines that allow AI agents to pull facts, take defined actions, and leave a verifiable trail. That's how organizations turn widespread adoption into lasting business value.

The Fast Five Download

1. **AI Maturity Starts with Data Maturity.**
   AI is only as strong as the data it learns from. Generative models built on public data hit a plateau; agentic AI requires governed, private, and permissioned information. Invest in data foundations before scaling AI capability. Use EIM to identify high-value private datasets and apply AI where process value is clear.

2. **Governance Is the New Infrastructure.**
   The principles that keep enterprise data compliant—metadata, permissions, lifecycle control, and auditability—are now prerequisites for AI. Governance defines how intelligence learns, remembers, and acts safely within your organization.

3. **Move Inward for Value: Internet → Intranet → Extranet.**
   Public data powers generative AI (content), internal data powers agentic AI (action), and connected ecosystems will one day power AGI (collaboration). Each step inward increases accuracy, accountability, and value—and demands stronger controls.

4. **Data Quality Defines AI Performance—and Its Footprint.**
   Curated, clean data reduces hallucinations, improves reliability, and lowers compute waste. The new figure of merit balances quality, training time, and energy consumption. Better data governance now means faster, greener, and more accurate AI later.

5. **AI Must Follow Data's Rules.**
   Unlike traditional software, AI remembers what it sees. That makes its memory part of your governance landscape. Treat AI learning as a lifecycle: decide what models can learn, what they should retain, what they must forget, and how you'll audit them.

Chapter Two

The Rise of Enterprise Artificial Intelligence

As the technology landscape evolves, artificial intelligence has the potential to reshape many aspects of our lives. From enhancing workplace productivity to revolutionizing how we interact with information and each other, AI is becoming a critical part of our personal and professional lives.

Enterprise artificial intelligence (EAI) is redefining enterprise performance by turning intelligence into context. As adoption deepens across customer experience, operations, and content publishing, the real advantage isn't just automation—it's contextual understanding. This chapter will explore key AI technology concepts, fundamental principles, and applications across different sectors.

> *The number of companies that have fully modernized, AI-led processes has nearly doubled from 9% in 2023 to 16% in 2024. Compared to peers, these organizations achieve 2.5x higher revenue growth, 2.4x greater productivity and 3.3x greater success at scaling generative AI use cases.*[8]

Contextual intelligence enables AI to grasp business intent, interpreting not just data, but the structures, workflows, and goals that define how an organization creates value. By mapping relationships across metrics, processes, and business logic, AI can anticipate outcomes, model dependencies, and recommend actions aligned with strategic priorities. It effectively bridges the gap between analytics and execution—transforming insight into measurable decisions that drive growth, efficiency, and competitive differentiation.

However, alongside its benefits, some important ethical considerations and implications must be addressed. By understanding AI's dual nature—its potential to innovate and its capacity to disrupt—we can better prepare for a future in which this technology plays a central role. As we discussed data in the first chapter, here we will start to unpack how trusted, secure data is the cornerstone of effective AI. Good data is the key to driving innovation while preventing negative disruption as AI proliferates.

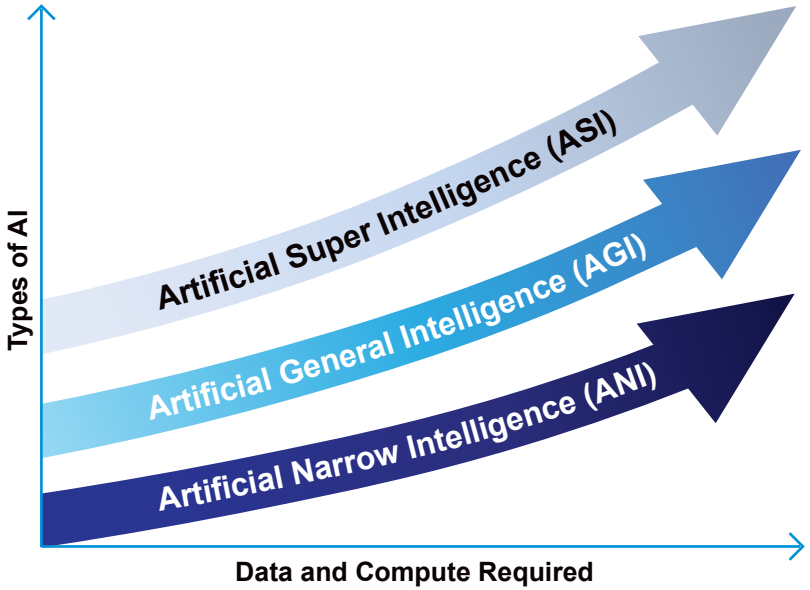
Defining AI

There are many definitions of AI, but according to the International Organization for Standardization (ISO), "Artificial Intelligence (AI) is a branch of computer science that creates systems and software capable of tasks once thought to be uniquely human. It enables machines to learn from experience, adapt to new information, and uses data, algorithms and computational power to interpret complex situations and make decisions with minimal human input."[9]

AI is not a single concept or a single technology. In fact, "AI is a broad field with numerous subfields, each with its own objectives and specifications. It is an umbrella term that encompasses a lot of technologies, including machine learning, deep learning, and natural language processing (NLP)."[10]

Artificial intelligence usually falls into three categories: narrow, general, and superintelligence. The easiest way to understand the differences is to think about how each one learns. Artificial Narrow Intelligence (ANI) is like a student who excels at just one subject. For example, it might be great at playing chess, recognizing faces, or predicting traffic patterns—but it can't do much outside its specialty. DeepMind's AlphaGo and its successor AlphaZero marked major milestones in AI by mastering complex games through self-learning and scaled reinforcement techniques, demonstrating powerful generalization within constrained domains—yet still firmly within the realm of narrow AI rather than true AGI.

Artificial General Intelligence (AGI), on the other hand, is more like a well-rounded graduate student. AGI can pick up new subjects, connect ideas, and solve problems in many different areas, much like a person can. Then there's Artificial Superintelligence (ASI), which goes a step further. ASI would be a kind of genius that outperforms at everything—reasoning, creativity, and even improving itself.



AI Falls Into Three Categories

The European Commission's *AI Watch* report describes ANI as systems that "can perform one specific task and operate within a predefined environment. ANI can process data at high speed and boost the productivity and efficiency in many practical applications. While ANI is superior in specialized domains, it is incapable of generalization, i.e., to re-use learned knowledge across domains."[1]

The report further explains, "AGI refers to machines that exhibit human intelligence. In other words, AGI aims to perform any intellectual task that a human being can."[12] We are not yet at the stage of AGI, as AI's intelligence is not human in nature; it is simulated. To fully achieve AGI, AI systems need to be capable of learning tasks (specifically, without retraining), exhibiting autonomous reasoning, and understanding cause-and-effect in context.

ASI is not yet defined in the standards and is acknowledged as a future state beyond AGI: "Artificial superintelligence (ASI) is a hypothetical software-based artificial intelligence (AI) system with an intellectual scope beyond human intelligence. At the most fundamental level, this superintelligent AI has cutting-edge cognitive functions and highly developed thinking skills more advanced than any human."[13]

Artificial intelligence can be classified in two primary ways: by capability (how closely it approaches human-like cognition) and by functionality (how it behaves and interacts with data). AI researcher Arend Hintze introduced a widely recognized functional framework that explains how systems process information and respond to their environment.

According to Hintze's framework, at the most basic level, Reactive Machines operate only on present inputs with no ability to learn from the past—IBM's Deep Blue chess system being a well-known example. Limited Memory AI adds the ability to retain short-term data to inform decisions, and it represents the foundation of nearly all modern AI, from autonomous vehicles to recommendation engines. Beyond this, the field moves into theoretical territory: Theory of Mind AI imagines systems capable of understanding human beliefs, emotions, and intent, while Self-Aware AI represents a hypothetical stage in which machines possess true consciousness and self-perception. While those higher stages remain speculative, understanding this spectrum helps frame where today's enterprise systems operate—overwhelmingly within the Limited Memory category, where value is realized through responsible data use, governed learning, and disciplined deployment at scale.[14]

As AI has evolved and different categories of AI have been identified, a common theme has emerged: data, compute, and governance are core for the different variants of AI. Models and capabilities may change, but the ability to organize, secure, and operationalize information remains the defining advantage. This is where Enterprise Information Management serves as a foundation for the application of AI, or Enterprise Artificial Intelligence (EAI).

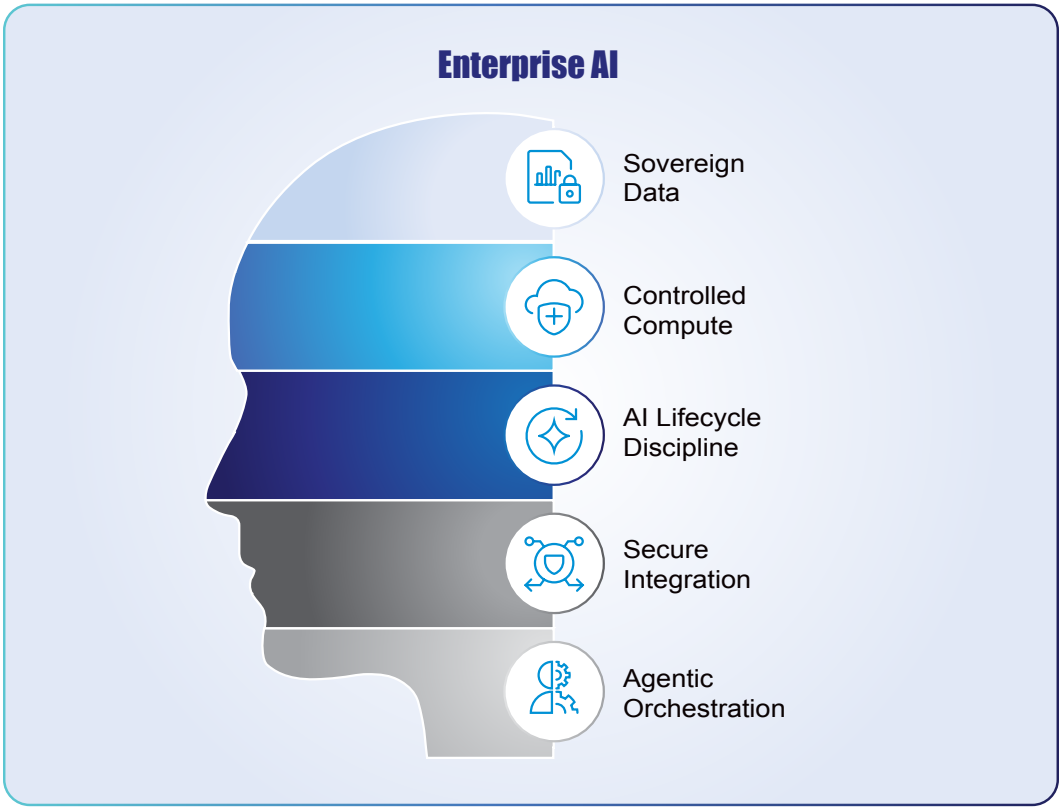
Enterprise Artificial Intelligence

Enterprise AI is not a separate class of intelligence; it is a term that describes the strategic application and integration of various AI technologies and capabilities within an organization to solve specific problems, automate processes, and drive decision-making. EAI primarily falls under the umbrella of Artificial Narrow Intelligence (ANI)/Weak AI, as the systems are designed to perform specialized tasks to enhance operations, not exhibit human-like general intelligence or consciousness.

Enterprise AI is built on:

- Trusted and governed data (the “sovereign data” layer)
- AI lifecycle management platforms (e.g., MLOps, LLMOps)
- Hybrid or sovereign cloud infrastructure
- Secure APIs and orchestration layers
- Agentic AI systems coordinating multiple specialized models

Enterprise AI is a governed architecture—not a single model. It stacks sovereign data, controlled compute, AI lifecycle discipline, secure integration, and agentic orchestration to deliver trusted automation at scale. It is a deployment context for operationalizing proven AI technologies and capabilities.



Enterprise AI

To deliver value, EAI solutions draw from a broad toolkit:

- **Machine learning** enables predictive analytics—with the ability to anticipate equipment failures, forecast demand, or optimize inventory.
- **Natural language processing (NLP)** powers intelligent chatbots, document summarization, and customer sentiment analysis.
- **Computer vision** brings automation which can be used for manufacturing inspections and enhancing safety and security monitoring.
- **Robotic process automation (RPA**) streamlines structured, repetitive tasks such as data entry and invoice reconciliation. And increasingly, generative AI supports content creation, code generation, and knowledge assistance.

What differentiates enterprise AI is not the underlying model type—it is the governed integration of these technologies into business workflows, data systems, and decision processes. Success comes not from isolated models but from orchestrating them responsibly at scale, underpinned by trusted data, secure infrastructure, and strong information governance. Enterprise AI differs fundamentally from consumer-grade AI in both purpose and design. Consumer AI focuses on enhancing individual experiences—recommending movies, assisting with personal tasks, or powering virtual assistants. These systems typically operate at small scale, rely on publicly available or user-provided data, and require limited integration with other tools. Their value lies in convenience and personalization for a single user.

By contrast, EAI is built for scale, security, and strategic impact. It operates on sensitive, proprietary business data stored in CRM records, ERP systems, and other operational databases and it must adhere to strict governance, compliance, and cybersecurity requirements. Enterprise AI integrates deeply with existing systems and workflows, automates complex cross-departmental processes, and delivers measurable outcomes such as operational efficiency, risk reduction, cost savings, and innovation. In essence, enterprise AI is the industrial application of modern AI technologies, engineered to operate across large environments where accuracy, accountability, and trust are as important as intelligence itself.

Discover how an international airport is using enterprise AI to keep 90+ million passengers moving smoothly across the globe in the following case study.

Case Study

An International Airport

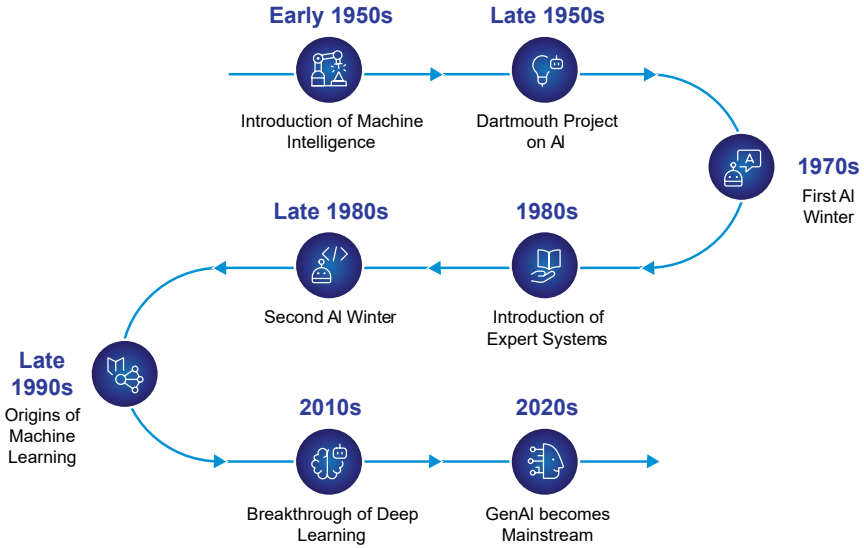
> *Much of our data was siloed across multiple systems, and ensuring accuracy, particularly for tracking passenger flows and processing times, was a real challenge. Staff often lacked real-time insights or predictive tools to manage queues, staffing, and congestion proactively.*

Airport IT Service Management Lead

Serving more than 90 million travelers annually, this airport is among the world's busiest for international passenger traffic—and one of the most digitally advanced. It stands out as a global hub known for innovation, efficiency, and exceptional customer service. Since opening in 1960, the airport has expanded dramatically, adding new runways, terminals, and concourses to accommodate growing air traffic.

Laying the digital foundation for this growth wasn't easy. With stakeholders ranging from airlines to police, customs, and service providers, communication is complex. Everyone needs access to the same data for coordinated decision-making. As part of a broad service management initiative, the airport partnered with a technology provider to extend its monitoring capabilities. An AI operations management component provides centralized, intelligent monitoring and management across complex IT environments. It enhances observability, reduces alert noise, predicts problems, and helps maintain uptime.

Real-time insights and intelligent monitoring have transformed IT from a backend function into a driver of service quality, stakeholder confidence, and customer satisfaction—with measurable impacts. Using AI on top of an EIM infrastructure, the airport has been able to prevent 30 percent of incidents with proactive monitoring, better align IT operations with business needs, and strengthen customer service through IT excellence.



The Evolution of Modern AI

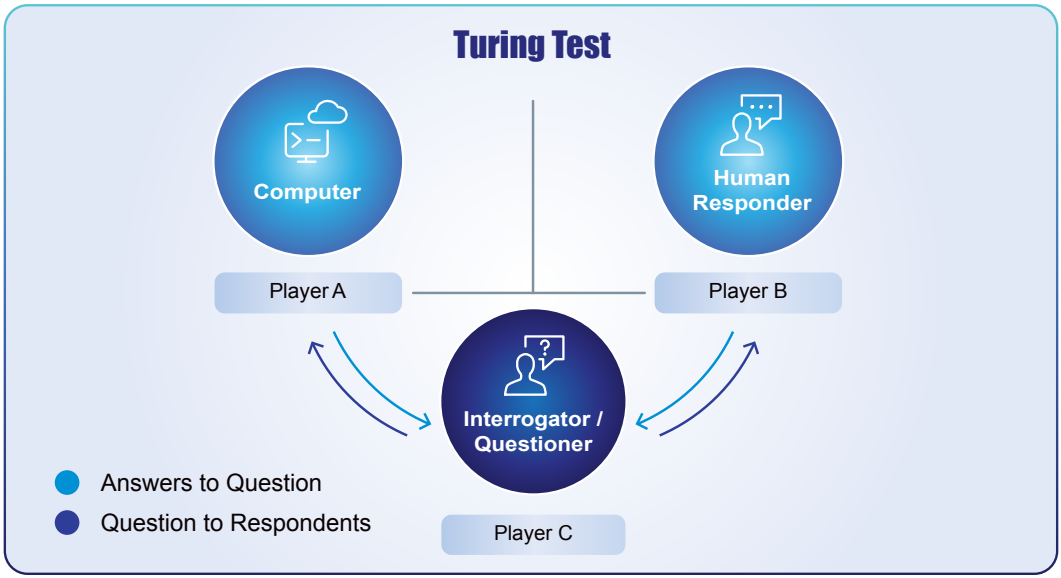
Over the last 75 years, AI has evolved into what we recognize today, with some years marked by incredible innovation and others by hype as the technology developed. Let's take a walk down memory lane to understand how we got here.

Early 1950: While AI has evolved over decades, Alan Turing is recognized as one of the early innovators who, in his 1950 journal article, "Computing Machinery and Intelligence," proposed that machines could simulate human reasoning and introduced the Turing Test for machine intelligence.[15]

Late 1950: Fast forward to 1956, when the term "artificial intelligence" was introduced during the Dartmouth Summer Research Project on Artificial Intelligence. This conference, organized by John McCarthy, Marvin Minsky, Nathaniel Rochester, and Claude Shannon, is recognized as the origin of AI as a research topic. This event brought together researchers to formalize the goal of creating machines capable of human-like reasoning and learning."[16]

1970s: However, the excitement from the conference didn't last long. While research progressed slowly, the reality of AI failed to live up to expectations, and early projects proved unsuccessful. The term "AI Winter" was coined to describe a period in which criticism of the lack of progress, including the *Lighthill Report* in the UK in 1973, led to government funding being cut off.[17]

1980s: After the 1970s AI Winter, AI research got its second wind in the 1980s with the rise of expert systems, programs built on "if–then" rules designed to mimic human behavior. These systems started showing up everywhere, and for the first time, companies began to see real commercial value in AI. This application of AI was narrow and task-specific, rather than anything close to true general intelligence.[18]



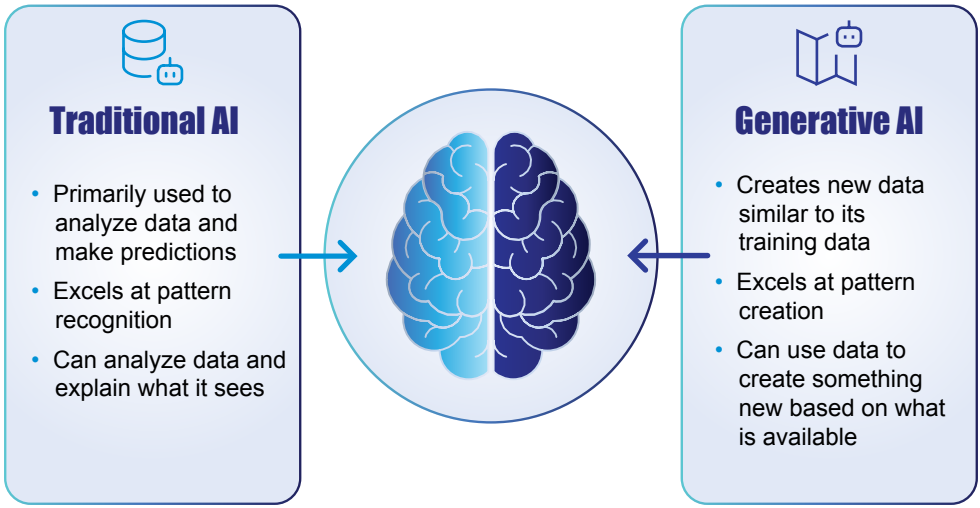
The Turing Test

Late 1980s/Early 1990s: But just as things were looking positive, there was a second AI Winter. In the late 1980s, the excitement died off as businesses found these programs expensive to build and maintain. Also, the limitations of the programmed logic became apparent. As funding dried up, AI experienced another downturn.[19]

Late 1990s: While AI went through a slower period, research didn't stop. Researchers worked on different approaches, moving away from hard-coded if-then patterns and looking at opportunities for machines to learn from data. This was the rise of modern machine learning. Some of the breakthroughs in the 1990s included algorithms for neural networks and decision trees. This was also when learning from data became a critical factor in the evolution of AI.[20]

2010s: Another breakthrough came in 2012 with the dawn of Deep Learning. This happened when a neural network called AlexNet dominated the ImageNet competition in image recognition, dramatically reducing error rates. This was a breakthrough for research because it showed that AI could outperform humans in visual recognition. Google, Facebook, and later, OpenAI built on this momentum, creating AI systems that could not only recognize images but also translate languages and generate text.[21]

2020s: Today, generative AI (GenAI) has become mainstream. Large Language Models (LLMs) like GPT, Claude, and Gemini are maturing and advancing AI capabilities. There has also been a realization that the size of models, the data used for training, and the computing power available are all crucial for performance. With these innovations, consumers are getting hands-on experience with AI, leading to rapid adoption in everyday life. Enterprise AI is also becoming a differentiator for business performance.



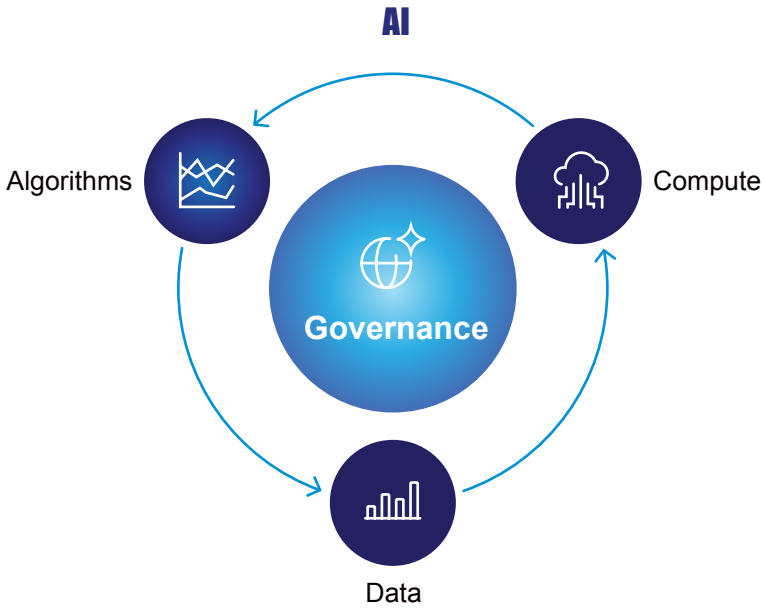
The Differences Between Traditional and Generative AI[22]

Data, Compute, Algorithms, and Governance as the Fuel for the Modern Enterprise AI Engine

Artificial intelligence in the 2020s has advanced through the convergence of three forces—data, compute power, and algorithms—working together under the discipline of governance. Data provides the essential fuel, the raw material that allows AI systems to learn, adapt, and generalize across domains. The quality, labelling, and integration of that data determine how effectively models perform: diverse, well-governed datasets produce more accurate and resilient outcomes.

Compute power enables scale. Advances in hardware—particularly graphics processing units (GPUs), tensor processing units (TPUs), and elastic cloud-based infrastructure—have made it possible to train models at a scope that was unimaginable a decade ago.

At the same time, algorithmic innovation has accelerated, giving rise to foundational models that support today's generative AI and multimodal AI systems. Together, these three elements—data, compute, and algorithms—form the technical core of modern AI. But governance provides the integrity layer that ensures each operates responsibly. When these forces work in concert, enterprises gain not only progress in reasoning and creativity, but also trust, compliance, and sustainable performance.



AI = The Combination of Data, Compute, and Algorithms

As history has shown, the evolution of artificial intelligence has rarely followed a straight path. Progress has unfolded through familiar cycles of optimism and correction—each surge of innovation followed by a period of recalibration. Early breakthroughs often inspired outsized expectations, which gave way to disillusionment when results fell short. Yet these cycles have been essential to the field's maturity, forcing researchers and enterprises alike to balance ambition with realism.

Over time, one insight has proven consistent: sustainable enterprise AI capability depends on equilibrium. True progress arises from the synergy among three interdependent pillars—well-managed data, scalable and efficient compute, and continually improving algorithms. Organizations that align these elements within a strong governance framework are the ones turning experimentation into measurable business value.

In the following case study, a medical research company uses enterprise AI to connect clinical, financial, and patient outcome data across the country, providing holistic analysis to help value-based health care transformation.

Case Study

A Country-Wide Healthcare Platform

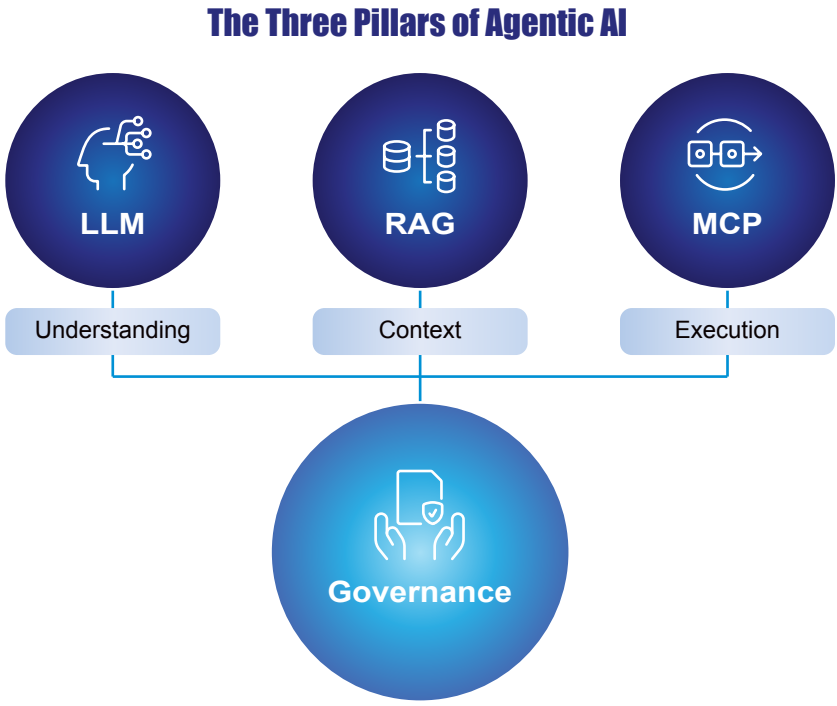
A Dutch medical research company allows its users (hospitals, government, pharmaceutical companies, and insurance companies), under strict data privacy regulations, to compare their performance and patient experiences and outcomes across hospitals and clinicians. It is continually helping healthcare professionals deliver value-based healthcare, using combined clinical, financial, and patient outcome measurement data. The organization needed a solution capable of providing an intuitive, online dashboard, suitable for scaling up. They selected a combination of AI and Business Intelligence (BI) reporting.

More than 5,000 users regularly access the solution to review performance and make comparisons with their peers. Using a detailed analytics dashboard, they can drill down to the details behind high-level metrics. By having ready access to this analytical intelligence, clinicians have been able to identify areas that are working well and areas that need further consideration. They can then apply appropriate improvements where necessary. For example, using the solution has helped reduce complications after colon cancer surgeries by more than half over four years.

With all hospitals in the Netherlands now using the solution, more clinical areas are being planned for inclusion. The full scope of possibilities AI provides is only just becoming apparent. Other areas, such as decision support where patients and clinicians can choose the optimal treatment together, is an exciting use case for the medical research company.

The Expanding Role of AI Agents

AI agents are moving rapidly from concept to core capability. Across industries, they're reshaping how work gets done—automating what's repetitive, accelerating what's strategic, and amplifying human expertise. In customer service, agents now monitor behavior patterns, flag churn risks, and trigger retention campaigns before a support ticket is even filed. In sales, they qualify leads, automate follow-ups, and deliver real-time insights that help close deals faster. Marketing teams are using AI to optimize segmentation and personalize campaigns at scale. In product development, intelligent agents sift through feedback, benchmark competitors, and accelerate roadmap decisions. Wherever data meets repetition, AI is stepping in—not to replace people, but to extend what they can accomplish.



Three Pillars of Agentic Enterprise AI

Large language models (LLMs) are algorithms that excel at understanding natural language, retrieving information, and delivering clear, conversational responses. But executing real tasks—configuring marketing campaigns, building user journeys, or testing pricing models—requires context: an understanding of how enterprise systems actually work. This is where Retrieval-Augmented Generation (RAG) and Model Context Protocol (MCP) architectures redefine the boundaries of capability.

Retrieval-Augmented Generation (RAG) is a process that strengthens LLM performance by injecting relevant, domain-specific knowledge into each response. Proprietary documentation, code repositories, and process instructions—securely integrated through RAG—give an LLM access to the "how" behind the task. Rather than relying solely on public data, it draws from the organization's governed knowledge base to generate precise, compliant guidance.

The Model Context Protocol (MCP) server completes the loop. Acting as the communication layer, an MCP server bridges generative AI with enterprise systems, databases, and APIs. It allows the AI to move beyond conversation into action—retrieving data, performing transactions, or triggering workflows in real time. Modern software environments may include hundreds of MCP endpoints, each enabling the AI to execute a specific operation under policy control.

Together, these three pillars—LLMs, RAG, and MCP—form the foundation for agentic AI in the enterprise. They turn language into logic, intent into execution, and insight into measurable outcomes. This is the next evolution of intelligent systems: governed, contextual, and capable of working alongside humans to drive transformation across every function.

A global mining company has done just that—accelerating its research project timelines with AI, in the case study below.

Case Study

A Global Mining Company

A global mining company, with headquarters in Brazil, produces iron, nickel, copper, manganese, and more. The company undertakes careful research to assess both the viability and the social and environmental impacts of its mining operations. Their research projects can take up to ten years. Typically, cross-functional teams spend weeks or months manually collecting and consolidating information for review as new product opportunities, market fluctuations, or environmental standards emerge. The mining company's research projects were hampered by low-level manual work and an inadequate AI assistant that lacked scalability for global reach.

With a history of technological innovation to support its operations, the company sought a solution that could help its specialists cut down repetitive manual tasks, speeding up the research stage for both new and existing mines. A spokesperson from the global mining company said, "Information about each mining project is typically stored in different formats across siloed systems and accessing it takes up a significant amount of valuable time as workers search through mountains of documentation. AI, with its ability to quickly ingest and analyze large volumes of data, presented the perfect opportunity for reducing this manual work."

The mining company built a proof of concept with an AI vendor and, through expert training and AI best practices, they have been able to boost their AI response accuracy by 47 percent. Using AI for researching mining projects, the company has reduced months of low-level manual work and stimulated rapid growth. If they need to assess the feasibility of using an existing mine to produce ore, for example—something that a geologist would complete in two months—relevant information can be consolidated in just a few hours, helping the company rapidly close in on viable investment opportunities and stay ahead of market shifts.

A Path Forward for AI

Looking back over the past 75 years of artificial intelligence, one clear lesson stands out: true success in AI has never been about technology alone. While breakthroughs in data, compute, and algorithms have fueled remarkable progress, the most enduring impact has come from aligning these advances with strong governance, ethical principles, and human collaboration.

Enterprise AI represents more than the next phase of artificial intelligence—it marks a fundamental redesign of how people engage with technology. Unlike traditional generative AI, which produces outputs in response to prompts, agentic systems demonstrate autonomy, initiative, and adaptive reasoning. They can plan, act, and learn within real-world contexts, moving from conversation to execution without constant human direction.

This shift signals the quiet retirement of the Graphical User Interface (GUI) as the dominant interaction model. The buttons, tabs, and menus of the GUI era are giving way to direct collaboration with intelligent agents through natural language and voice. Instead of navigating software, users now express intent—and the system interprets, decides, and acts.

The result is not the disappearance of the interface, but its evolution. The visible surface of software recedes, and what remains is intelligence that operates through conversation, context, and trust. In this new paradigm, productivity is no longer measured by clicks per minute, but by the quality of outcomes achieved through human-AI partnership.

Agentic intelligence is already reshaping how organizations produce, manage, and personalize content. Research cycles are automated, first drafts generated, and experiences curated in real time—tailored to audience behavior and preference. AI doesn't just react; it reasons, predicting the downstream impact of every change. For enterprises, the opportunity is clear: contextual intelligence doesn't replace human judgment—it amplifies it, scaling expertise, governance, and creativity across the organization.

As we look ahead, the next era of AI will be defined not just by greater power, but by greater autonomy, transparency, and accountability. It will be defined by systems that can act intelligently while remaining explainable and aligned with human values. Understanding what AI is, where it came from, how it works, and when key milestones occurred, provides the foundation for thoughtful leadership in shaping what comes next.

With this context in mind, the next chapter explores the intersection of data and AI, examining how the fusion of information and intelligence is creating new possibilities for innovation, trust, and value in the modern enterprise.

The Fast Five Download

1. **AI Is Broad, Evolving, and Foundational.**
   Enterprise artificial intelligence is not a single technology but an umbrella term covering diverse subfields like machine learning, deep learning, and natural language processing. It ranges from narrow, task-specific systems (ANI) to the conceptual goal of superintelligent systems (ASI). Understanding these distinctions is key for informed decision-making.

2. **Data Quality and Governance Are Critical.**
   The effectiveness and trustworthiness of AI depend on high-quality, well-governed data. Data is the "fuel" for AI innovation; without reliable, secure, and well-managed data, AI systems are prone to errors, bias, and operational risk.

3. **Technology Progress Follows Hype Cycles.**
   AI's history is marked by cycles of rapid innovation and periods of disillusionment (AI winters). These cycles have matured the field, highlighting that sustainable value comes from balancing technological advances with realistic expectations and prudent investment.

4. **Compute Power and Advanced Algorithms Drive Modern AI.**
   Breakthroughs in hardware (GPUs, TPUs, cloud infrastructure) and algorithm design have enabled today's large-scale, generative AI systems. The synergy between data, compute, and algorithms is what sets leaders apart in the AI space.

5. **Governance, Ethics, and Human Alignment Are Essential for the Future.**
   The next era of AI will be defined by systems that are not just powerful, but also transparent, explainable, and aligned with human values. Success will require strong governance, ethical frameworks, and human oversight to ensure AI enhances business value while building trust.

Chapter Three

The Intersection of Data and Artificial Intelligence

In this chapter, we explore the intersection of data and artificial intelligence, focusing on how information becomes intelligence.

Building on the foundations set out in Chapter 1 (Data) and Chapter 2 (AI), we look at how data and intelligence form a continuous value chain. Data fuels the AI engine; AI, in turn, unlocks the latent value of data. Continuous learning closes the loop, driving accuracy, adaptability, and insight over time. Governance connects these worlds—ensuring that as enterprise intelligence grows, it remains explainable, auditable, and aligned with organizational trust. Finally, we consider the strategic and economic implications of bringing data and AI together.

Where Data and Intelligence Meet

In Chapter 1, we traced the evolution of data—how it became the foundation of Enterprise Information Management and how its structure, stewardship, and accessibility generate business value. Chapter 2 took a closer look at artificial intelligence as the engine of automation and intelligence, tracing its technological evolution beyond the hype cycle toward real-world, agentic AI deployment.

Throughout this book, our central thesis is that data and AI are symbiotic. Data gives AI the context and potential to learn, while AI transforms data into actionable insights. Together, they are driving innovation across modern enterprises.

High-performing AI requires high-quality data. This is data that is well-governed, structured, context-rich, and secure. Not all data is created equal. Different datasets have different requirements, particularly as organizations balance public and private data. Public datasets train the Large Language Models (LLMs) that underpin tools like ChatGPT, but for enterprises, private, customized data is the critical differentiator. Strategies that maintain the privacy and sovereignty of this data, while enabling AI to learn from it, are essential for competitive advantage.

It's at this intersection—where enterprise data meets intelligent systems—that the true potential of enterprise AI is realized. Here, context becomes capability, and information becomes insight. Organizations that can harness this relationship responsibly will define the next era of digital performance.

Can AI Replace Data and Enterprise Information Management?

As AI adoption increases, a common question is whether AI can replace existing data and information management solutions. The short answer is no. However, it is the intersection of information management and AI that drives outcomes. One can't act without the other. AI automates data-specific actions, like data extraction and classification, whereas information management provides secure, organized content, and importantly, the foundational structure and rules for governance and compliance that AI does not.

While data and information management solutions provide the fuel for AI, AI is also transforming information management. It does this through:

- **Automation** - AI automation tags documents, runs extracts, summarizes reports, and reduces human error across key workflows.
- **Insights** - AI delivers valuable insights on the content that is being managed, including deriving key insights, sentiment, and other important notes.
- **Search and Retrieval** - AI, in combination with the metadata in content management makes search interfaces more accurate, efficient, and easier to use.

Information management is the gatekeeper for trusted data; data quality defines the credibility of every AI decision. The two disciplines are deeply interconnected: effective AI relies on governed, high-integrity data, while information management gains new speed and intelligence through AI-driven automation. Integrating the two ensures consistency, compliance, and context across the information lifecycle (we explore this in greater depth in Chapter 5). AI can enhance how organizations manage content—but it cannot replace the discipline and governance that make information trustworthy.

This interdependency between AI and information management is illustrated in the following case study about a global foods producer that is applying AI to its business information to modernize operations and improve performance.

Case Study

A Global Foods Manufacturer

Crop Scouting Using Drones

A foods manufacturer with operations around the world has implemented several strategies to position itself as an industry leader in AI adoption. What follows are excerpts of an interview with the company's EIM Director.

"As part of our transformation project, we're exploring how artificial intelligence can help us modernize operations. Today, roughly ten percent of our data is stored in the cloud. It's not a big number yet, and the cloud solutions we've used so far have been private to ensure the security of our proprietary information. But the technology is advancing quickly, and we're becoming more open to public cloud adoption—provided we can ensure strong governance and maintain ownership of our data.

AI is becoming central to how we manage and extract value from our information. We're using AI-driven systems to pull insights from our operational data, helping management run our plants more efficiently. The results are tangible: higher-quality products, more sustainable practices, and measurable improvements to the bottom line.

AI has also inspired entirely new ways of working. We're piloting drone-based crop monitoring—an extension of a practice we've used for years with satellite imagery. Satellites helped us estimate crop health, but they don't perform well under cloud cover. Drones, on the other hand, can be programmed to fly over entire fields, capture high-resolution images, and feed that data directly into our AI models. Once processed, the models predict crop performance, identify stress or disease, and even recommend specific irrigation or fertilizer adjustments. That same insight is then integrated into automated fertilizer spreaders, which apply the right amount of treatment in the right places—reducing waste and improving yield.

We're also advancing into predictive agriculture. By combining AI models with decades of historical weather and crop data, we can forecast growing conditions two to three years out in specific regions. These models aren't perfect, but they're increasingly accurate and incredibly useful for planning.

Every region of the world is different—its soil, weather, crops, and farmers. Our challenge is to adapt to all of them, and AI helps us do that at scale. The technology lets us understand local conditions in real time and make decisions that improve productivity, sustainability, and resilience. What used to take weeks of manual analysis now happens continuously. AI has become not just a tool for insight, but a partner in how we grow, produce, and feed the world."

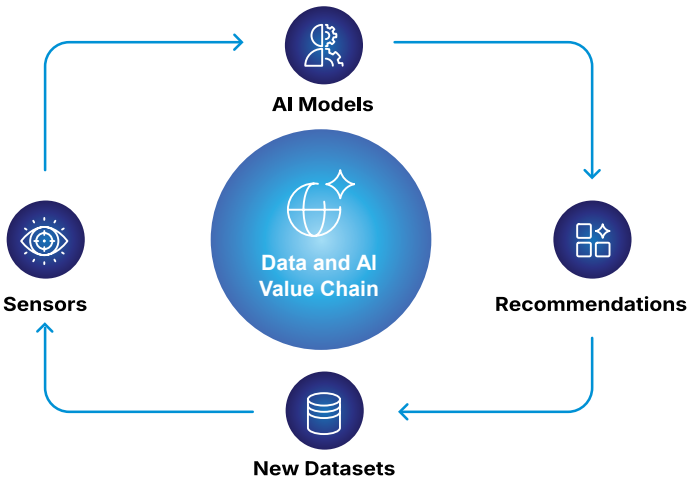
The Data and AI Value Chain

Unlocking value from data begins with understanding the data and AI value chain. This process starts with data generation and collection, where access to enterprise data becomes a fundamental enabler. Once collected, data must be integrated, cleaned, and governed to ensure quality and reliability. Organizations that have invested in strong information management practices are better positioned to accelerate AI adoption, because they have already done the foundational work of enabling their data.

However, data alone is not enough. Without structured processes and workflows, data is not actionable. AI becomes valuable only when applied to real business challenges, integrating into these workflows to generate measurable outcomes. This is where AI model training, fine-tuning, and validation come into play. LLMs are initially trained on public datasets, but enterprises can extend their value by fine-tuning them with private data or by using Retrieval-Augmented Generation (RAG) pipelines that connect AI to internal knowledge sources. The right strategy depends on the organization's goals, resources, and maturity level. However, regardless of approach, data quality and model governance are critical requirements.

The final and often overlooked step in the value chain is the feedback loop. Many organizations rush to deploy AI capabilities without establishing mechanisms for continuous learning and improvement. This is where the true value emerges, especially with AI. Iterative fine-tuning allows model accuracy to improve over time and drive more impactful results.

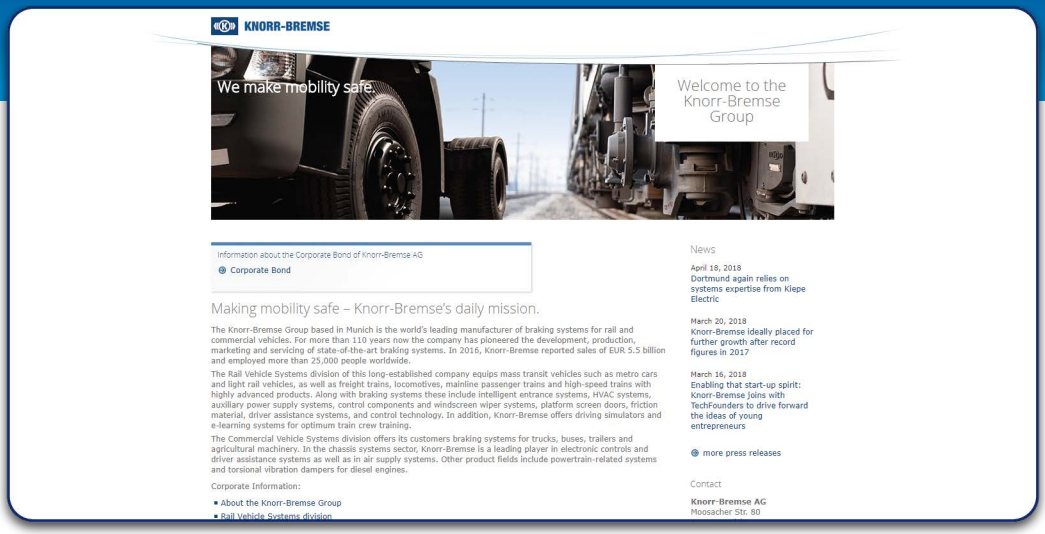
To put the data and AI value chain into context, consider an example from manufacturing. Sensors on the factory floor collect data, then feed this data into the AI models. Based on this data, the models make recommendations to optimize performance. This, in turn, generates new datasets that can continually and iteratively be improved.



This approach is demonstrated in the following case study which describes how Knorr-Bremse keeps the wheels rolling with predictive maintenance powered by actionable insights.

Case Study

Knorr-Bremse

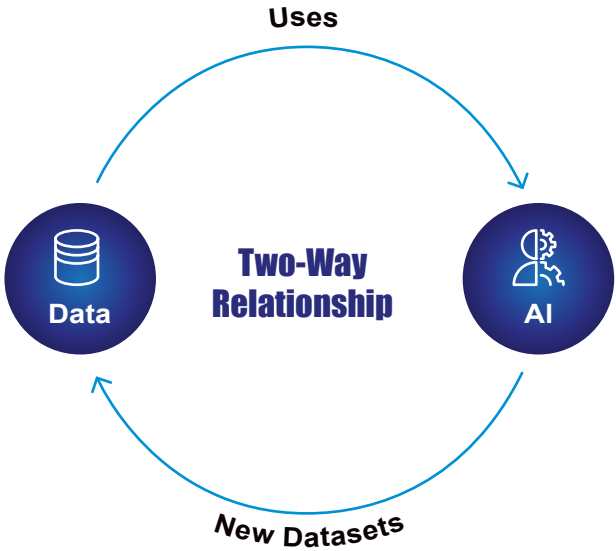


Knorr-Bremse Group

Based in Munich, the Knorr-Bremse Group is the world's leading manufacturer of braking systems for rail and commercial vehicles. For more than 110 years now the company has pioneered the development, production, marketing, and servicing of state-of-the-art braking systems.

Knorr-Bremse's iCOM (intelligent Condition Oriented Maintenance) platform brings digitization to the rail business, connecting wireless-enabled sensors aboard trains to a back-office cloud-based network, using an IoT (Internet of Things) model. This platform transmits detailed data that can help predict repair and replacement needs. The iCOM platform required a powerful and user-friendly analytics component to enable the analysis of the data received to help users make data-driven decisions.

The ability to make predictive, data-driven decisions results in more efficient and cost-effective repairs. With data being continually collected, the volumes across a fleet are significant. Customers now have the ability to visualize the data through interactive graphical dashboards, reducing the reliance on IT to create new reports. For example, they can provide heat-maps of condition-based events, such as overheating brakes on a specific incline, helping customers put measures in place to reduce component failures, extending component life, and ultimately, saving money.



AI and Data Form a Two-Way Relationship

Data as the Fuel for AI

Data is the fuel that powers the AI engine. The quantity, quality, and diversity of data matters far more than the complexity of the AI models themselves. High-quality, diverse datasets give AI systems the context they need to learn effectively. Simple AI can deliver impressive results on high-quality and diverse datasets, whereas complex AI cannot deliver the same results on low-quality and homogenous datasets.

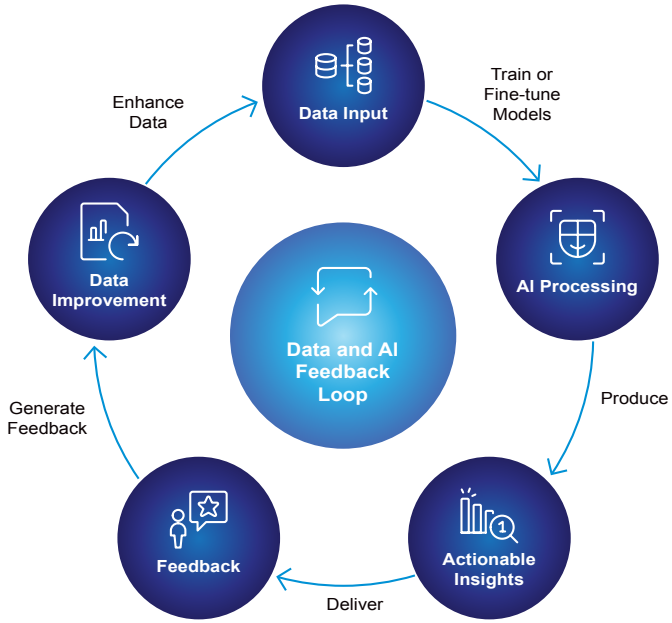
As described in Chapter 1, both structured and unstructured data fuel this mix. Unlocking this data safely and responsibly is the key to meaningful AI adoption in business contexts. For most organizations, success depends not on training massive public models but on leveraging private data strategically within existing frameworks. And once this private data is unlocked for AI, protecting that AI becomes critical. This is the key to the concept of sovereignty that we will discuss later in the book. Differentiating between public and private datasets, and providing the appropriate protections for those private datasets, is an urgent priority.

AI doesn't merely consume data—it interprets, enriches, and organizes it for use across the enterprise. In this sense, AI and data form a two-way relationship. AI uses data to learn, but it also enhances the value of data by improving its structure, integrity, and accessibility.

The Continuous Feedback Loop

Every effective enterprise AI system utilizes a continuous feedback loop: data trains AI models, AI produces insights, and those insights generate new data that refines both the model and the underlying datasets. Intelligence improves not in a straight line, but in cycles of learning.

For instance, recommendation systems constantly learn from user behavior. Each interaction creates new data that helps the system make better predictions. Over time, this iterative refinement increases accuracy, personalization, and efficiency. Think of this in the context of your favorite online shopping website. Every click, purchase, or pause creates new signals that reshape the system's understanding of user intent. The next set of recommendations reflects what the model has learned since the last one. It's trained to provide you with relevant recommendations, but as you continue shopping, it uses that data to generate new insights and over time improve the quality of the recommendations.



AI and Data Form a Two-Way Relationship

Equally important to this process are observability and monitoring. The loop must be governed and models evolved responsibly. Continuous oversight of model performance and data flow ensures that AI systems remain reliable, explainable, and aligned with business objectives. As we will explore later in the book, the operational management of AI systems cannot be an afterthought; it must be contemplated as a strategic capability that underpins long-term success.

Governance at the Intersection

Governance lies at the heart of the data and enterprise AI intersection. On the data side, governance focuses on privacy, lineage, access control, and compliance with regulations such as GDPR (General Data Protection Regulation). On the AI side, governance emphasizes fairness, transparency, accountability, and explainability.

These two domains are now coming together under shared principles such as ethics, auditability, and trust. Emerging AI Trust Frameworks and international standards, like ISO/IEC 42001 for AI management and ISO/IEC 38505 for data governance, illustrate this convergence. As these frameworks mature, they will shape how organizations design, deploy, and monitor AI responsibly. We take a deeper dive into data and AI governance in chapters 5 and 6, respectively.

> *Integrating data and AI creates competitive advantage — governing them responsibly is what turns it into lasting economic value.*

Strategic and Economic Implications

Finally, integration of data and AI creates both strategic advantage and economic opportunity. Organizations that align these capabilities effectively are better equipped to innovate, optimize operations, and differentiate in competitive markets.

With so much anticipation from boards and executive leadership on the potential for enterprise AI, it's easy to understand some of the market disappointment around the pace of change and impact. This has put a spotlight on early AI pilots in enterprises and their relative success. However, it's worth noting that many early AI pilots have underdelivered because they relied on publicly trained models without contextualizing them with enterprise data. Enterprise leaders need to understand that their competitive advantage lies in safely and securely unlocking this data. The next phase of success lies in taking a data-centric AI approach that prioritizes improving data quality and process design over building ever-more complex AI models.

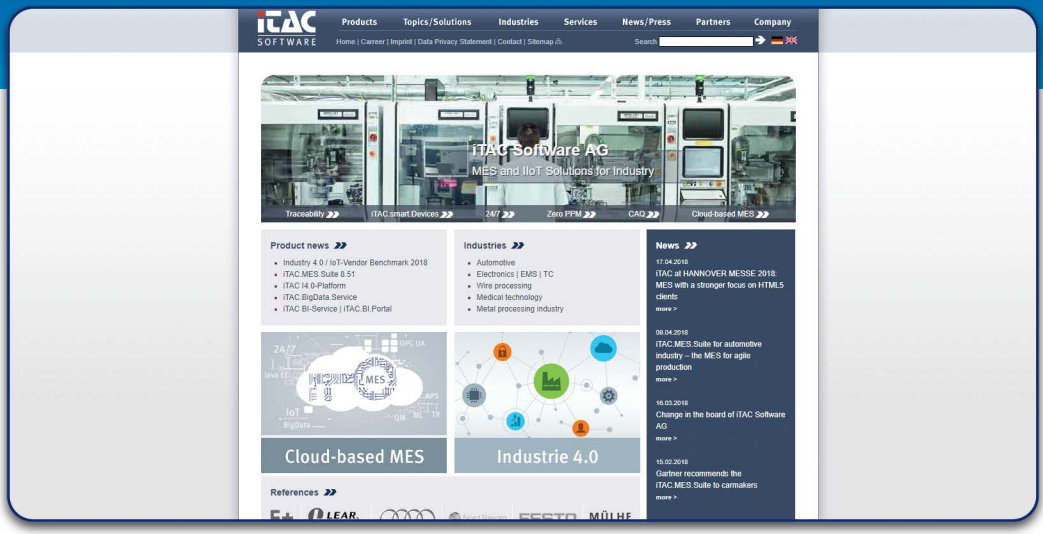
Good data and sound processes lead to reliable AI outcomes.

While large-scale computing remains necessary for training foundational models, most enterprises can achieve meaningful value through smaller, targeted deployments. Understanding your data requirements helps determine what level of compute investment is truly needed, preventing overspending and aligning AI initiatives with real business value. This also helps to reduce concerns around AI for leaders and employees who might still be working to fully understand the technology.

Discover how iTAC Software AG is using intelligence to enable smart factories in the following case study.

Case Study

iTAC Software AG



iTAC Software

Since its founding, iTAC (Internet Technologies and Consulting) Software AG has been specializing in providing internet technologies for the manufacturing industry. The manufacturer of standard software and products for cross-company IT applications is an industry leading system and solution provider of Manufacturing Execution Systems (MES) for the entire supply chain.

To offer its customers the greatest possible transparency and decision-making capability for production control, and to meet growing demands related to the Internet of Things (IoT), iTAC wanted to integrate Business Intelligence (BI) and analytics software into their MES suite. Doing so would support customer demands for manufacturing intelligence, quality control, and traceability. In addition to rapid, effective implementation and seamless integration, iTAC required the customization of reports, analysis, and dashboards with full interactivity and security. All these needed to be web-based, offer transparent personalization for various applications, and be available through different channels.

iTAC now has the BI, operational, and analytical capabilities it needs to support customer demands for greater intelligence, quality control, and traceability throughout the entire manufacturing process. The solution ensures transparency in metrics management and supports product lifecycle management, budget control, and quality assurance, as well as field activity management. The company's clients can access and analyze large amounts of data centrally with extensible support for future expansion, delivering competitive advantage.

As we've covered in this chapter, data and AI are inseparable partners, with data as the fuel for the AI engine. AI without data is directionless, and data without AI is not actionable. Together, they form the foundation of intelligent enterprise decision-making.

As organizations increasingly move toward AI-driven decision frameworks, strong governance and strategic alignment become essential. The intersection of data and AI represents not only an operational shift but also an innovation frontier, redefining how organizations think, decide, and compete. This convergence marks the beginning of a new chapter in digital transformation, one where information truly becomes intelligence.

The Fast Five Download

1. **Prioritize Data Quality and Governance.**
   Establish data readiness as an organizational mandate, not a project deliverable. Direct your teams to perform comprehensive data audits and implement governance policies that ensure accuracy, security, and accessibility across all critical information assets. Make data quality a board-level priority to maximize AI effectiveness.

2. **Integrate AI into Real Business Workflows.**
   Embed AI in high impact business processes to identify two to three key operational areas (e.g., customer support, supply chain optimization, risk management) where it can deliver immediate benefits. Task business and technical leaders with deploying AI solutions that leverage proprietary data to address real business challenges.

3. **Establish Continuous Feedback Loops for AI Improvement.**
   AI performance is never static; it requires continual monitoring and training. Institute an organizational policy for ongoing AI model performance monitoring—including user feedback loops and automated retraining using new data. Assign accountability for this process to ensure models remain accurate, personalized, and aligned with business goals.

4. **Align Data and AI Governance for Trust and Compliance.**
   Bring data and AI under a single governance framework. Appoint a cross-functional task force that unites privacy, security, compliance, and ethical oversight to create consistent standards for how intelligence is built and applied. Adopt or benchmark against emerging standards (such as ISO/IEC 42001 and 38505) to proactively manage legal, reputational, and operational risks.

5. **Take a Data-Centric Approach to AI Investment.**
   Tie all investment decisions to data value and business outcomes. Before approving new AI projects, require business units to articulate how the initiative unlocks value from enterprise data and delivers measurable business results. Limit investment in large-scale AI models unless justified by unique data assets and a clear path to ROI.

Chapter Four

Making it Secure—The Importance of Cybersecurity

Innovation must be balanced by trust to ensure that the intelligence we build cannot be turned against us. In this chapter, we explore how cybersecurity must evolve alongside AI. As intelligent systems reshape how enterprises operate, new risks demand equally advanced defenses. We'll examine emerging threats, and the strategies required to secure data, models, and AI-driven operations against them.

62% of organizations experienced a deepfake attack involving social engineering or exploiting automated processes, while 32% said they experienced an attack on AI applications that leveraged the application prompt in the last 12 months.[23]

In recent years, cyber threats have evolved from simple breaches to sophisticated assaults aimed directly at enterprise AI systems—and the stakes have never been higher. As organizations accelerate adoption of technologies such as generative AI (GenAI), we are witnessing a surge in attacks that leverage AI for phishing, deepfakes, and advanced social engineering. At the same time, a new wave of vulnerability is emerging: malicious actors who exploit GenAI infrastructure, manipulate prompts, or compromise chained AI workflows to infiltrate and disrupt enterprises.

In the previous chapter, we examined how the intersection of data and enterprise AI creates opportunities for innovation and operational efficiency. But opportunities also bring unwanted risks, and as organizations rely on private data to fuel their AI engines, they may inadvertently expose themselves to new and evolving cyber risks. The protection of enterprise data and AI must keep pace with technological evolution, as data and AI are attractive targets for threat actors.

In the following feature, an energy company lays the foundation for AI and advanced analytics within a secure EIM system, building an enterprise architecture that blends its data with processes for governance and cybersecurity controls.

Case Study

A Nordic Energy Company

This energy-generation organization operates in a highly regulated sector, managing vast volumes of technical documentation critical to safety and operations. Faced with the challenge of enabling over 900 employees to reliably access the latest approved versions of these documents across office and plant environments, the company recognized that legacy, fragmented systems lacked the governance and visibility required for modern risk and trust management. In an era where data is both an asset and a vulnerability, establishing a security-by-design approach became imperative.

To build a robust foundation, the company implemented a unified content management environment underpinned by strong identity and access controls, workflow automation, and document lifecycle governance. By centralizing control and enforcing policy-driven access rights, the system ensured that only the appropriate users could reach sensitive operational records, at the right time and from the right context. Automated workflows moved documents through review, approval and archiving in a governed fashion, strengthening the security of the data plane while maintaining usability for field and office teams alike. With this architecture in place, the organization laid the groundwork for advanced analytics and AI-enabled capabilities—on the understanding that those must rest on secure, well-managed information.

The results were transformative. The company achieved a high stability record and dramatically improved user productivity, with near-real-time access to mission-critical content supporting both safety and operational integrity. But perhaps more important: they now possess the trusted information infrastructure required to introduce AI-driven search, insights, and decision-support tools—securely and responsibly. In short, by treating cybersecurity, data governance, and AI readiness as intertwined components, the company moved from document management to a modern intelligence-platform posture—anchored in trust, visibility, and automation.

> *We spend upwards of 70 percent of our time playing defense from a technology perspective, whether it's regulatory or cybersecurity threats. We have to remain vigilant in protecting the bank and our clients' data and keep up with the latest changes and patches that addresses vulnerabilities.*
>
> CTO and Managing Director of a Global Bank

The Cyber Threat Landscape for Data and AI

According to the World Economic Forum's *Global Cybersecurity Outlook 2025*, "GenAI tools are reshaping the cybercrime landscape by enabling criminals to refine their methods and automate and personalize their techniques. With 47% of organizations citing their top concern surrounding GenAI as the advance of adversarial capabilities, cybercriminals are harnessing the efficiency of AI to automate and personalize deceptive communications. Some 42% of organizations experienced a successful social engineering attack in the past year, a number that can only increase with advances and the malicious adoption of AI."[24]

Cybersecurity for enterprise AI must be approached from a multidimensional perspective—one that recognizes the full spectrum of threats spanning data, models, infrastructure, and human interaction. The cyber threat landscape for data and AI runs across infrastructure, governance, and human behavior. Traditional cyber risks, such as unauthorized access, insider threats, and ransomware, continue to target enterprise systems and compromise critical data. And as organizations move more of their data and operations into cloud environments, the overall attack surface continues to grow. Threat actors continue to exploit weaknesses in identity management, network segmentation, and vulnerable software. These foundational threats create the conditions for more advanced forms of attack that exploit the growing reliance on AI.

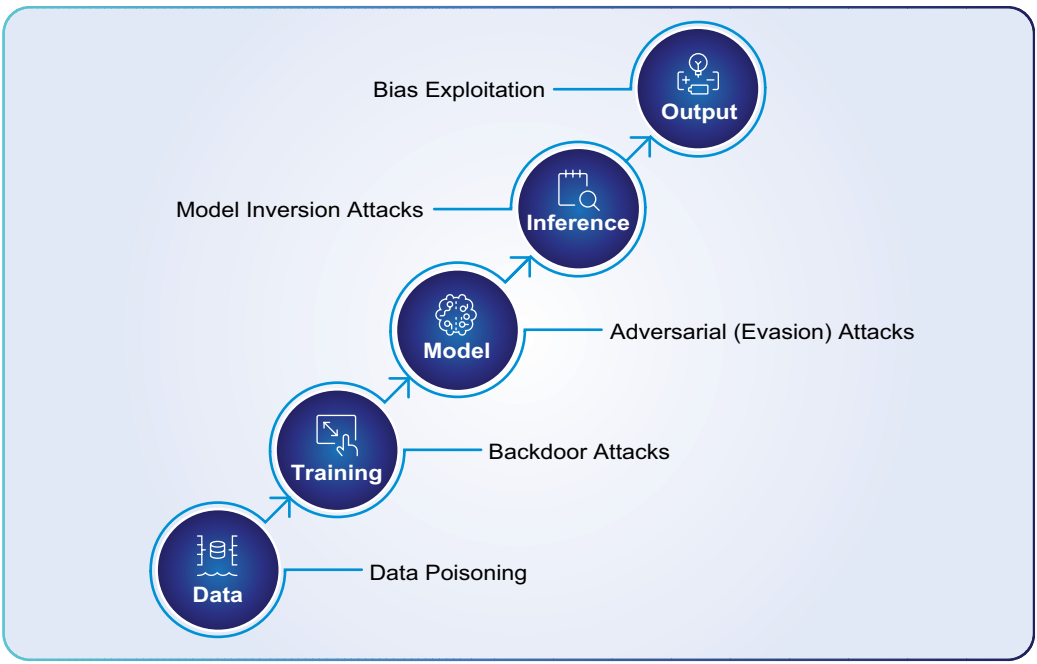
Some of the expanding attack surfaces include the data pipelines used to train LLMs and the models themselves. As researchers from IBM and Carnegie Melon University have observed: "Growing applications of large language models (LLMs) trained by a third party raise serious concerns on the security vulnerability of LLMs. It has been demonstrated that malicious actors can covertly exploit these vulnerabilities in LLMs through poisoning attacks aimed at generating undesirable outputs."[25]

In addition to model poisoning, other security risks such as data exfiltration and prompt injection are becoming more commonplace, with the latter being one of the biggest challenges for security in LLM.

Emerging AI-specific threats introduce new vulnerabilities that go beyond conventional data breaches. Because new threats emerge every day, it is impossible to build an up-to-date, all-encompassing list of attacks. However, some of the most common types include:

- Data poisoning attacks
- Backdoor attacks
- Adversarial (evasion) attacks
- Model inversion attacks
- Bias exploitation attacks

The diagram below shows the AI model lifecycle mapped to the different types of cyberattacks we will review in this section. The lifecycle begins with **Data** collection and preparation, which feeds into the **Training** phase where the model learns. This results in a trained **Model**, which is then used for **Inference** (the process of making predictions or decisions) to generate the final **Output** (a prediction, classification, decision, or generated response).



Mapping Cyberattacks to AI Models

Understanding how these different cyberattacks relate to the AI model lifecycle puts them in context for where threats can occur. Let's look at the threats in more detail.

1. Data Poisoning

Data poisoning attacks are common during the data phase in advance of training, through collection and ingestion. In these attacks, threat actors inject malicious inputs into the training dataset, corrupting how the model learns and undermining its integrity and reliability. The root issue lies in a flawed assumption: most learning algorithms presume that training data is clean and representative of reality. In security-sensitive environments, that assumption simply doesn't hold true.[26]

2. Backdoor Attacks

Backdoor attacks are a form of data poisoning where a trigger pattern is hidden in the model during training. The model will behave normally for regular inputs but then will produce a malicious output when the trigger appears. These types of attacks can be complicated to detect because they remain inactive until the trigger condition is met. In this case, "an adversary can create a maliciously trained network (a backdoored neural network, or a BadNet) that has state-of-the-art performance on the user's training and validation samples, but behaves badly on specific attacker-chosen inputs."[27]

3. Adversarial Attacks

Another common type of attack is an adversarial attack. These occur when threat actors try to manipulate the AI model's inputs to produce incorrect results. Sometimes these changes can be so small they aren't recognizable, but they can alter behavior and undermine safety in AI use cases such as medical imaging or autonomous navigation.[28]

4. Model Inversion Attacks

Model inversion attacks pose a threat to privacy and personal data. They do this through attempts to "reconstruct sensitive input data from model parameters, outputs, or intermediate representations."[29] In other words, the attack essentially reverse engineers the model to expose the specific, private data it learned from.

5. Bias Exploitation Attacks

The final type of attack we'll highlight is bias exploitation attacks, which take advantage of bias that already exists in the dataset to manipulate decision-making. These attacks are unlike data poisoning, as they do not introduce new data into the dataset. Instead, they exploit inherent inequities that are already present in the data to achieve an attack.[30]

Across both the public and private sectors, risks now extend beyond technical compromise (like gaining system access) to include data manipulation (like altering or poisoning data). These are just five examples, showing how threat actors are attacking different parts of the AI model lifecycle. For example, in the public sector, governments have faced ransomware attacks on public infrastructure that have impacted critical services. Likewise, in the private sector, companies have experienced model interference from threat actors that affect their websites and recommendation systems.

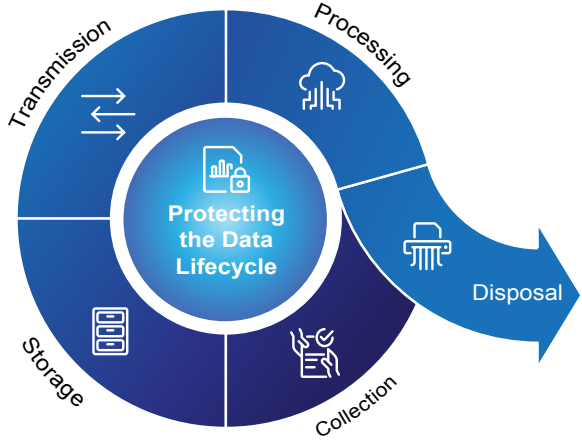
More broadly, GenAI has been used to spread misinformation. These attacks exploit model bias and erode the public trust in AI. These cases highlight that cybersecurity for enterprise data and AI is no longer confined to protecting systems. It is about defending the integrity of the data and decisions and preserving public trust in the Cognitive Era.

Data Security Foundations

This review of the threats highlights a central theme: the data used to train enterprise AI models must be secure. As organizations scale their use of AI, the volume and sensitivity of the data they manage will continue to grow exponentially. Recall the number of parameters used to train small and large language models and how the volume grows as we get to AGI. For enterprises leveraging private datasets to build private AI, it is critical to ensure the confidentiality and integrity of that data throughout its lifecycle. Building this foundation requires a "security by design" approach, combining robust technical controls with strong governance mechanisms. This strategy is essential to safeguard information while maintaining compliance with standards and regulations.

Protecting the Data Lifecycle

In general, data goes through different lifecycle phases, including collection, storage, transmission (distribution), processing (archiving and retention), and disposition. Protecting data at each stage requires a combination of preventive, detective, and corrective controls to defend against cyber threats.



Mapping Cyberattacks to AI Models

Collection

Data collection needs to be handled carefully, as it introduces opportunities for data compromise. It is essential to understand what data is being collected and for what purposes. ISO/IEC 27001:2022 provides a framework to help organizations understand how to protect information through its lifecycle. It offers a set of control categories to ensure that data collection and processing are lawful, fair, and transparent.[31]

Storage

After data has been safely collected, it needs to be securely stored. This can be in on-premises infrastructure or in cloud environments. General data protection includes encryption at rest, access controls, and segregation of sensitive data. It can also include capabilities like immutable storage, which may be part of a broader data protection strategy to mitigate cyberattacks such as ransomware. This must be part of your enterprise's zero-trust data protection strategy (more on this shortly).

Transmission

Data transmitted or distributed between systems is vulnerable to interception. To protect this data in transit, technical methodolgies like encryption are used. Encryption does not prevent data from being intercepted, but it makes the data unusable if it is.[32]

Processing

The data processing stage is a critical point where data can be intercepted or manipulated, making strong access controls essential to prevent unauthorized access. At this stage, the primary risk involves privacy breaches, especially when sensitive datasets are used for AI model training or analytics. To mitigate these risks, new computation methods have been developed. Homomorphic encryption, for example, preserves privacy by enabling operations on encrypted data without decrypting it. In addition, federated learning represents a shift toward secure, distributed AI. This allows models to be trained locally across multiple decentralized datasets. This "bring the code to the data" approach minimizes the need to centralize sensitive data, reducing exposure risks while maintaining model performance.[33]

Data Disposal or Deletion

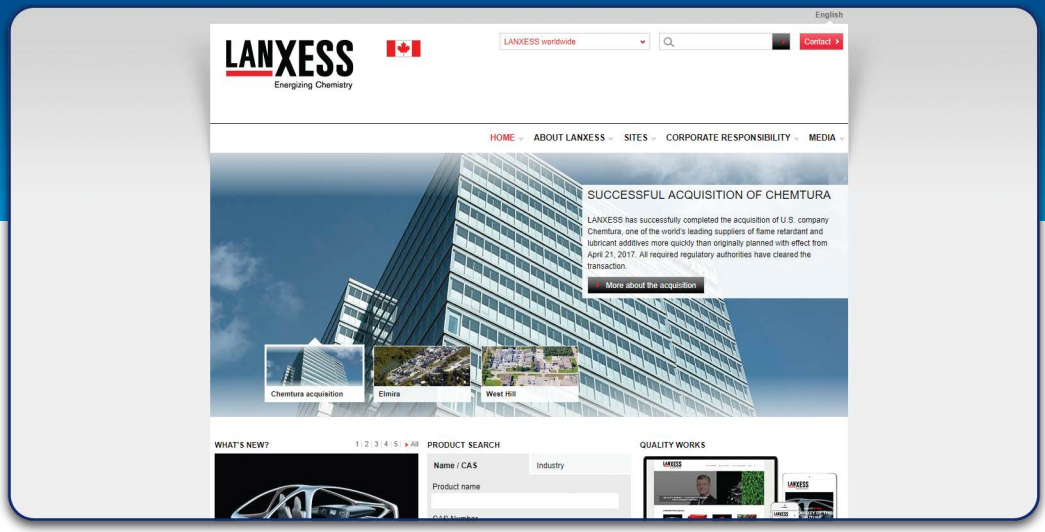
Secure deletion of data is the final stage and ensures that old or redundant data is permanently removed. Under privacy regulations, such as GDPR Article 17, there is a "right to erasure" or "right to be forgotten," which means that organizations must demonstrate that they have effectively executed deletion requests.[34]

Each data lifecycle stage is interdependent, and a weakness in any one can compromise the entire lifecycle. Understanding the risks across the lifecycle ensures that, as you develop a zero-trust data protection strategy, you have considered all aspects.

In the following case study, a leading chemicals company is using an Enterprise Information Management system to manage their data lifecycle, achieve compliance, and secure their data across multiple processes, partners, and locations.

Case Study

LANXESS



LANXESS

The core business of LANXESS is the development, manufacturing, and marketing of chemical intermediates, additives, specialty chemicals, and plastics. What follows are excerpts of an interview with the company's Process Expert, ECM.

"Given the complexity of our portfolio, when we manufacture products (chemical intermediates, additives, specialty chemicals, and plastics), our processes leave paper trails that stem from scientific research through to sales and marketing.

A typical starting point for research occurs when a customer requests a new product feature. Typically, we would then conduct research with an external partner, so there would be requirements around secure access and collaboration. Because we are a company that manufactures and distributes globally, our products, operations, and paper trails have to comply with global regulations.

An Enterprise Content Management (ECM) platform helps us to ensure that information is compliant—from the research conducted to the procedures that engineers establish to manufacture at scale, to the construction and operation of a plant, and finally, through to sales and marketing. We deal with large volumes of paper every day. Each step in a process has to be compliant and well documented, especially given that we operate in 25 countries and each one has a different set of regulations.

Compliance is a benefit as a result of effective information management, along with efficiency and productivity—specifically being able to find information more quickly. To realize these benefits, we have to show our internal customers how using the technology will make their jobs easier. ECM delivers the tools we need to balance compliance and security with usability."

Zero-Trust Architecture for Enterprise AI

We have reviewed cyber threats related to data and AI, focusing specifically on the data lifecycle and the points where attacks can occur. To protect against these threats, the National Institute of Standards and Technology (NIST) defines a Zero-Trust Architecture (ZTA) as a strategic approach to cybersecurity that assumes no implicit trust within a network. The model is based on the idea that you should never trust and always verify, and this philosophy must govern every access decision. Instead of relying on defences such as firewalls or VPNs, zero-trust leverages continuous verification and access control across all assets, users, and data flows.

According to NIST SP 800-207, the Zero-Trust model redefines traditional enterprise security by focusing on:

- **Identity-centric protection**: Every access request must be authenticated and authorized in real time.
- **Least privilege access**: Users and systems receive only the minimum level of access necessary to perform their function.
- **Dynamic policy enforcement**: Access decisions are evaluated in real time based on factors such as user behavior and data sensitivity.
- **Micro-segmentation**: Networks are divided into small, isolated zones to limit the movement of threat actors in the event of a compromise.
- **Visibility and analytics**: Continuous monitoring and threat detection ensure that certain behaviors trigger automated responses.

Zero-trust is not a single solution. It is achieved through a combination of technology solutions, including identity and access management (IAM), multi-factor authentication (MFA), encryption, continuous monitoring, and automated policy enforcement.[35] AI IAM will become a critical security component of any enterprise system.

Find out how a Latin American entertainment company is working to combine these technology solutions in their plan to evolve to a zero-trust security model in the feature below.

Case Study

A Latin American Entertainment Company

With millions of customers and thousands of employees across multiple countries, a leading Latin American entertainment company faced growing challenges managing identity and access for a large, distributed workforce. Over time, fragmented systems and manual provisioning made it difficult to maintain visibility across 15,000 user identities and more than 400 applications. The lack of unified governance slowed response times, created security blind spots, and made it harder to advance toward a zero-trust model.

To address this, the company implemented a comprehensive Identity Governance and Administration (IGA) framework, consolidating global identity data into a single source of truth and central point of control. Integrated with HR systems, Active Directory, and dozens of enterprise applications, the platform automated provisioning, deprovisioning, and access reviews—reducing manual workloads by half. Intelligent alerting, continuous attestation, and role-based access controls reinforced compliance, minimized risk, and enforced least-privilege principles across the enterprise.

The results were immediate. The company gained end-to-end visibility into more than 15,000 identities, streamlined access management, and strengthened its security posture across a global footprint. With identity governance now at the core of its cybersecurity strategy, the company is well positioned to advance its zero-trust model—extending the same rigor and automation to protect its data, applications, and AI-driven operations across the digital enterprise.

AI Security and Model Protection

Zero-trust, as we just reviewed, provides a philosophy and strategy for protecting access, but we must also consider AI security and model protection more broadly. AI models differ from traditional IT systems in that they combine logic with the ability to learn from data continuously. We reviewed earlier the attack surfaces throughout the AI model lifecycle.

To protect against these risks, organizations are adopting strategies that combine classic cybersecurity approaches with new ones. This can include training teams and models on adversarial attack approaches, watermarking models, and running red team tests of their pre-deployment environments. For context, a red team is a group that simulates real-world cyberattacks to test an organization's security. Their goal is to find weaknesses in systems, networks, and people.

Training can improve model performance by exposing it to adversarial examples during training, thereby increasing its resilience against adversarial inputs.[36] Model watermarking provides assurance and helps identify unauthorized reuse of models.[37] Red team tests are helpful in exposing vulnerabilities through simulated attacks before deployment.

In combination with a zero-trust approach, these can be powerful tactics to protect against attacks. However, these are just a few of many potential approaches, and this should be defined as part of an overall AI strategy across the enterprise.

Looking Ahead: The Future of Cybersecurity for AI

This chapter has looked at the growing importance of cybersecurity in relation to enterprise AI, highlighting the rising number of cyberattacks targeting enterprise AI systems. With reports indicating that 62 percent of organizations have faced deepfake attacks and concerns about GenAI's adversarial capabilities, the urgency of addressing AI and data-related cyber risks is apparent. As organizations leverage private data to enhance operational efficiency, they are simultaneously exposing themselves to complex vulnerabilities that threaten their AI models and data.

We also analyzed how these attacks work, outlining threats like data poisoning, backdoor attacks, and model inversion attacks. These risks illuminate some of the limitations of traditional cybersecurity approaches in protecting advanced AI systems. By understanding how these attacks relate to the different phases of the AI model lifecycle, organizations can better anticipate potential vulnerabilities and implement strategies for data protection and model security.

Looking to the future, organizations must adopt proactive, adaptive cybersecurity frameworks that incorporate AI-driven defence approaches to counter AI-powered attacks. This includes developing intelligent threat-detection systems and new risk-assessment models. Ultimately, collaboration across public and private sectors, coupled with investment in innovative cybersecurity solutions, will be essential to outpace the evolving threat landscape and ensure the safe integration of AI technologies into enterprise operations.

As organizations strengthen their cyber defenses, one truth becomes clear: security and trust are inseparable. Protecting enterprise AI systems isn't only about defending against attacks—it's about ensuring that the data powering those systems remains accurate, ethical, and reliable. In the next chapter, we'll explore the foundation of trusted AI: data governance.

The Fast Five Download

1. **Adopt a Zero-Trust Architecture for All Data and AI Systems.**
   Immediately implement a zero-trust security model that assumes no implicit trust within your network. Enforce continuous identity verification, least privilege access, dynamic policy enforcement, and micro-segmentation to minimize the risk of both internal and external breaches.

2. **Secure the Entire Data Lifecycle with Integrated Controls.**
   Mandate that all data—across collection, storage, transmission, processing, and disposal—is protected with layered security measures. This includes encryption at rest and in transit, strong access controls, immutable storage, and strict compliance with regulations like GDPR and ISO/IEC 27001:2022. Any gaps in one stage can compromise the entire system.

3. **Harden AI Models Against Emerging Threats.**
   Establish protocols to defend against AI-specific attacks such as data poisoning, backdoor exploits, adversarial inputs, model inversion, and bias exploitation. Incorporate adversarial training, model watermarking, and regular "red team" testing to identify and remediate vulnerabilities before deployment.

4. **Build Security by Design into AI Initiatives.**
   Insist that every new AI or data project incorporates security and privacy by design from inception. Require cross-functional teams—including data, IT, compliance, and security—to work together to ensure technical and governance controls are integrated into AI model development and operations.

5. **Invest in Proactive, Enterprise AI-Driven Cybersecurity Capabilities.**
   Allocate resources to develop and deploy intelligent, adaptive cybersecurity solutions powered by AI. These should include automated threat detection, risk assessment tools, and real-time monitoring to keep pace with evolving AI-enabled attack methods. Foster collaboration with industry peers and public sector partners to stay ahead of emerging threats.

Chapter Five

Data Governance—The Foundation of Trusted Enterprise AI

Before AI can think, it must trust the information it's built on. Governance is what makes that possible. It's the discipline that turns scattered content into a coherent, compliant, and usable asset—one that can safely feed intelligent systems without compromising security or integrity.

Enterprise Information Management treats governance as an operating principle, not a checklist. It rests on four interlocking pillars: metadata, permissions and access control, retention and lifecycle management, and auditability. Each one defines how data behaves across its lifespan—and together, they form the backbone of trusted intelligence. In this chapter, we'll examine each of these pillars and their relationship to optimized, compliant, and secure AI.

> *Forrester forecasts that AI governance software spending will quadruple by 2030.*[38]

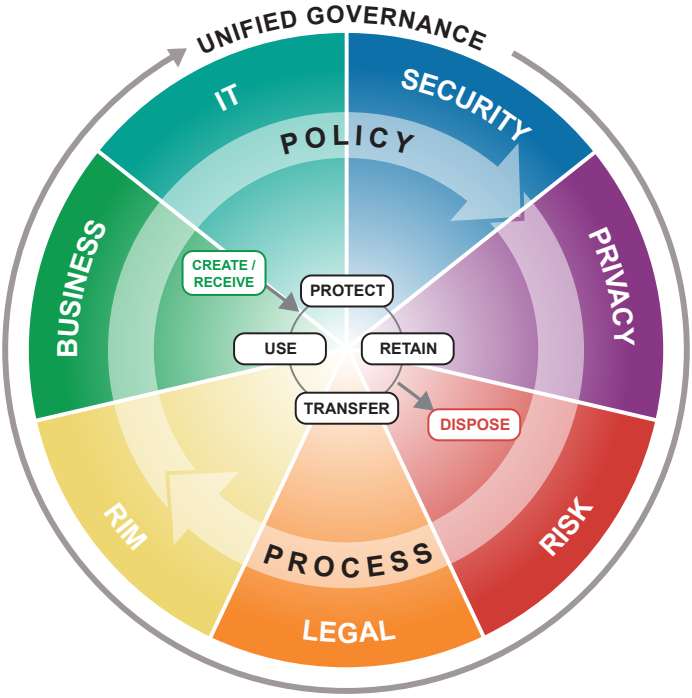
Good Governance is Good Business

Information governance is the practice of implementing policies, processes, and controls to manage information in support of regulatory, legal, risk, environmental, and operational requirements. As volumes of enterprise information increase, so too does the need for digital governance to ensure that this information is managed, secured, and searchable. From a technology perspective, governance relies on the effective management of information throughout its lifecycle, from creation or capture and classification to long-term archival or deletion.

Successful information governance programs demand that companies balance the needs and priorities to mitigate legal and business risks with the costs required to manage both unstructured and structured information. For an information governance strategy to be effective, key resources and stakeholders need to be identified, empowered, and supported; policies must be incorporated into relevant processes; education and training should be provided to all employees; technology infrastructure optimized; and the appropriate solutions implemented to support secure and reliable operations.

In the following feature, ASR Nederland is demonstrating how good governance is good for their business, enabling them to comply with regulations and providing a strategic advantage through improved customer service.

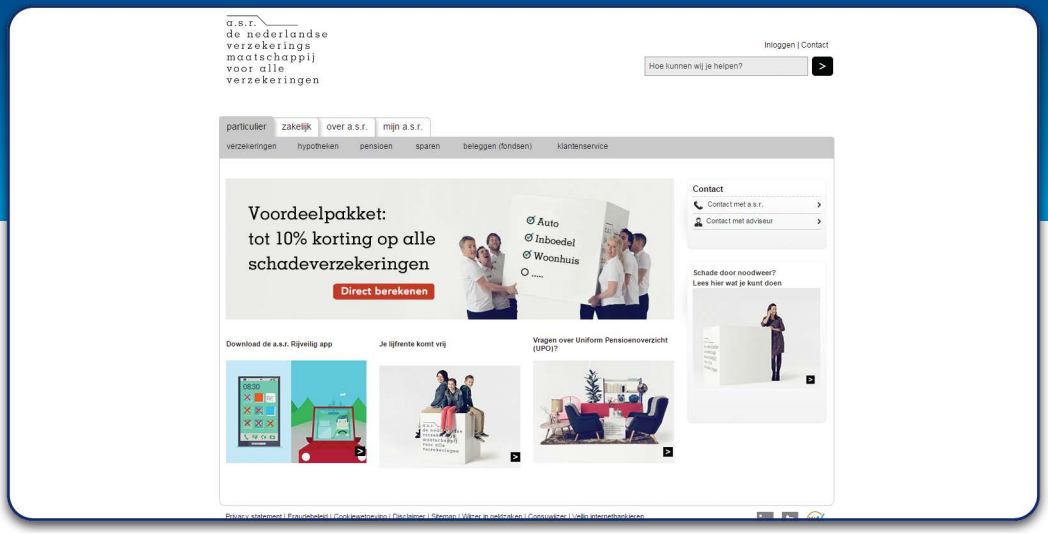
Balancing Value, Risk, and Cost



Information Governance Reference Model[39]

Case Study

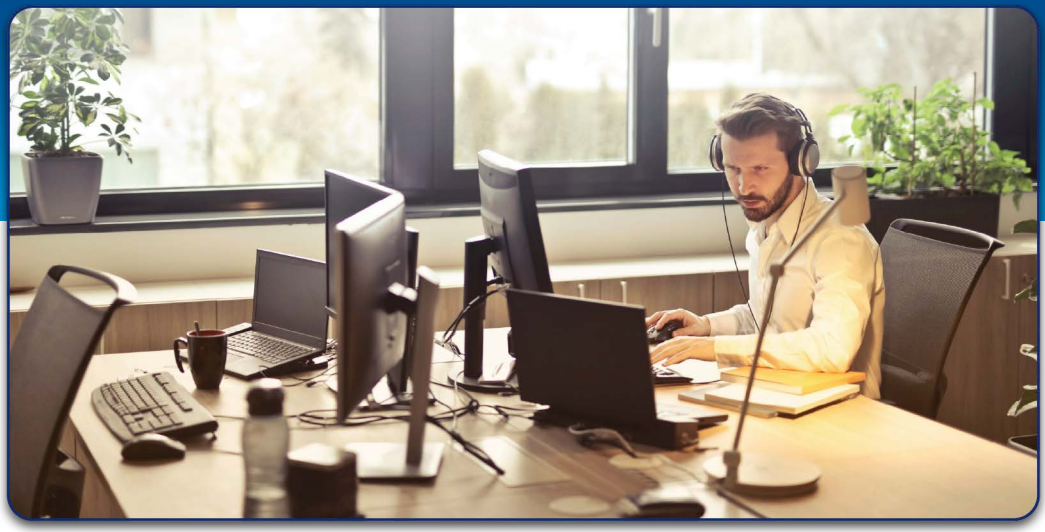
ASR Nederland



ASR Nederland

One of ASR's core business processes is disability income insurance. Previously, this claims process was paper-driven. Both medical and technical information were kept in one folder and accessible to unqualified personnel, consequently leading to a non-conformance with Dutch privacy law. In addition, ASR required a significant amount of storage space to store the continuously growing folders. ASR recognized the need for a solution that would improve business processes, enable collaboration between departments, reduce costs across the organization, and permit only authorized access to information to comply with regulations.

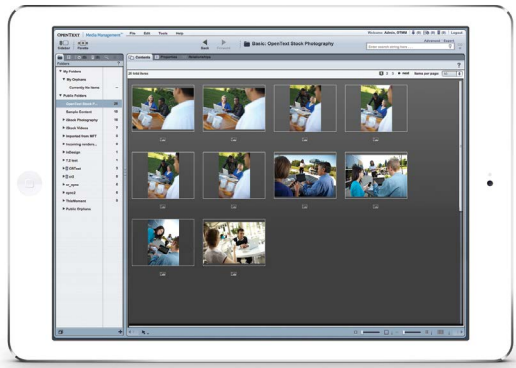
Using a combination of business process modeling and operational improvement solutions, ASR has been able to modernize existing processes while responding to legislative change. For example, medical and technical information related to disability claims are now separated and only accessible to qualified personnel—helping ASR comply with privacy legislation. As well, the entire claims management process can be measured to give management visibility into processes. The flexible environment supports a new way to benchmark so that business activities can be monitored across numerous divisions.



The solution gives ASR an enterprise-wide standard claims processing system that has dramatically improved internal efficiencies and increased productivity. Employees now process 80 percent of claims on time, which has led to a 25 percent reduction to the claims processing team, and services costs and indemnity have been significantly reduced—all of which enable ASR to deliver new products faster, comply with regulations, and provide better customer service.

Now that we've seen how data governance benefits the enterprise, let's consider the four key pillars of strong data governance introduced at the beginning of this chapter.

Pillar 1: Metadata—The Context Behind Every Decision



Metadata in a Digital Asset Management System

Metadata is the DNA of digital information—the hidden context that tells systems what something is, where it came from, and how it should be used. It links content to business purpose and transforms raw data into something searchable, governable, and meaningful.

Information enters the enterprise through many doors. Some is born digital, created by people using word processors, spreadsheets, CAD software, or email clients. Some originates in business systems, generated by Enterprise Resources Systems (ERPs), Customer Relationship Management (CRM), or databases with defined schemas and relational structures. Other content is captured from analog sources, as scanners. Then there's machine data from sensors, logs, and telemetry, and web and social content from intranets, collaboration tools, and portals. Organizations also produce multimedia—training videos, marketing assets, and recorded meetings—all of which carry operational and legal value.

Managing this diversity requires a control layer. Metadata—classification, retention tags, provenance, and sensitivity—serves as that control plane. It allows automated permissioning, targeted search, version control, and records enforcement. It's also the foundation for responsible enterprise AI: without metadata, an AI model can't distinguish between a draft and a final version, or between a public brochure and a privileged client file.

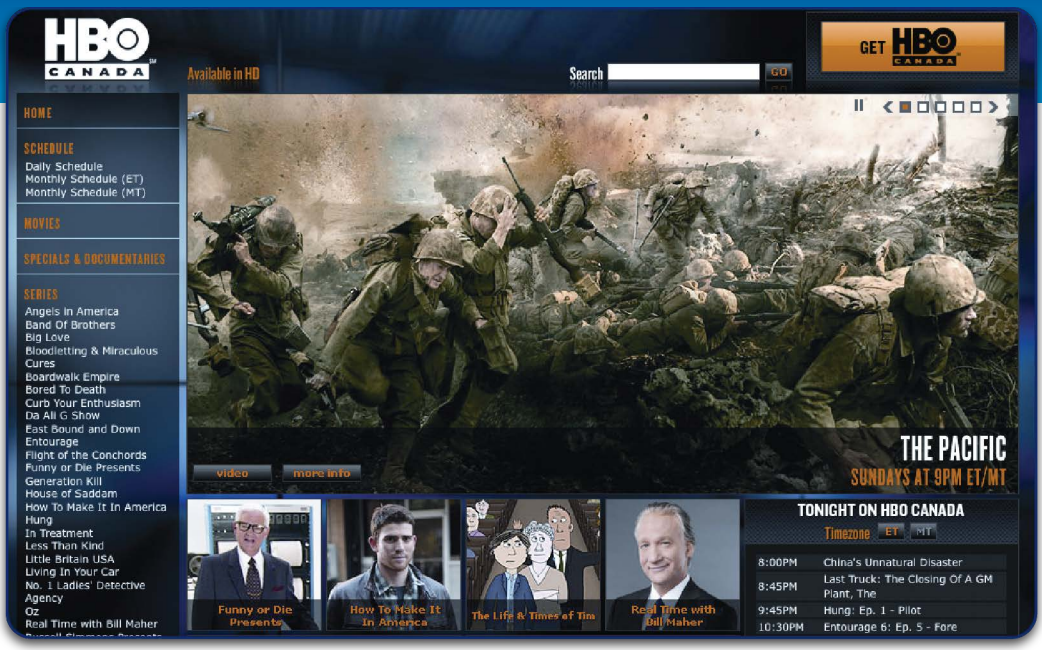
Metadata provides the essential context—who created something, when it was changed, where it came from, and how sensitive it is. These details give meaning to raw content and help both people and intelligent systems understand what can be trusted, what can be shared, and what should be protected.

Without unified metadata, AI training is unreliable or unsafe. EIM provides the framework to map governance directly to information models, ensuring that automation and AI respect the same business, legal, and ethical boundaries that already define trusted data.

Metadata isn't a static label—it's a living framework for policy enforcement and machine reasoning. As AI matures, metadata becomes the connective tissue between governed data and intelligent action. Discover how HBO relies on metadata to consolidate and manage assets throughout their lifecycle.

Case Study

HBO



HBO's Media Management System

HBO is America's most successful premium television network, offering rich digital media content, blockbuster movies, innovative original programming, provocative documentaries, concert events, and championship boxing. HBO sought a solution that would allow them to easily access and share digital content both within HBO and the larger Time Warner family. The requirements for the overall system functionality and user experience entailed the system handling large volumes of content, as well as addressing disparate databases, workflows, and use cases for each of the organizations.

HBO's Media Management implementation encompassed all of HBO's digital photographs supporting such areas as marketing, promotions, advertising, and sales. These assets can range from location shots from films to a gallery of quality professional photos of HBO celebrities.

Part of their overall strategy was to ensure careful management of metadata. Assets are tagged with corresponding metadata, such as contractual information, as early as possible to ensure that metadata travels with the asset throughout its lifecycle. This meta-tagging process is enforced with an embedded workflow component. The HBO digital asset management system is accessed by all of the Regional Offices and currently holds more than 325,000 assets.

> *If governance defines the rules, permissions enforce them—one decision at a time.*

Pillar 2: Permissions and Access Control—Who Can See What, When, and Why

Permissions define the boundaries of trust. They determine who can view, edit, or share information—and under what conditions. For decades, these principles have protected corporate and personal data. In the AI era, they take on new urgency. Every decision an intelligent system makes depends on access: what data it can see, what it can learn from, and what actions it's authorized to perform.

In an enterprise information environment, permissions are not simple IT switches—they are the enforcement layer of governance. Version control, workflow approvals, records holds, and selective publication all depend on them. Effective permission models regulate not only what users can do, but also when and why. A document that can be edited today might be locked tomorrow under a regulated process or legal hold. This dynamic control ensures that information remains traceable and trustworthy, even as it moves through complex lifecycles and collaborative environments.

Permission and Access Control

Modern EIM systems achieve this precision through granular permissions. Every object—document, folder, workflow, or image—carries its own security profile, defining access for each user and group across the system. At enterprise scale, where users may number in the hundreds of thousands, these models can translate into billions of unique permission combinations. Yet this complexity is necessary. Without the ability to assign security at the most granular level, an information system cannot truly be considered secure. It's this flexibility that allows organizations to emulate the physical controls of a secure workspace—digitally and at scale.

As AI becomes another "user" in the system, those same permission structures must extend to intelligent agents. If a document is confidential, the AI must know it too. Permissions are no longer just about control; they're about confidence—ensuring that every person and every system interacts with information purposefully, within defined boundaries, and under full accountability. This is how organizations protect privacy, preserve competitive advantage, and ensure that AI operates safely inside the zones it's authorized to learn from.

The case study below featuring a European investment bank illustrates the effective use of permissions in classifying documents across locations to achieve operational and governance objectives.

Case Study

A European Bank

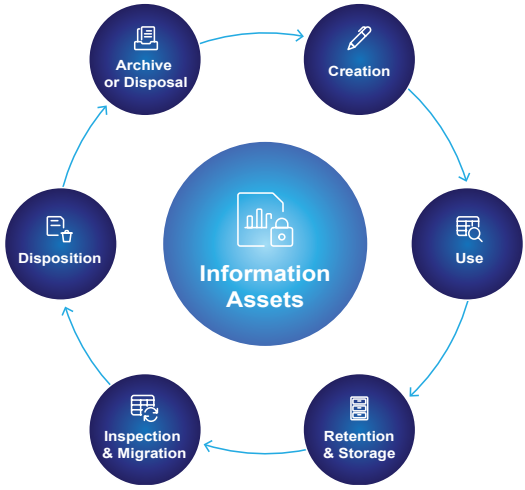
An investment bank in Europe finances capital investments aligned with European Union policy objectives—the literal infrastructure of a more integrated Europe. With operations spanning roughly 150 countries outside the EU, secure and efficient remote access to documents isn't a convenience—it's mission-critical. To achieve this, the bank implemented an EIM system as part of a broader IT modernization effort to transform every major process in the bank: borrowing, lending, and administration. The system was fully embedded within the bank's IT ecosystem so that content, data, and workflows could move seamlessly between systems, ensuring consistency and compliance across all operations.

Governance lies at the heart of this system. The investment bank developed a bank-wide taxonomy that defines not only how content is categorized but how it aligns with business processes and regulatory frameworks. Based on international best practices—including the DIRKS methodology and ISO 15489 standards—the taxonomy is paired with a sophisticated access control model that applies at the highest levels of classification. Together, these models form a living governance framework: the taxonomy maps what information exists and where it belongs, while the permissions model governs who can access it, under what conditions, and for what purpose. The result is a digital knowledge map that reflects the institution's structure, accountability, and decision rights.

This disciplined information architecture now provides the foundation for AI enablement. With a consistent taxonomy and granular permissioning, they can train AI tools to retrieve, summarize, and classify documents safely—knowing that every action taken by an intelligent agent adheres to the same access and compliance rules as a human user. Governance ensures that AI doesn't just automate tasks but operates within the same boundaries of trust that define the bank's human workflows.

The results validate the approach. Two months after launch, user adoption rates were 20 percent higher than projected, with 100 percent of vital records from new lending and borrowing operations supported in the system. Within weeks, the repository contained over 600,000 documents, growing by roughly 100,000 per week. This success demonstrated that when governance, taxonomy, and access control work together, they don't slow innovation—they make it scalable.

Pillar 3: Retention and Lifecycle Management—Knowing When to Keep and When to Let Go



Good Governance Ensures Security, Compliance, and Business Continuity

Information governance isn't just about storage; it's about stewardship. Every piece of content has a life: creation, use, revision, retention, and eventual disposal. Managing that lifecycle is how organizations stay compliant, efficient, and sustainable.

Regulated information or records come from every corner of the enterprise—ERP and CRM systems, email, documents, scanned paper, telemetry, medical devices, even aviation maintenance systems. The first step in governance is capture: bringing this information in through controlled channels such as digital mailrooms, system connectors, or APIs. Each record must arrive with its metadata, timestamps, and provenance intact to ensure authenticity and legal defensibility. Governance begins not when information is stored, but at the moment it enters the system—when the trail of trust is first created.

Once captured, records are distributed across layered storage environments that reflect their purpose and risk profile. Operational systems handle active records; content management repositories enforce versioning, classification, and retention; and immutable archives preserve communications and evidence for legal or regulatory use. In analytics environments, regulated data may be tokenized or masked to protect privacy while still enabling insight. Long-term archives—on tape, in object storage, or in sovereign clouds—provide non-erasable retention where required by law.

An EIM platform embeds retention policies directly into the systems where content lives. This ensures that the same document that supports a business decision today can be archived tomorrow—or automatically deleted when its legal or operational value expires.

The same principles that govern enterprise records now extend to artificial intelligence. As AI systems generate, consume, and learn from enterprise content, their inputs and outputs must be treated with the same rigor as regulated data. Each model interaction becomes its own record—subject to capture, classification, retention, and auditability. Governance ensures that AI learns from trusted sources, acts within defined boundaries, and produces outcomes that are explainable, defensible, and aligned with enterprise policy. In this way, the disciplines that built confidence in data governance become the guardrails for responsible intelligence.

Pillar 4: Auditability—Proof That Governance Works

In traditional records management, auditability meant logs, version histories, and paper trails. In the AI era, it also means model transparency—understanding what information shaped an outcome.

Auditability should be incorporated into the content lifecycle. Every document, transaction, and system event carries a traceable history of changes and approvals. When extended to AI, this same principle provides explainability—showing not just what a model decided, but which data contributed to that decision. This visibility is what turns governance into trust. Auditability assures regulators, executives, and the public that automation operates within defined boundaries. It transforms compliance from a reactive process into a verifiable standard for responsible intelligence.

These governance capabilities are bundled in an EIM platform in the cloud. With the evolution of AI, governance has to come first because it defines the rules of engagement between people, data, and intelligent systems. Metadata provides the map; permissions define access; lifecycle management ensures balance; and auditability proves accountability.

Without these foundations, AI is guessing. With them, it becomes part of a disciplined information ecosystem—one that learns, reasons, and acts within the boundaries that make intelligence safe, lawful, and human-aligned.

Global and Regional Regulatory Pressures[40]

A Complex Governance Landscape

In today's global marketplace, the regulatory landscape is complex, especially for global firms. Organizations are subject to industry-specific regulations and standards as well as regional or national regulations. According to these regulations, they are held accountable for their actions and must be able to access years of historical data in response to requests for information at any given time.

The relationship between compliance and governance is reciprocal. Compliance serves as a driver for information governance, and information governance, in turn, can simplify compliance. In the face of growing volumes of data, there is a strong need for governance programs to help transform organizations to enable them to benefit from the better management of their information. Enterprises that implement EIM as a governance platform are realizing the opportunities it gives them to drive business transformation efficiently and successfully through optimized intelligence and AI.

Compliance is Multifaceted

Compliance, Sovereignty, and the Shape of Modern Governance

Data sovereignty has moved from a compliance footnote to a design principle. It now defines where data lives, who can reach it, and under what jurisdiction those actions fall. In an AI-driven world, this matters deeply: models trained or hosted in one region may still be governed by the laws of another. The result is that sovereignty is no longer a legal abstraction—it's an architectural constraint. Every storage choice, API, and training dataset must now account for the regulatory geography it touches.

Privacy Laws and Regional Regulation

Europe set the global pace with the General Data Protection Regulation (GDPR). It transformed cross-border data flows from a technical assumption into a legal engineering challenge. GDPR codified principles of lawfulness, purpose limitation, minimization, and accountability—mandating clear consent, impact assessments, and data subject rights. Its enforcement has reshaped how enterprises design systems: data inventories, metadata-driven workflows, and automated deletion policies are now baseline governance features, not optional controls.

The EU Data Act extends these ideas to cloud mobility. Providers must now support interoperability and enable customers to exit cloud environments freely—no lock-ins, no excessive transfer fees. For architects, that means building with portability in mind: open standards, reversible formats, and cloud independence by design. Sovereignty, in Europe, is being legislated into existence.

Across the Atlantic, the United States is assembling a de facto federal standard one state at a time. Over twenty states now enforce their own comprehensive privacy laws, each defining consent, sensitive data, and user rights differently. This patchwork demands policy-as-code: automated rules that adapt to jurisdictional nuance and ensure the right law applies to the right record, user, or transaction. The CLOUD Act further complicates matters by granting U.S. authorities access to data held by U.S.-based providers, even when stored abroad—forcing global enterprises to think carefully about contractual control and storage sovereignty.

Canada's Layered Model

Canada approaches sovereignty through layered accountability. Federally, PIPEDA, or the Personal Information Protection and Electronic Documents Act, sets the baseline for responsible handling of personal information, permitting cross-border transfers but maintaining that organizations remain accountable for protection end to end. Its forthcoming replacement—the Digital Charter Implementation Act (Bill C-27)—introduces the Consumer Privacy Protection Act (CPPA), a Data Protection Tribunal, and the Artificial Intelligence and Data Act (AIDA), designed to govern responsible AI development and deployment.

At the provincial level, compliance becomes more granular. B.C.'s FOIPPA, or Freedom of Information and Protection of Privacy Act, reforms have relaxed residency restrictions for public data, while Ontario's health privacy law, the Personal Health Information Protection Act (PHIPA) continues to enforce strict standards for health information. Financial regulators, such as OSFI, or Office of the Superintendent of Financial Institutions, through Guideline B-10, have elevated data-location and cloud oversight to board-level responsibilities. The message is consistent: sovereignty in Canada is both practical and provincial, demanding careful mapping of where data resides and who can access it.

Global Compliance and Industry-Specific Rules

Beyond North America and Europe, data sovereignty pressures are global. China's Personal Information Protection Law (PIPL) requires explicit security assessments for cross-border transfers of "important data." India's Digital Personal Data Protection Act (DPDP) adds localization-style provisions and new transfer conditions that could influence where and how AI workloads operate. Each regulation tightens expectations for lawful transfer, explicit consent, and retention discipline.

Industry regulations amplify these demands. The U.S. HIPAA, or Health Insurance Portability and Accountability Act, is framework governs electronic health records with strict access control, encryption, and breach notification. The FDA's (Food and Drug Administration's) 21 CFR Part 11 sets standards for trustworthy electronic records and signatures in regulated manufacturing and clinical environments. The FTC, or Federal Trade Commission, enforces "reasonable care" over consumer data security, while the FAA, or Federal Aviation Administration, defines authenticity and traceability requirements for digital maintenance records in aviation. Together, they reinforce a common truth: regulated data must be captured, retained, and auditable throughout its lifecycle.

Sovereignty and AI

For artificial intelligence, these laws translate into operational limits and design choices. Enterprise AI cannot learn from what it cannot lawfully see. Sovereign clouds—built to localize storage, processing, and access—are becoming the architectural answer to regulatory fragmentation. They allow organizations to deploy AI where the data lives, respecting jurisdictional boundaries while maintaining the control needed for compliance and trust.

As EAI models grow more agentic, sovereignty will define their perimeter: what they're allowed to read, what they can retain, and how their actions are logged and explained. Compliance is no longer about static records—it's about dynamic systems that think, learn, and act under legal supervision. An Enterprise Information Management platform with embedded governance is now the operating system for intelligence itself.

Governance as the Operating System of Trust

In a world where information moves across borders, clouds, and algorithms, governance defines the rules of engagement. It ensures that data remains accurate, traceable, and defensible, no matter where it travels or how it's used.

Effective governance requires more than documentation. It demands executive sponsorship, streamlined processes, automated policy enforcement, and identity-centric security. It requires that every action on data—from capture to disposal—be visible, auditable, and aligned with legal and ethical standards.

Modern information management frameworks now embed these controls directly into daily operations. Metadata, permissions, and retention aren't afterthoughts; they're embedded logic that keeps systems honest and AI accountable. By treating information as a managed asset—one with provenance, purpose, and lifecycle—organizations transform governance from a cost of doing business into a source of competitive advantage.

Ultimately, governance is what allows enterprises to trust their intelligence. It connects the ethics of how we manage information with the mechanics of how AI learns from it. When done right, governance doesn't slow innovation—it makes it sustainable.

We discuss the governance of AI in more detail in the following chapter.

The Fast Five Download

1. **Make Governance an Enterprise Mandate.**
   Establish a cross-functional governance council that includes business, IT, legal, and compliance leaders. Give it authority to set enterprise-wide data policies, approve AI use cases, and monitor adherence. Governance isn't an IT project—it's a management discipline.

2. **Operationalize Permissions and Access Control.**
   Move from static role-based permissions to dynamic, policy-driven access. Map who can see or use specific information and extend those same controls to AI systems. Treat every AI interaction as a governed event—with audit trails, expiry dates, and explicit accountability.

3. **Map and Classify Critical Data Assets.**
   Conduct enterprise data inventories to locate high value, regulated, and sensitive information. Use EIM tools to tag content with metadata—ownership, sensitivity, and retention—so it can be used safely for AI training, automation, and analytics.

4. **Embed Compliance and Sovereignty into Architecture.**
   Design for jurisdictional complexity from the start. Choose sovereign or regional cloud configurations where data residency matters. Automate compliance through metadata and policy-as-code, so rules about where data can live or move are enforced by design, not by audit.

5. **Govern AI Like You Govern Data.**
   Treat models as managed assets with the same expectations as data: documented provenance, lifecycle control, and retraining governance. Require that every AI initiative demonstrate lawful data use, explainable decisions, and measurable ROI before it scales.

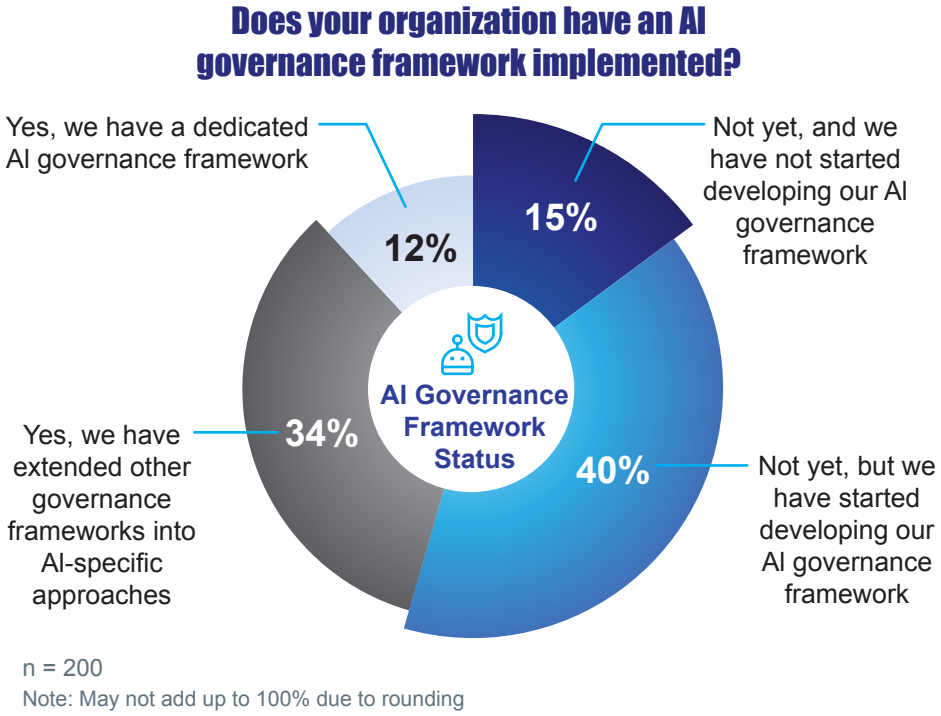
Chapter Six

The Governance of EAI

As discussed in the previous chapter, with technological advances come the need for effective governance and controls. While data governance is more mature in its history and evolution, the need for AI governance is catching up quickly. AI governance provides the policies, processes, and controls that ensure EAI technologies are aligned with organizational objectives and regulatory requirements.

In this chapter, we'll explore how governance transforms AI from a technical capability into a trusted, strategic asset. We'll explore the importance of AI governance in both private and public sectors with a focus on scope, ethics, compliance, risk management, and accountability.

According to Gartner, only 12% of organizations have implemented a dedicated AI-governance framework, while 55% report they have not yet done so.[41]



Gartner Survey of IT and Data and Analytics Leaders on AI Strategy[42]

As AI becomes embedded in every aspect of business, governance has emerged as its critical foundation. Effective AI governance assigns responsibility, defines oversight, and ensures that intelligent systems operate ethically and transparently. Without it, organizations risk exposing themselves to bias, privacy breaches, and reputational harm. Yet many still struggle—lacking the expertise, coordination, and unified data needed to govern AI at scale.

Looking ahead, governance will determine not just how AI is deployed, but how it earns trust. Future-ready enterprises are already aligning governance with evolving regulations and embedding responsible AI practices into their operations from the start.

In the following case study, read about how a global consulting firm is one of Gartner's 12 percent when it comes to AI governance.

Case Study

A Global Consulting Firm

The firm is an innovative leader in online and mobile strategy, design and development, and cybersecurity, offering world-class knowledge and resources from the leading global business and technology consultancy. They recognize today's digital inflection point, one where artificial intelligence, automation, and cloud technologies are reshaping business models, workforce dynamics, and even organizational culture. The following are excerpts from an interview from a top tech analyst at the firm.

"Alongside digital transformation, data itself has evolved. It's no longer just about transactions—it's about context. Value now lies in the relationships between structured and unstructured data: the conversations, images, and signals that give meaning to what's measured. AI and analytics make it possible to extract that meaning at scale, transforming unstructured information into actionable insight. When combined on a unified information platform, AI-driven analytics unlock exponential potential, revealing connections and risks we could never see before.

But with this opportunity comes responsibility. As AI deepens its role in enterprise decision-making, the importance of cybersecurity has never been greater. Every intelligent system depends on trusted data and secure infrastructure. A robust security practice that encompasses governance, compliance, and proactive defense helps secure the company's data. We understand that no matter how technologies evolve, the fundamentals remain constant: clear frameworks, enforced policies, and vigilant oversight, consolidated on an EIM platform.

As enterprises embrace hybrid and multi-cloud models, the question isn't just where to store data, but how to protect it. AI amplifies both the power and the risk of digital transformation, making cybersecurity not just a technical safeguard, but the foundation of trust in an intelligent enterprise."

What Is the Scope of EAI Governance?

AI governance guides how an enterprise develops, deploys, and manages AI in alignment with its strategic objectives and regulatory obligations. As an extension of both corporate and IT governance, EAI governance addresses challenges such as model oversight, bias, data management, cybersecurity risk controls, and compliance. Most organizations now establish policies on responsible AI use that embed principles such as fairness, transparency, and accountability throughout the AI lifecycle. These guardrails are becoming essential for ensuring trustworthy, responsible AI adoption and maintaining public confidence in modern intelligent systems.

Leading frameworks today that guide EAI governance include the Organisation for Economic Co-operation and Development (OECD) AI Principles, the European Union's proposed AI Act, the National Institute of Standards and Technology (NIST) AI Risk Management Framework (AI RMF), and the International Organization for Standardization (ISO) standards on AI.

Increasingly, EAI governance also extends beyond the enterprise's immediate systems to the models and infrastructure it depends on. New regulatory frameworks, including the EU AI Act (2024) and U.S. Executive Order 14110 on AI Safety (2023), distinguish between AI system governance (the way an enterprise manages its own use of AI) and model-level governance (the obligations of those developing or fine-tuning general-purpose or "frontier" AI models). Enterprises are now expected to perform due diligence on model suppliers before integration (NIST, 2023; European Commission, 2024). This introduces accountability across the AI supply chain.

> *Data ethics is about more than compliance: it's about doing the right thing, even when the law doesn't require it.*[43]

Ensuring Ethical and Responsible AI

Ethical governance ensures that AI systems are fair, transparent, and respectful of human rights. While the term "ethical AI" may feel contemporary, its roots trace back decades to foundational discussions in computer ethics. In his landmark 1985 essay, "What Is Computer Ethics?", Moor highlighted,

> "A typical problem in computer ethics arises because there is a policy vacuum about how computer technology should be used. Computers provide us with new capabilities and these in turn give us new choices for action. Often, either no policies for conduct in these situations exist or existing policies seem inadequate. A central task of computer ethics is to determine what we should do in such cases, i.e., to formulate policies to guide our actions. Of course, some ethical situations confront us as individuals and some as a society. Computer ethics includes consideration of both personal and social policies for the ethical use of computer technology."[44]

Later writings considered AI ethics specifically, including the "Principles on Artificial Intelligence" (2019) by the OECD, and, more recently, "Recommendation on the Ethics of Artificial Intelligence," published by the United Nations Educational, Scientific and Cultural Organization (UNESCO) in 2022. With 194 member states in the UN, this latter set of recommendations is the most wide-reaching framework published to date.

The recommendations provide a strong rationale for the need for ethical guidelines:

> "AI systems raise new types of ethical issues that include, but are not limited to, their impact on decision-making, employment and labour, social interaction, health care, education, media, access to information, digital divide, personal data and consumer protection, environment, democracy, rule of law, security and policing, dual use, and human rights and fundamental freedoms, including freedom of expression, privacy, and non-discrimination. Furthermore, new ethical challenges are created by the potential of AI algorithms to reproduce and reinforce existing biases, and thus to exacerbate already existing forms of discrimination, prejudice, and stereotyping."[45]

The recommendations further observe that, as AI takes on more and more tasks previously executed by human beings, its impact on humanity will expand. It has the potential to profoundly alter how we understand the world around us, as well as our very sense of self.[46]

Ethical AI recommendations include (but are not limited to) the following principles:

- **Proportionality and Do No Harm**: Covering the breadth of use of AI and the appropriateness to the context of use
- **Safety and Security**: Avoidance of harm, including security risks
- **Fairness and Non-Discrimination**: Including requirements to promote social justice and to safeguard fairness
- **Sustainability**: Including a consideration of human, social, cultural, economic, and environmental impacts on sustainability
- **Right to Privacy, and Data Protection**: Governing the use of data for AI
- **Human Oversight and Determination**: Maintaining human control over AI
- **Transparency and Explainability**: Including a broad understanding and explanation of the use of AI and relevant data in specific cases
- **Responsibility and Accountability**: Promoting human rights and freedoms
- **Awareness and Literacy**: Leveraging education, training, and media literacy to increase awareness of the use of AI
- **Multi-Stakeholder and Adaptive Governance and Collaboration**: Respecting international laws and national sovereignty[47]

As ethical AI governance institutionalizes the "Do no harm" principle, embedding values such as non-discrimination, accountability, and transparency is critical for businesses and imperative for public sector organizations. Shifting the conversation from a checklist to an engineered system means we should think of ethics as infrastructure. That means embedding ethical guardrails into every phase of the AI lifecycle. In doing so, ethics becomes part of your operational architecture, defining what your organization stands for and how it behaves—not just what it produces. As enterprises move toward responsible innovation, ethical and responsible AI are indispensable for sustaining growth and trust.

Comprehensive AI Governance Framework

Managing Risks and Safeguarding Trust

AI introduces unique risks not covered by traditional IT governance. For this reason, strengthening accountability and oversight is essential. From a reliability perspective, because AI can fail in unpredictable ways, rigorous testing is required with strong fallback protocols. On the quality and performance side, continuous monitoring helps minimize risks. Most important, though, is ensuring security, privacy, and safety, because incidents can damage an organization's reputation and erode public trust. Integrating AI risk management with broader Enterprise Risk Management (ERM) processes ensures AI risks are treated with the same rigor as financial or operational risks.

The following best practices make up a robust governance framework:

Integration with Enterprise Governance

As pointed out above, EAI governance intersects with existing structures—corporate governance, IT governance, and risk management, and requires the definition of roles, responsibilities, and oversight at all levels. Trusted AI governance is achieved through task based policy management as an extension to existing RBAC (Role Based Access Controls) for humans—and now, agents. Building trust requires cross-functional teams that blend technologists, ethicists, legal advisors, and sometimes, even customers. Because AI is a newer technology, the risk profile should be considered high while the full scope of risks is being quantified.

Policies and Standards

For enterprise organizations and their employees, having clear policies, codes of conduct, and internal standards makes expectations explicit and enforceable. These must be reinforced often and coded into AI agent business rules so autonomous decisions follow the exact same ethical framework to achieve desired outcomes. Most critical is the use of protected or private company data and ensuring that the guidelines for its use with respect to public AI models are straightforward.

Auditability

Governance requires robust documentation, logging, and audit trails for all AI systems, supporting both internal reviews and regulatory audits. Setting this as a core operating principle can ensure you are proactive and identify issues before they happen. We described these aspects of data governance in the previous chapter.

Transparency

Transparency is the foundation of trustworthy AI governance—it ensures that decisions made by intelligent systems are understandable, traceable, and open to scrutiny. The principle of Transparency, Explainability, and Contestability (TEC) provides a structured approach: organizations must design monitoring processes and conduct regular "health checks" to evaluate how clearly AI systems communicate their reasoning and how fairly they operate. By documenting decision logic, disclosing data use, and enabling users to question or challenge outcomes, enterprises transform AI from a black box into an accountable, human-centered system—one where visibility, fairness, and trust are built into every decision.

Development and Operations

A privacy-by-design approach to AI development and operations ensures that data protection is engineered into every stage of the system lifecycle—from conception to deployment and beyond. Rather than treating privacy as a compliance requirement or an afterthought, it becomes an architectural principle guiding how data is collected, processed, and retained. This means minimizing data use to what's strictly necessary, applying anonymization and encryption by default, and embedding user consent and control mechanisms directly into workflows. Continuous monitoring and privacy impact assessments keep systems accountable as they evolve. By aligning development and operations with privacy-by-design principles, organizations not only reduce regulatory risk—they also build trust, resilience, and a competitive advantage grounded in ethical innovation.

Incident Response

While Chapter 11 covers the need for a different approach to operations, it is worth highlighting, in the context of AI governance and risk management, that protocols for rapid response to AI failures, including human appeals and remediation, are essential for accountability and continuous improvement.

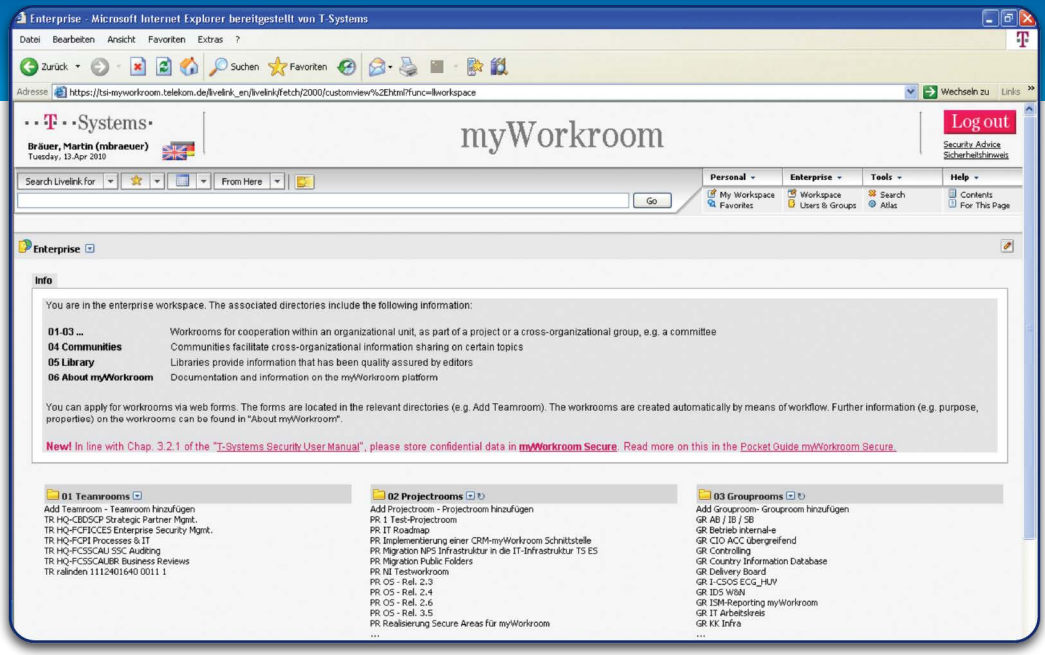
All of these elements are critical to managing risk and safeguarding trust. Because many organizations have not yet fully operationalized AI, it is worth considering how these elements impact your overall strategy.

Today's AI governance also demands explicit security and resilience controls tailored to generative AI. Traditional IT security frameworks often do not cover threats related to generative systems like prompt injection, hallucination, output manipulation, etc. NIST's Generative AI Profile (2024 draft) and CISA's Secure by Design guidance (2024) recommend AI-specific threat modeling, adversarial red-teaming, monitoring for data exfiltration, and provenance tracking of model outputs (CISA, 2024; NIST, 2024). Organizations should institute measures for novel risks associated with generative models to ensure security, reliability, and accountability across the entire generative-AI lifecycle.

In the following feature, a European telecom company is managing the lifecycle of its information to meet compliance and data governance objectives, with strict rules about how long to keep information and when to dispose of it.

Case Study

T-Systems



Company-Wide Enterprise Information Management System

With operations in more than 20 countries, T-Systems, the busiest customer brand of Deutsche Telekom, is the provider of choice for conducting global business by many major European customers. Around 160,000 companies and public bodies make use of T-Systems' integrated services—everything from managing data centers and global Internet protocol services to developing and administering applications.

T-Systems' teams needed a platform that would allow them to come together quickly and easily to exchange information and ensure the professional and efficient execution of customer projects. Approximately 40,000 T-Systems employees are now using a company-wide Enterprise Content Management (ECM) platform for collaboration, document management, and knowledge management.

T-Systems is enhancing its collaboration platform with an extranet gateway to facilitate collaboration with customers and partners and a lifecycle management system for project rooms with storage periods of up to 10 years. This second feature will enable T-Systems to meet its compliance obligations in the area of corporate governance, while simultaneously making valuable, but dormant project information searchable at a later date.

Leading Frameworks, Regulations, and Standards

The regulatory landscape for AI is rapidly evolving, with compliance now a major governance driver. There are a combination of voluntary frameworks, like the National Institute of Standards and Technology (NIST) Risk Management Framework (RMF), and obligatory frameworks (like the EU AI Act) covered in Chapter 5. But even the voluntary frameworks are becoming a requirement for many organizations in terms of implementing a structured approach to trustworthy AI. Governance frameworks serve a purpose in helping to translate requirements into controls, policies, and oversight requirements to guide enterprises through adoption.

Although the regulatory landscape is evolving, there are a variety of frameworks available today that can help an enterprise structure AI governance:

OECD AI Principles: These were adopted in 2019 by 46 countries and represented one of the first standards on AI governance. Five key principles were outlined pertaining to AI governance, as follows:[48]

1. AI should benefit people and the planet by driving inclusive growth and well-being.
2. AI systems should be designed to respect human rights, democratic values, and diversity.
3. There should be transparency and explainability in AI systems.
4. AI systems must be robust, secure, and safe throughout their life cycles.
5. Organizations and individuals developing, deploying, or operating AI should be accountable for its outcomes.

EU AI Act: The Regulation of the European Parliament and of the Council Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) was adopted in 2024. It is one of the first comprehensive legal frameworks for AI, setting requirements based on different risk levels, ranging from minimal to unacceptable. Key requirements of the Act are as follows:[49]

- Transparency for AI-generated content and biometric systems
- Strict compliance, testing, and documentation for high-risk AI systems (e.g., healthcare, critical infrastructure, and public administration)
- Prohibition of AI use that manipulates behavior or exploits vulnerabilities
- Mandatory human oversight, risk management systems, and alignment to the EU's digital and data governance regulations

NIST AI RMF: The NIST Risk Management Framework, published in 2023, provides a voluntary, widely adopted framework for identifying, assessing, and managing risks in AI systems. It looks at mapping context and intended use, measuring AI risks, managing those risks through a series of controls, and governing AI systems across their lifecycle. This framework is designed to work alongside security guidelines for zero-trust architectures.

The framework acknowledges that AI technology is still evolving: "The AI RMF is intended to be practical, to adapt to the AI landscape as AI technologies continue to develop, and to be operationalized by organizations in varying degrees and capacities so society can benefit from AI while also being protected from its potential harms."[50]

ISO/IEC 42001:2023: ISO and the International Electrotechnical Commission (IEC) have developed standards for AI management and governance. This includes standards on AI Management Systems (AIMS) (ISO/IEC 42001:2023), AI Concepts and Terminology (ISO/IEC 22989:2022), and AI System Lifecycle Processes (ISO/IEC 23053:2022).

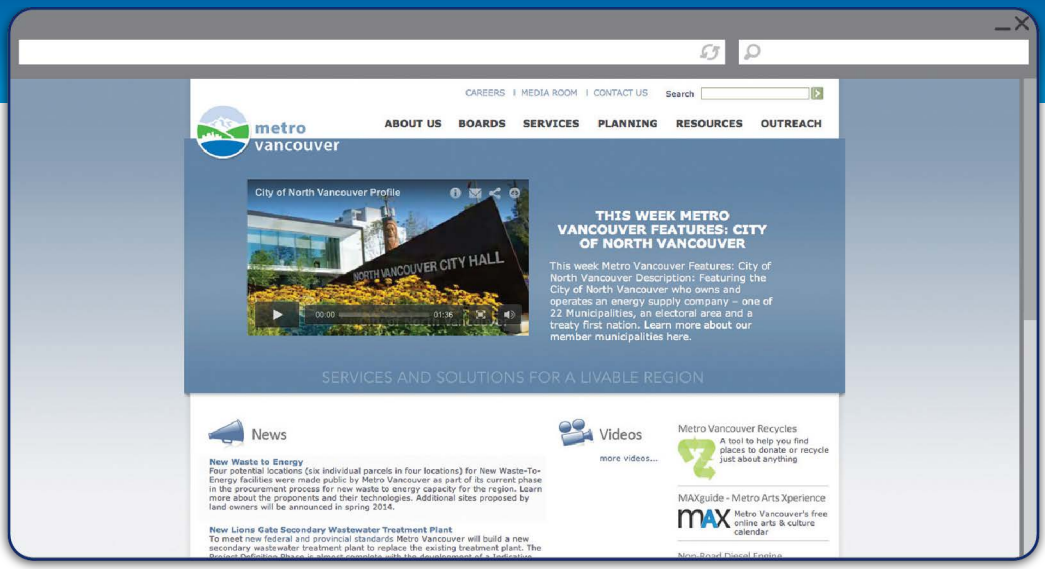
Together, these standards and principles give enterprises a structured foundation for responsible innovation. They translate high-level ideals—fairness, transparency, accountability—into actionable governance practices aligned with global expectations. By anchoring their AI programs to these frameworks, your organization can build systems that are not only compliant, but consistent, explainable, and trusted across borders.

There are other standards and frameworks, but these are the most broadly used and adopted. Over time, as technology evolves, new frameworks will emerge, so taking an adaptable approach to how you define controls is key to preventing future rework.

In the following feature, Metro Vancouver is proving that good governance is good business. An EIM backbone is helping to make sure that the Region can prove through audits that the documents in the system are trustworthy records—and that they comply with statutes and regulations while promoting good business practice.

Case Study

Metro Vancouver



Metro Vancouver

Metro Vancouver is one of 29 regional districts that were created by the provincial government to ensure that all British Columbia residents have equal access to commonly needed services. Regional parks, affordable housing, labor relations, and regional urban planning are significant services provided directly to the public. The Region supports thousands of full-time employees and serves a population of over three million.

The Region needed a central, secure repository for storing and distributing electronic records. An e-government solution would enable them to enforce retention periods and disposition rules based on preset periods to help control risks, reduce storage costs, and ensure regulatory compliance. They were also looking for an improved user experience for the profiling of documents that included automation and improved accuracy.

The system currently contains almost two million documents. An automated records management solution removes the complexities of electronic records management, making the process transparent to the end user. It maps record classifications to retention schedules, which fully automates the process of ensuring that records are kept as long as legally required and then destroyed when the time elapses. Enforcing governance across the region, each of its 14 departments is responsible to comply with policies, best practices, and procedures issued by the corporate records team. The system is helping to make sure that the Region can prove through audits that the documents in the system are trustworthy records—and that they comply with statutes and regulations while promoting good business practice.

The Path Forward on EAI Governance

AI governance is essential for both the public and private sectors. The implementation timelines and scope are relatively similar; however, there are a few subtle differences. For the public sector, the emphasis is on transparency and citizen trust. Governance is driven by public accountability, ethics, and compliance with human rights. For the private sector, the focus is more on innovation, business risk, and regulatory compliance. Governance is integrated with corporate social responsibility and Environmental, Social, and Governance (ESG) agendas, balancing agility with impact. Both sectors benefit from aligning with international frameworks and standards, and both must treat AI governance as a dynamic, evolving program.

Overall, EAI governance ensures ethical principles, legal compliance, risk management, and accountability are embedded throughout the AI lifecycle and across organizational boundaries. Successful AI governance blends high-level principles with concrete processes and tools, supported by a culture of responsibility at all levels. As AI technologies and regulations evolve, ongoing investment in governance will be critical, not only to mitigate risk but to build trust, drive sustainable innovation, and secure competitive advantage.

AI governance goes beyond purely technical considerations to incorporate ethical and social dimensions too. Many organizations now adopt formal policies around responsible AI use, embedding key principles like fairness, transparency, accountability, and respect for human rights throughout the AI lifecycle. These guardrails are becoming essential not just for compliance, but for sustaining trust in AI-driven operations. Without them, the promise of intelligent systems risks being undermined by ethical lapses, privacy breaches, or governance failures.

The next wave of AI governance concerns the alignment and control of autonomous and agentic AI systems that can initiate actions without explicit human approval. Governance requirements are expanding to include autonomy limits, real-time supervision, and escalation pathways when models display deceptive or goal-seeking behaviors (UK AI Safety Institute, 2024). Similarly, compute and capability thresholds are becoming a policy tool to identify when AI development should trigger external review (NIST, 2024; CISA, 2024). For enterprises, this means EAI governance must shift from static policy compliance to continuous monitoring, assurance, and adaptive risk management. Organizations that institutionalize AI governance as a living system of controls, oversight, and external validation will be best positioned to innovate responsibly in the frontier.

In the following case study, discover how an enterprise software leader reduced document types by 96 percent to prepare for AI innovation and automation.

Case Study

A Global ERP Vendor

> *The possibilities for employee self-service are unlimited. For example, if an employee submits a document to change their address or marital status, AI-powered automation can update their employment record without anyone from the HR team getting involved.*
>
> Head of Global HR Delivery

Managing millions of employee records across a global workforce presented significant governance and compliance challenges. Manual, time-consuming processes made regulatory requirements—such as GDPR—difficult to meet consistently, while aging systems lacked compatibility with next-generation HR technologies. To support modernization, the organization set out to transform its information governance framework, automating compliance and embedding "security and privacy by design" into every stage of HR data management.

The new governance model unified document retention, disposition, and access policies across regions, replacing thousands of inconsistent templates with standardized global formats. Automated retention scheduling and deletion policies now ensure continuous compliance, reducing operational risk while freeing HR teams from manual oversight. Strong encryption, access controls, and audit trails reinforce data integrity, while governance automation enables faster, more reliable decision-making.

With this foundation in place, the organization is preparing for the next phase—leveraging AI to enhance document classification, automate records management, and further strengthen governance at scale. By combining robust technical controls with strong oversight and accountability mechanisms, it is evolving from compliance maintenance to proactive governance—building a secure, data-driven environment ready for intelligent innovation.

The Fast Five Download

1. **Make AI Governance a Strategic Imperative.**
   Establish executive support and clear ownership for AI governance to ensure all initiatives align with ethical, legal, and organizational objectives.

2. **Build Ethics and Accountability into the AI Lifecycle.**
   Embed ethical guidelines, risk controls, regulatory compliance, and accountability measures at every stage, from design to deployment and monitoring, to actively prevent bias and unintended harm.

3. **Activate Leading Frameworks and Standards.**
   Implement frameworks such as the OECD Principles, EU AI Act, NIST AI RMF, and ISO 42001 to translate best practices and regulatory demands into actionable controls and oversight.

4. **Integrate AI Governance Across the Enterprise.**
   Align AI governance with corporate, IT, and data governance by clarifying roles, responsibilities, and processes, ensuring comprehensive oversight from project planning through decommissioning.

5. **Drive Continuous Improvement and Trust.**
   Institute ongoing audits, adapt governance protocols as technologies and regulations evolve, and embed a culture of learning and accountability to sustain trust and long-term value.

Chapter Seven

The Architecture of Sovereign EAI Implementations

As described in earlier chapters, 90 percent of the world's data is locked behind firewalls, residing in private, proprietary, or sensitive environments. Only ten percent is publicly accessible, and it is this minority that has largely powered the first wave of generative AI (GenAI). To unlock the full potential of GenAI, Agentic AI, and ultimately Artificial General Intelligence (AGI), public and private sector enterprises must develop secure, sovereign mechanisms to access and utilize the 90 percent without compromising privacy, security, or national control. In this chapter, we'll show you how you can do this using a hybrid approach that integrates sovereign data and EAI on an EIM platform.

> *New risks—such as foreign administrations being empowered to push the kill switch—have raised concerns at global organizations.*[51]

In today's digital economy, data is the most foundational asset. It fuels innovation, drives productivity, and underpins national security. As AI transforms every sector and geopolitical considerations rapidly evolve, it's more critical than ever for leaders to safeguard the privacy and protection of their data, infrastructure, and AI capabilities. This challenge extends from the enterprise to the national level, where it is imperative that countries develop sovereign plans for AI leadership.

A country's ability to lead in the AI era depends on its ability to control and harness its most valuable digital resource: data. Without full control, countries risk having their digital infrastructure annexed, either technically or legally, by foreign jurisdictions. This is not just a matter of innovation; it is a matter of national security.

IT leaders increasingly regard sovereignty over both infrastructure and data as a strategic imperative. In a world of geopolitical tension, trade restrictions, and rapidly evolving regulatory frameworks, dependency on distant or politically constrained providers has become a material business risk. Forward-looking organizations aren't just meeting compliance obligations; they're adopting resilient, jurisdiction-aware architectures that can withstand disruption, maintain legal certainty, and preserve operational continuity under any circumstance.[52]

Digital Sovereignty Definitions

Increasingly, discussions globally on data and AI have focused on the importance of digital sovereignty. This refers to the ability of a nation or organization to maintain control over its digital assets, data, systems, and operations, ensuring independence from external influence and compliance with domestic regulations.

Depending on the sensitivity of the data, achieving digital sovereignty may require one or more of the following elements:

- **Data Sovereignty**: Ensuring that data is stored, processed, and managed within a specific jurisdiction, with strict controls to prevent access or transfer to foreign entities or under foreign laws.
- **Operational Sovereignty**: Ensuring that operations are situated in a specific jurisdiction, and that personnel managing digital assets are citizens of that jurisdiction with appropriate security clearances.
- **Technological Sovereignty**: Maintaining control over infrastructure, including physical data center security, access rights, and management of hardware, software, and encryption keys. This includes sovereignty of the control plane, a set of services critical for integrating applications with underlying infrastructure.
- **Legal Sovereignty**: Ensuring that technology vendors and cloud service providers are governed exclusively by a specific jurisdiction's law.

A Balanced Hybrid Approach

To compete in the AI era, nations must leverage the immense scale, innovation, and flexibility of global public cloud services. This necessity, however, creates a fundamental tension with the security imperative to maintain sovereign control. A hybrid model is the essential solution to this challenge. This approach balances both requirements by acknowledging that not all data requires the same level of protection. Sensitive sovereign data is protected on secure platforms and a domestically owned and operated infrastructure layer, while public datasets and citizen-facing services can utilize global hyperscalers to achieve the necessary scale.

Discover how a global leader in technology and services leveraged a hybrid approach of data and AI with GenAI to analyze historical cases involving millions of documents and thousands of terabytes.

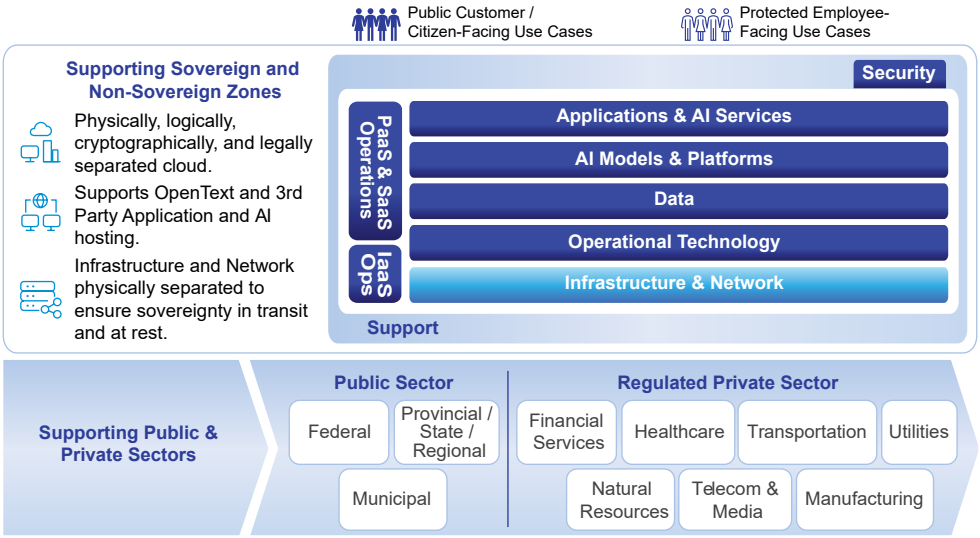
Case Study

A Global Tech Leader

A global leader in technology and services shapes universal trends in automation, electrification, digitalization, and connectivity. Its strong industrial presence drives innovation to improve processes, including optimizing legal operations.

As a global enterprise, legal challenges are an inevitable part of operating at scale, but lengthy internal investigations and unwieldy early case assessments were hampering their ability to define next steps and diverting the company from innovating and creating value. Inefficient processes led to increased costs and risk, given the absence of technology to support case knowledge and control early in the process. The company sought a technology solution to help them make better and faster decisions by quickly processing and analyzing large amounts of internal data—and help shape how the legal case proceeded.

The company adopted a hybrid approach. Their legal team used it with GenAI to crunch vast datasets in the case assessment phase. They then used a large language model to ask the relevant questions and get answers within minutes to determine their case strategy. The global company was able to transform their legal workflows, enabling faster data-driven decisions and proactive investigations. Through AI integration and training, its legal teams were able to deliver superior service.



High Level Architecture of Sovereign Data and AI

Architecture for Sovereignty

The architectural framework above provides a high-level view of the critical components for enabling the Sovereign Data and AI capabilities on an EIM platform for both the public and private sectors. This framework ensures that secure services are delivered to customers in an efficient manner, protecting their critical data.

Key aspects of this architecture include:

- **Dual Data Architecture**: Sensitive data is protected within a sovereign layer, while publicly available data is processed in a hybrid cloud environment (i.e. an environment that integrates public and private cloud).
- **Multi-Agent AI Model**: "Private AI Agents" operate within the sovereign stack, while "Public AI Agents" deliver services via hybrid cloud, ensuring secure boundaries and data integrity.
- **Extensibility**: Designed to incorporate additional datasets.
- **Data Security and Governance**: Adhering to policy and controls around protection and use of data.
- **Core Principles**: Trust, security, national control, and resilience.

What follows is a breakdown of the above architecture.

The Infrastructure and Network Layer

Sensitive data is hosted within infrastructure operated by trusted telecommunications and data center providers. These environments are engineered to meet the most stringent security and sovereignty requirements, employing zero-trust protocols—security frameworks that verify every connection, device, and user continuously rather than assuming any element is safe—and air-gapped configurations, in which critical systems are physically or logically isolated from public networks to prevent unauthorized access or data leakage. Deployments remain within defined national or regional borders, with operations managed exclusively by security-cleared personnel to ensure compliance with all applicable laws, regulations, and defense-grade standards.

For data and workloads that do not require full sovereignty, such as publicly available datasets or citizen- and customer-facing digital experiences, the framework incorporates global hyperscalers. These platforms provide the scale, flexibility, and advanced tooling needed to support innovation, responsiveness, and cost-efficiency, while operating under strict governance boundaries that prevent sovereign data exposure.

Across both zones, the architecture is unified by a common technology stack integrating capabilities in the areas of data and information management, AI models, and AI applications.

The Operational Technology Layer

The operational technology layer is critical for enabling the deployment of data, AI models, platforms, applications, and AI services. It provides the bridge between infrastructure, network, and applications.

In a multi-cloud and hybrid world, standardization at the operational layer is essential. Adopting open protocols and interoperable frameworks allows organizations to maintain portability of workloads—the ability to move applications and data seamlessly between on-premises, private, and sovereign clouds without refactoring or security trade-offs. This is particularly critical for AI workloads, where compute intensity, data gravity, and regulatory constraints demand both flexibility and control.

Operational technology governance also extends to monitoring, observability, and automation. Unified control planes and orchestration tools enforce consistent configurations, patch management, and compliance verification in real time. In this sense, the operational layer ensures that every AI deployment, from model training to inference, runs within trusted boundaries, adheres to defined jurisdictions, and scales with confidence.

The Data Layer

As the foundation for EAI, the data layer must support the needs of both the public and private sectors. It enables secure, intelligent, and scalable data management across government and public sectors with the extensibility to support private sector needs.

The architecture requires support for both explicit and implicit data hierarchies. Explicit structures include folder hierarchies, taxonomies, schemas, version control, and audit logs. Implicit structures include metadata fields, semantic relationships, ontologies, tags, and usage-based clustering. These are woven together using metadata-driven orchestration and semantic engines, enabling AI systems to reason across both structured and unstructured data.

Agentic Use Cases

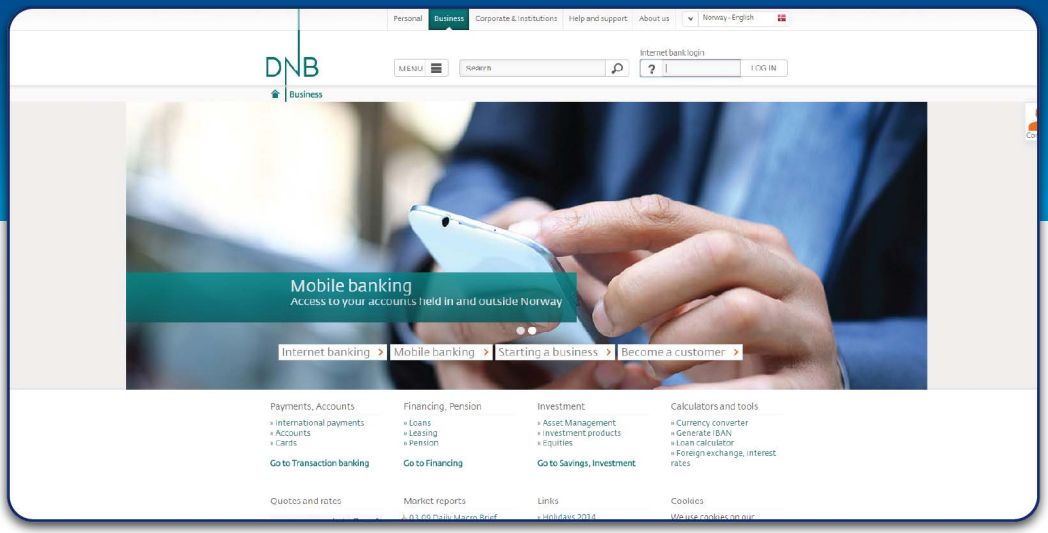
Agents will drive productivity and efficiency gains while delivering better customer service and business outcomes. Some sample agentic use cases include:

- **Healthcare**: Personalized health navigation, benefits eligibility, and virtual triage
- **Housing**: Application processing, permitting, eligibility screening, and subsidy management
- **Banking**: Proactive fraud detection, personalized financial guidance, and automated loan processing
- **Transportation**: Dynamic route optimization, autonomous fleet management, and predictive maintenance
- **Taxation**: Audit flagging, fraud detection, and support for completing tax filings

In the following case study, find out how DNB Finans is using AI and data to streamline the administration of car fleets, detect fraud, and improve satisfaction for their leased car customers.

Case Study

DNB Finans



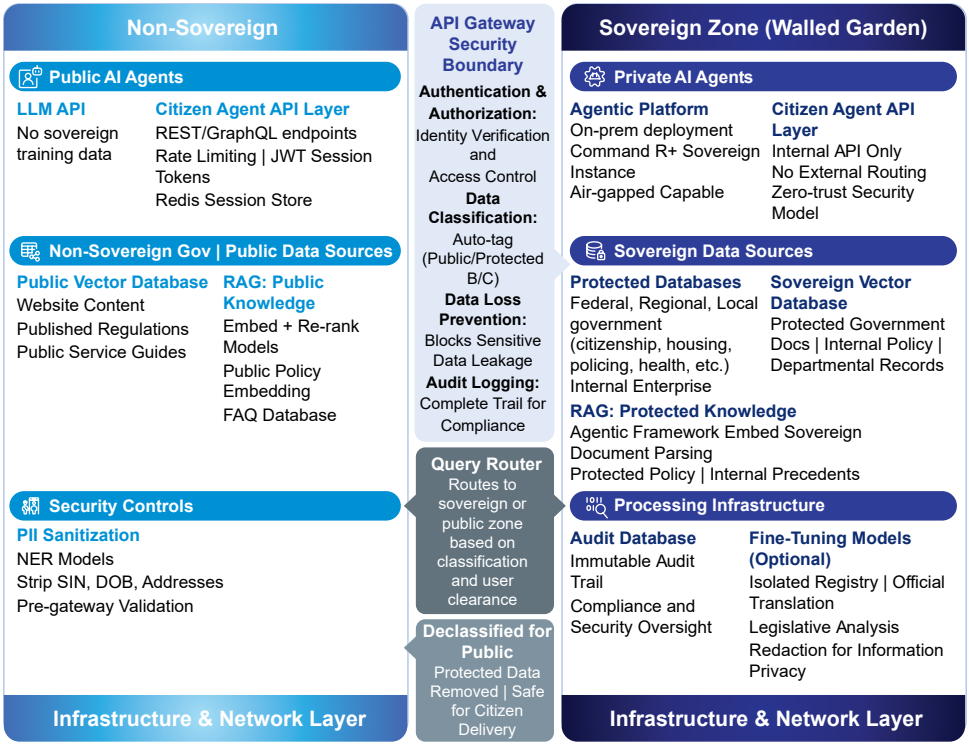
DNB Finans

DNB Bank Group in Norway is Scandinavia's second largest bank, employing 13,430 people and managing total assets worth €250 billion ($273 billion U.S.). Its subsidiary, DNB Finans, is one of the largest finance companies in the Nordic region. In the private sector, the organization has a dominant position in the car financing market with more than 300,000 financed vehicles in its portfolio.

DNB Finans is always looking for new ways to add value for its customers. The most valued services it can offer are those that help businesses control costs by providing greater visibility on their spending. To this end, the Autolease division of DNB Finans wanted to deepen the BI it provided its clients. For example, the system could provide up-to-date statistics to help customers keep track of all car-related costs, including information about fuel use, CO2 emissions, leasing costs, damage reports, and fraud alerts. At the same time, the Company needed to establish customized cost-center structures so that clients would be able to monitor activity by business unit. It was important to DNB Finans that the software would be easy to use without training—the goal was to achieve a user experience that was similar to consumer social networks like Facebook.

The Company rolled out a business intelligence and reporting solution to be used by more than 30,000 leased car customers. The solution is highly intuitive, featuring colorful visual representations of data, including dashboards for users and logical controls for fraud detection and easy administration of car fleets. Since the deployment, DNB Finans has seen customer satisfaction levels rise from 4.4 to 5.1 on a scale of 1 to 6 for "quality of reporting solution".

The system has also drawn an additional 31 percent in user logins, increasing activity on the car financing system. DNB Finans anticipates a return on investment within a short 2.5 years. Its customers now have early visibility into issues like excessive mileage or fuel-related fraud, and are able to pinpoint the business units responsible, enhancing their ability to act and increasing their loyalty through valuable business information. This solution gives the company a significant competitive differentiator in a crowded marketplace.



Detailed Sovereign Data and AI Architecture

Dual Data Architecture

The diagram above presents a detailed architecture for a secure, dual-zone data and AI platform, distinguishing between the environments for the Non-Sovereign or Public Zone, and the Sovereign or Private Zone.

The purpose of this architecture is to ensure that sensitive enterprise and government data and operations are segregated from public or less-sensitive domains, while still enabling controlled interactions where necessary in the public domain. It addresses the need for secure data and AI, while providing flexibility to drive efficiency and cost-effective deployments, enabling improved customer experiences.

Let's break it down.

The Non-Sovereign/Public Zone

In a dual-sovereign data and AI architecture, the Public Zone serves as the controlled interface between open knowledge and enterprise intelligence. It enables organizations to leverage non-sensitive, publicly available data and AI services without compromising internal sovereignty or compliance obligations. By isolating public interactions through secure gateways and sanitization protocols, the Public Zone allows innovation and external connectivity to thrive within clearly defined, governed boundaries.

This zone is comprised of:

Non-Sensitive and Public AI Agents: This feature includes interfaces like large language model (LLM) APIs that do not use sensitive data. The Public Agent API Layer offers endpoints for accessing data, with measures to control usage, secure sessions, and store session data.

Non-Sovereign/Public Data Sources: Here, the system accesses non-sensitive and public databases, published regulations, and service guides. It also uses public knowledge bases to improve the accuracy and relevance of the information it provides.

Security Controls: Security measures include sanitization of Personally Identifiable Information (PII) using Named Entity Recognition (NER) models to strip sensitive information such as date of birth before any gateway validation.

The Sovereign / Private Zone

The Sovereign or Private Zone is the intelligence core of a dual-sovereign data and AI architecture—where sensitive, mission-critical operations take place under full organizational control. Designed for regulated and high-assurance environments, this zone governs the use of private agents, confidential data sources, and secure compute infrastructure. Every process—from model training to inference—is executed within a zero-trust, air-gapped framework, ensuring that national, corporate, or institutional data remains fully sovereign, compliant, and auditable.

This zone is made up of:

Private Agents: This capability is reserved for enterprise public sector or private sector users and agents that are accessing sensitive data. It features an agentic platform capable of air-gapped deployment. The Private Agent API Layer here is internal only, with zero-trust security.

Sovereign Data Sources: This includes protected databases that contain sensitive information, including HR or Finance data, as well as sensitive departmental records. The Retrieval-Augmented Generation (RAG) pipeline in this context uses protected knowledge sources, including legal precedents, to produce accurate AI results.

RAG is essential in enterprise AI because it gives models governed access to relevant knowledge at runtime rather than relying solely on what they were trained on. Early implementations—often called naïve RAG—simply retrieved chunks of text and inserted them into prompts, which could be imprecise and prone to hallucination when context did not fully align. Graph-based RAG (Graph-RAG) represents the next evolution: it structures enterprise knowledge as relationships and entities, enabling the model to retrieve not just documents but the right contextual meaning. As a result, Graph-RAG significantly improves precision, traceability, and trust, reducing the need for oversize prompts and brittle "context stuffing."

Today, enterprises have three primary methods for providing context to AI models: large and well-crafted prompts within expanded context windows, RAG/Graph-RAG retrieval pipelines, and model tuning (including fine-tuning and embedding optimization). The future of enterprise AI lies in orchestrating these intelligently—shifting from manual prompt engineering toward governed, structured, and scalable context pipelines that enable AI systems to reason with enterprise knowledge securely and reliably.

Processing Infrastructure: Provides the accelerated compute capacity for secure workloads. This includes an immutable audit trail database for compliance oversight and optional fine-tuning of LLM models.

Shared Components and Security Measures

Between these zones lies an API Gateway enforcing strict authentication/authorization protocols, including identity verification via access control federation and multi-factor authentication (MFA). Data classification mechanisms auto-tag content by sensitivity level. Data loss prevention tools block sensitive data leakage across boundaries.

A query router directs requests to the appropriate zone based on classification level; only declassified-for-public responses are allowed back into the non-sovereign domain after protected data removal.

The Infrastructure and Network Layer

Both zones leverage robust infrastructure and network layers, ensuring physical and/or logical separation where required.

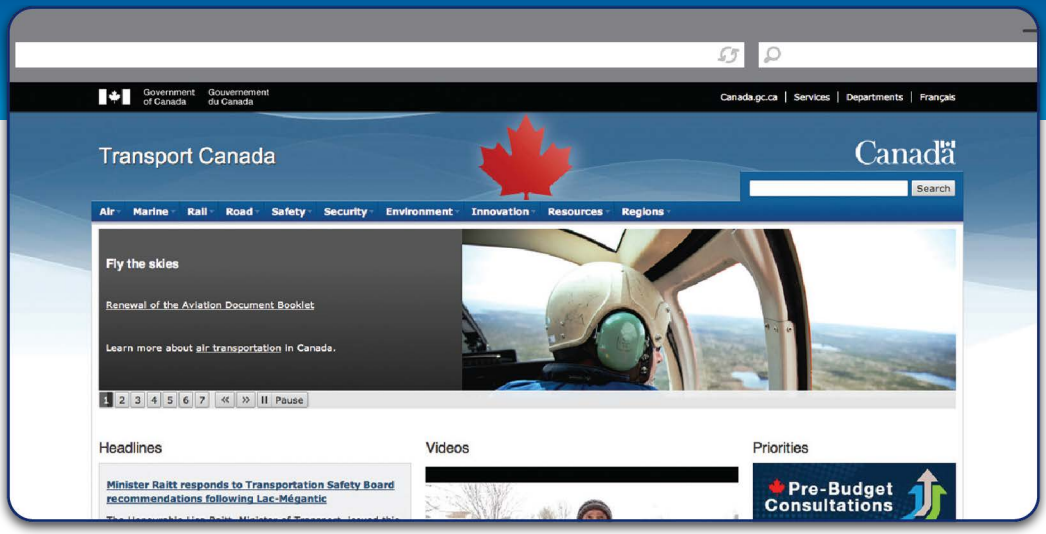
Sovereign Data Is Not a "New" Concept: A History of Private Sector Use Cases

Private sector use cases across regulated and unregulated industries can help to frame and shape this sovereign architecture. Protecting private and sensitive data has been a necessity for decades, and strong information management has been critical to enabling it.

The following feature about Transport Canada demonstrates how effective information management brings secure content to the fingertips of people and integrates critical content with business processes.

Case Study

Transport Canada



Transport Canada

Transport Canada's mission is to serve the public interest through the promotion of a safe, secure, efficient, and environmentally responsible transportation system in Canada. This requires effective information management to facilitate timely and informed decision-making among an extensive list of portfolio partners that include 15 Crown corporations, 17 port authorities, and 21 airport authorities, as well as other shared governance organizations.

Concerned about the dissemination of information through electronic means, privacy assurances, corporate memory loss due to employee turnover, and the need for real-time access to information to satisfy requests and litigation concerns, the Government of Canada (GC) championed an e-government solution based on records, documents, and information management. Transport Canada was the first Canadian government department to complete an e-government deployment, with more than four million records in a single library and 5,200 users to date at more than 117 sites—the largest single library deployment in the Canadian Public Sector.

Working as an integrated set of tools that facilitates the full use of electronic documentation—from capture and storage to organization, retrieval, sharing, reuse, protection, and disposal of information—the solution has become a mission-critical application for Transport Canada's managers and staff. It has helped the organization ensure the accuracy of its corporate records; unite a geographically dispersed and mobile workforce; meet legal obligations, including e-discovery requirements; improve productivity; and align information management with the Government On-Line (GOL) initiative. Using the system, Transport Canada has tripled productivity savings up to $4.6 million and expects further growth, staying on target to meet its annual cost avoidance savings estimate. As a result, the system paid for itself in just 1.17 years.

As cloud adoption has increased over the last several years, most enterprises are operating in a hybrid model of deployment across on-premises, data centers, and public cloud environments. It is only natural as AI adoption increases that these proven deployment models evolve to support a hybrid model for AI.

Bundesrechenzentrum (BRZ) in Austria opted for a hybrid approach, leveraging a cloud-based information management system to consolidate and govern sensitive data across 12 government customers, 40 government applications, more than 10 ERP systems, and mailing systems.

Case Study

Bundesrechenzentrum (BRZ)

Cloud-Based Information Management at BRZ

The Federal Computing Center (BRZ) is the IT service provider of the Austrian public administration. With 1,200 employees and a total annual turnover of 265.3 million euro, the BRZ successfully develops and provides e-government services for ministries, universities, social security providers, and public organizations. The BRZ deploys 320 IT processes, equips 1,200 locations throughout Austria with infrastructure, and services about 30,000 workplaces.

In 2000, the land and commercial registers of the Austrian Ministry of Justice were a typical example of process fragmentation. While the land registry data had been managed digitally since the 1980s, the original documents remained in the physical archives of courthouses and were inaccessible within processes. Moreover, the Ministry of Justice incurred the huge costs of archive maintenance and the risk of losing original documents.

BRZ decided to address the issue by implementing an Enterprise Content Management (ECM) solution. As the pilot study for the Land Registry was implemented, BRZ received more requests from administrations to manage documents electronically and integrate processes. In response, BRZ built a scalable ECM infrastructure called the "eGov Archive Service"—the first-ever Austrian private ECM-cloud service.

The solution provided a robust platform for 12 government customers, 40 government applications, more than 10 ERP systems, and mailing systems. The eGOV Archive Service manages 45 terabytes (TB) of data or 400 million objects, serves approximately 1 million transactions per day, and is accessed by 30,000 users (tax auditors, judges, police, customs officials, HR staff, and accountants) and potentially every Austrian citizen. Services include everything from managing, accessing, routing, and searching to legally compliant archiving of all kinds of documents, as well as tight integration with line-of-business and Enterprise Resource Planning (ERP) systems for a comprehensive cloud solution.

Foundation for Agentic AI

Unlocking the world's private data is the central challenge for the next wave of artificial intelligence. This chapter has provided the architectural blueprint to do so securely. The solution is a hybrid, dual-zone model that establishes a secure Private Zone for sensitive assets and a Public Zone for other workloads. This model creates a secure environment where Private AI Agents can analyze and act on protected enterprise or government data without risk of leakage, while Public AI Agents handle non-sovereign tasks—balancing control with scale and competitiveness. This architecture is the essential foundation for activating advanced AI, providing the trust and control needed for widespread deployment of agentic AI, the subject of our next chapter.

The Fast Five Download

1. **Mandate Sovereign Data Control.**
   Prioritize and enforce full control over national and organizational data and digital infrastructure. Establish policies and technical measures to prevent external influence, ensure data residency, and maintain compliance with domestic regulations.

2. **Implement a Dual-Zone, Hybrid AI Architecture.**
   Separate sensitive data and workloads onto secure, domestically operated infrastructure. Leverage public cloud platforms only for non-sensitive, scalable applications to balance innovation with security.

3. **Deploy Multi-Agent AI Models Strategically.**
   Activate Private AI Agents within protected zones to analyze and act on sensitive data. Use Public AI Agents for non-sovereign tasks, enabling organizations to scale AI innovation without compromising protected assets.

4. **Enforce Rigorous Governance and Security.**
   Apply strict authentication, advanced data classification, and robust data loss prevention tools. Ensure all critical activities are logged with immutable audit trails and operate under zero-trust protocols for maximum oversight and resilience.

5. **Accelerate Adoption of Proven Hybrid Architectures.**
   Adopt best practices from regulated sectors that have successfully managed hybrid environments. Invest in the secure integration of private and public cloud infrastructure to unlock and leverage the 90 percent of private data critical for next-generation AI.

Chapter Eight

Putting Agentic AI to Work

In this chapter, we'll explore how to put AI to work across your enterprise. A successful framework requires understanding the three levels of AI: Generative AI, which creates and synthesizes; Agentic AI, which makes decisions and takes action; and Artificial General Intelligence, which extends reasoning across domains much like the human mind. Together, these layers form the foundation for intelligent, adaptive enterprise AI systems.

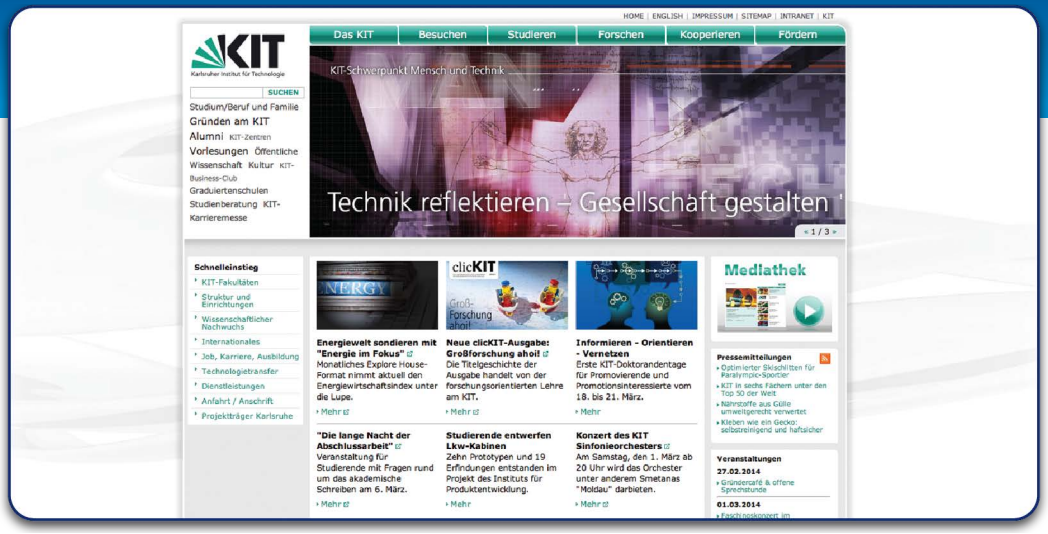
Enterprise AI has moved well beyond the novelty stage. Organizations are no longer experimenting with simple text generators or using AI to draft email subject lines. The focus has shifted—from isolated tools to autonomous collaborators that work alongside people. These are EAI agents: intelligent software entities that not only generate output but act, react, and adapt within dynamic business environments. Unlike traditional AI applications that respond to static prompts, EAI agents function more like digital colleagues—executing multistep workflows, engaging in contextual problem solving, and supporting daily operations with speed, consistency, and intelligence. The difference is subtle but profound: this new class of AI doesn't just answer questions—it gets work done.

EAI agents are moving beyond efficiency tools to become force multipliers for the enterprise. Always available, consistently accurate, and increasingly adept at understanding nuance, they deliver measurable lift without increasing overhead. Whether automating workflows, managing customer interactions, analyzing complex datasets, or guiding users through onboarding, EAI agents bring precision and scale to routine operations. Their reliability ensures uniform experiences, while their speed turns vast data into timely insight. The result is more than cost reduction—it's reclaimed capacity for strategic focus, innovation, and growth.

With integrated EIM and EAI, organizations in the public sector like the Karlsruhe Institute of Technology (KIT) gain leading-edge analytics capabilities, designed to mine, extract, and present the true value of information for improved research and analysis. Read about it in the following case study.

Case Study

Karlsruhe Institute of Technology



The Karlsruhe Institute of Technology (KIT)

The Karlsruhe Institute of Technology (KIT), one of the world's leading engineering research institutions, was founded in 2009 by a merger of Forschungszentrum Karlsruhe and Universität Karlsruhe. As a member of the Helmholtz Association, the largest science organization in Germany, KIT makes major contributions to top national and international research. According to its mission, the Organization operates along three strategic fields of action: research, teaching, and innovation. KIT currently has 9,000 employees and 24,000 students.

KIT needed a leading-edge solution that would give researchers, students, and the general public a faster way to find information across 600 websites and 200,000 associated web pages. On the back end, the institute wanted a robust website management solution that would support their 1,300 editors worldwide, on a day-to-day basis, by supplying metadata, key phrases, and the ability to automatically generate extracts of text. KIT also wanted a collaborative platform that would bring together researchers, scientists, and students.

KIT is using e-government technologies semantic navigation and content analytics in combination with website management to optimize web pages and provide relevant search results. Previously manual tasks that were labor intensive have been replaced by an automated solution that assigns metadata and supports entity extraction by generating teaser texts for new pages, saving users time and reducing error. Visitors are given personalized access to highly relevant information, facilitated by faceted search and related hits—resulting in a more satisfying end-user experience. With improved access to information and the ability to connect with researchers in similar areas of study, the website has evolved into an advanced research network that successfully meets the needs of all stakeholder groups.

Three Levels of AI

Generative AI (GenAI) gained widespread consumer popularity with models such as OpenAI's ChatGPT and Google's Gemini. These, along with other large language models (LLMs) and AI applications, are trained to make predictions or recommendations based on publicly available data sources, including websites, news, Reddit, and Wikipedia, among others. While GenAI models are useful for generating general insights, they are limited to general-purpose tasks. This is because they lack access to the private, real-time, and enterprise-centric data required for specific business use cases.

Agentic AI refers to artificial intelligence systems designed to function as autonomous agents. Unlike models that simply respond to a prompt, an agent can perceive its environment, create a multi-step plan, make independent decisions, and use tools to actively work toward a specific goal.

In an enterprise context, these agents are a powerful engine for productivity with data serving as fuel. They can be given access to private enterprise datasets and internal tools, allowing them to automate complex workflows that previously required human judgment. Agentic AI is powered by a 'digital brain'— a single, competent model that can process decades of human responses.

This technology is already reshaping industries, and enterprises that fail to adopt and orchestrate agentic AI will be left behind. It is also a route to Artificial General Intelligence (AGI).

Artificial General Intelligence (AGI) refers to AI that can understand, learn, and apply knowledge across a wide range of complex tasks, much like humans.[53] Such a technology would be capable of redefining not just sectors, but entire societies.

Like all modern AI, the capabilities of a potential AGI would be fundamentally shaped by the quality and scale of its training data. The foundations of AGI will likely come from the orchestration of thousands of specialized agentic AI instances within a secure and sovereign framework, as described in Chapter 7.

Building Agentic AI for the Enterprise

Good data and effective business processes are foundational to achieving optimal AI outcomes—and the reverse is equally true. With enterprise data safeguarded and large language models (LLMs) fine-tuned within your domain, the stage is set to build what we call "agentic capabilities" that deliver real business value.

Agentic AI is not just about technology; it's about building capabilities on top of your business processes and supporting a combination of people, processes, culture, and change management. When done right, it becomes much more than an experiment in generative output. Rather than merely asking a model to "summarize a document," agentic AI might detect a bottleneck in a workflow, break tasks into subtasks, call APIs or other systems to execute, monitor results, learn from them—and then refine the next step with minimal human direction.

Consider the findings of Massachusetts Institute of Technology's NANDA initiative ("The GenAI Divide: State of AI in Business 2025"): only about 5 % of enterprise generative-AI pilot projects achieved rapid revenue growth; the other 95 % failed to deliver measurable P&L impact. According to the researchers, the barrier was not the model or the hardware—it was the "learning gap" or the inability of AI systems and organizational workflows to adapt together.[54]

Among the lessons derived: allocate AI investments where they align to specific processes, not just high-visibility use cases; embed feedback loops so the system learns; integrate deeply into existing operations rather than bolt on a generic tool; and ensure change-management is in place so people and culture welcome the shift. In short: when data quality, process alignment, organizational readiness, and domain-specific modeling converge, you position your enterprise to move from pilot to real EAI-driven value creation.

The Case for Agentic AI

Organizations are increasingly adopting AI in response to pressures from rapid economic and technological change—including the need for digital transformation, new business models, real-time decision-making, global scale, and the ability to adapt to disruption.[55] AI agents, which can perform tasks semi- or fully autonomously, help them remain competitive, scale information flows, reduce cognitive load on humans, and improve agility.

Deploying systems of AI agents is only the start. The bigger challenge is sustaining them and ensuring they continue to deliver value, remain aligned with organizational goals, and evolve in step with the human-machine ecosystem.[56] Starting with well-known business processes is critical, and this will be covered in more detail in the following chapter. It is best to adopt a standards-based approach and begin by identifying discrete, simple tasks for your first agents. This method will establish the foundation for a more complex, orchestrated model in the future.

The following feature about a European Court of Human Rights demonstrates how EIM helps consolidate information to ensure accuracy and integration of AI with key processes—reducing administrative burden and improving performance. As a result, agencies are better equipped to deliver on their mission to protect citizens.

Case Study

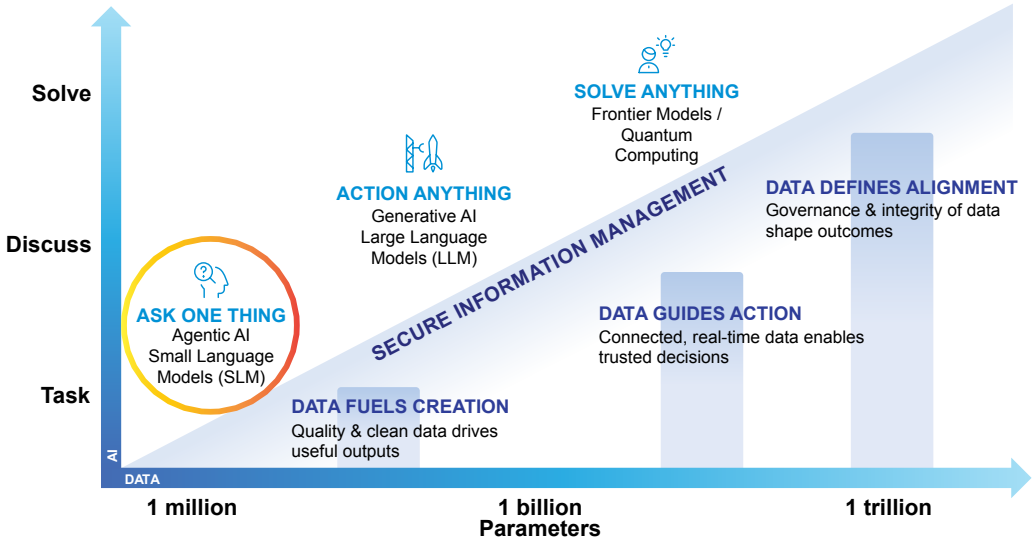
A European Court

The Court is part of the Council of Europe, an international intergovernmental organization that was established in 1949 to promote political democracy and human rights, social progress, and cultural identity continentwide.

Over the past decade, the Court has seen its caseload skyrocket—from 14,000 applications to more than 50,000. To manage this surge, the Court's IT department built an automated workflow solution that streamlined how committee and chamber cases moved through approval. What began as a digital transformation initiative has since evolved into an intelligent information ecosystem, powered by analytics, EIM, and now, Agentic AI.

Today, the Court's workflows do more than just route documents—they reason, adapt, and act. Built on a foundation of governed data, the system uses analytics to identify process bottlenecks and agentic AI to optimize them in real time. For example, the platform can detect when a case file lingers too long in review, automatically flag it for escalation, and redistribute workload across divisions to maintain throughput. Legal assistants no longer spend hours chasing paper trails; the AI monitors progress, generates dynamic reports, and recommends next steps—continuously learning from outcomes to improve future routing decisions.

The results speak for themselves: faster case turnaround times, fewer administrative bottlenecks, and more time for the Court's legal experts to focus on interpretation rather than administration. With analytics, EIM, and agentic AI working in concert, the Court has transformed from a reactive institution to a proactive one—ready to scale, adapt, and deliver justice at the speed modern caseloads demand.



This Information Trains All Forms of AI

Strong Data Foundations

The critical challenge is how to leverage secure, high-quality data to drive AI outcomes and achieve its full potential. As the above diagram illustrates, there is a direct link between strong data foundations and successful AI outcomes.

Beyond data, a successful strategy must also account for infrastructure. Different AI models have varying requirements, and the data and AI architecture must be designed to match the right model to the right business task.

Unlocking Private Data to Support Agentic AI

Given the quality and quantity of enterprise data sitting behind the firewall, it is crucial to leverage this private data. Fine-tuning or adapting an LLM with this domain-specific knowledge is what enables agentic AI to handle meaningful, real-world business use cases and applications.

Data pipelines, data lineage, and data flows will become critical. Every enterprise will need to become a data warehouse company. As we examine the breadth of data across the enterprise, it is clear that unlocking AI requires a strategy to work across both public and private datasets, which are each integral to how every private and public sector organization operates today. The following diagram illustrates examples of these datasets.

Examples of Datasets

Leveraging Private Data to Fine-Tune LLMs

Large Language Models rely on significant amounts of data to train. They learn from patterns in this data—including words, phrases, syntax, and semantic relationships.[57]

While the quality and scale of this initial training data are important, relevance is critical for enterprise use. As previously discussed, publicly trained LLMs (like those from OpenAI, Cohere, or Anthropic) are excellent for general-purpose tasks but lack deep context when it comes to specific businesses. To address this limitation, enterprises now employ multiple adaptation strategies to align models with their proprietary data and environments. The most established of these is fine-tuning, while techniques such as context engineering offer complementary flexibility and speed.

Fine-tuning a base model involves taking the publicly pre-trained model and continuing its training on a smaller, domain-specific, or proprietary set of data. This allows the model to learn the enterprise's unique vocabulary, data, and processes without exposing that private data to the public. This fine-tuning delivers a customized derivative model that performs better on enterprise and domain-specific tasks, as it has internalized patterns from private data.[58]

In parallel, context engineering enables enterprises to refine model behavior dynamically by structuring and updating the input context (e.g., prompts, examples, or metadata) rather than retraining the model. This approach allows faster, lower-cost adaptation, supports selective unlearning for privacy or legal compliance, and is particularly useful when working with closed-source models.[59]

In practice, organizations often combine both approaches: fine-tuning for deep domain alignment and long-term performance, and context engineering for agile, real-time adaptation. Together, they create a layered, sustainable strategy for aligning LLMs with enterprise goals and compliance standards.[60]

In the following feature, a travel tech leader in dynamic holiday packages is giving holidaymakers access to millions of real-time combinations. It uses technology to simplify, personalize, and enhance customers' travel experiences.

Case Study

A Travel Tech Company

With operations across multiple European markets expanding and demand for real-time holiday packages increasing, a travel technology company experienced a sustained surge in data volume and variety. Bookings, web interactions, partner feeds, marketing activities, and customer support engagements all generated high-velocity data with different structures and latency requirements. This growth threatened pursuit of governance, access pattern, and time-to-insight initiatives.

Over time, the data estate split into two silos: a data warehouse with ETL (Extract, Transform, Load) and reporting tools, and a data lake for raw ingestion. The separation created duplication, maintenance overhead, and slower analytics. Teams relied on different tools and custom "glue" code to bridge systems—introducing a "stark divide" that made growth harder and insights slower to deliver.

The company adopted a unified data access layer, eliminating separate ingestion pipelines and the need for complex glue code. With a common interface and shared toolset, engineers and analysts could query and process data consistently across systems. By merging environments and decoupling producers from consumers—while preserving full compatibility—the organization achieved a single source of truth. This integration enabled richer analytics, correlating BI data with marketing, CRM, and machine learning insights to power advanced, predictive customer models.

The company next moved to a containerized cluster environment using Kubernetes to automate deployment, scaling, and workload management. Query jobs can now spin up on demand and shut down when complete, using shared storage and right-sized compute for each task—from ETL to analytics dashboards. The result: greater scalability and efficiency, with lower compute costs, energy use, and carbon footprint.

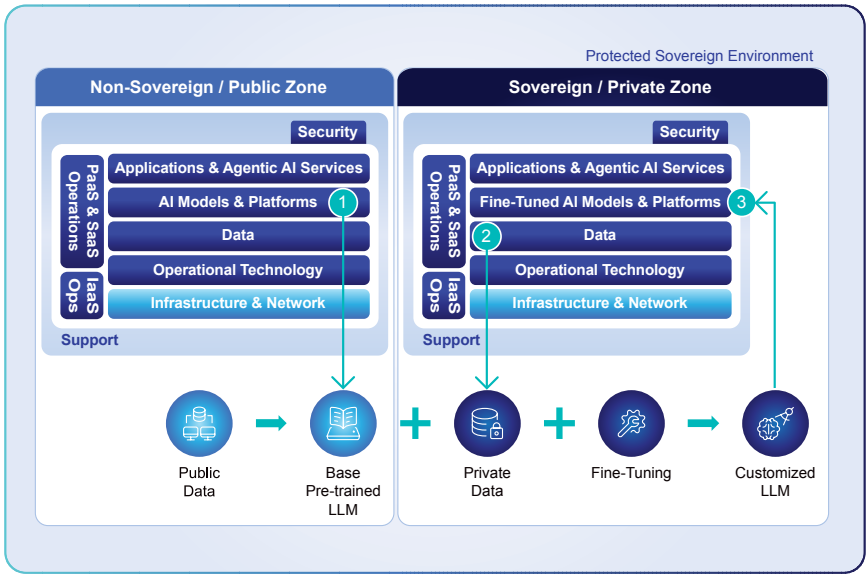
The company is able to study customer behavior across all of its channels and analyze every step of the customer journey—from preliminary searches to final payment. The implementation is positively impacting marketing campaign Return On Investment (ROI) and company revenue. In addition, AI driven algorithms for attribution and bidding automation help optimize marketing costs overall, leading to increased profits.

But Can I Guarantee the Sovereignty of My Private Data and Fine-Tuned Model?

This gets to the heart of the challenge. Your data—and the AI built on it—is your competitive advantage. The quality of your data defines the efficacy and integrity of your LLM. However, once you have trained an LLM on a specific dataset, it cannot unlearn that data.

This is a key reason why private data and private AI are essential. When you train a model, it internalizes the data patterns, making an indelible mark. These learnings become interconnected with other data, as part of both the specific examples and the broader underlying data distribution. Because of this, attempting to unlearn specific training data requires a massive amount of cleanup of the parameters and connections that drive the model's behavior. In "Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy, Research, and Practice," the authors highlight, "Deleting information from an ML [machine learning] model is not well-defined. First, information cannot be deleted from an ML model in the same way that it can from a database."[61]

While work is ongoing to refine approaches to "machine unlearning," it is not a simple path for a private or public sector enterprise. The need to protect sovereign or private data and the resulting model is paramount.



Sovereign Data and AI Architecture

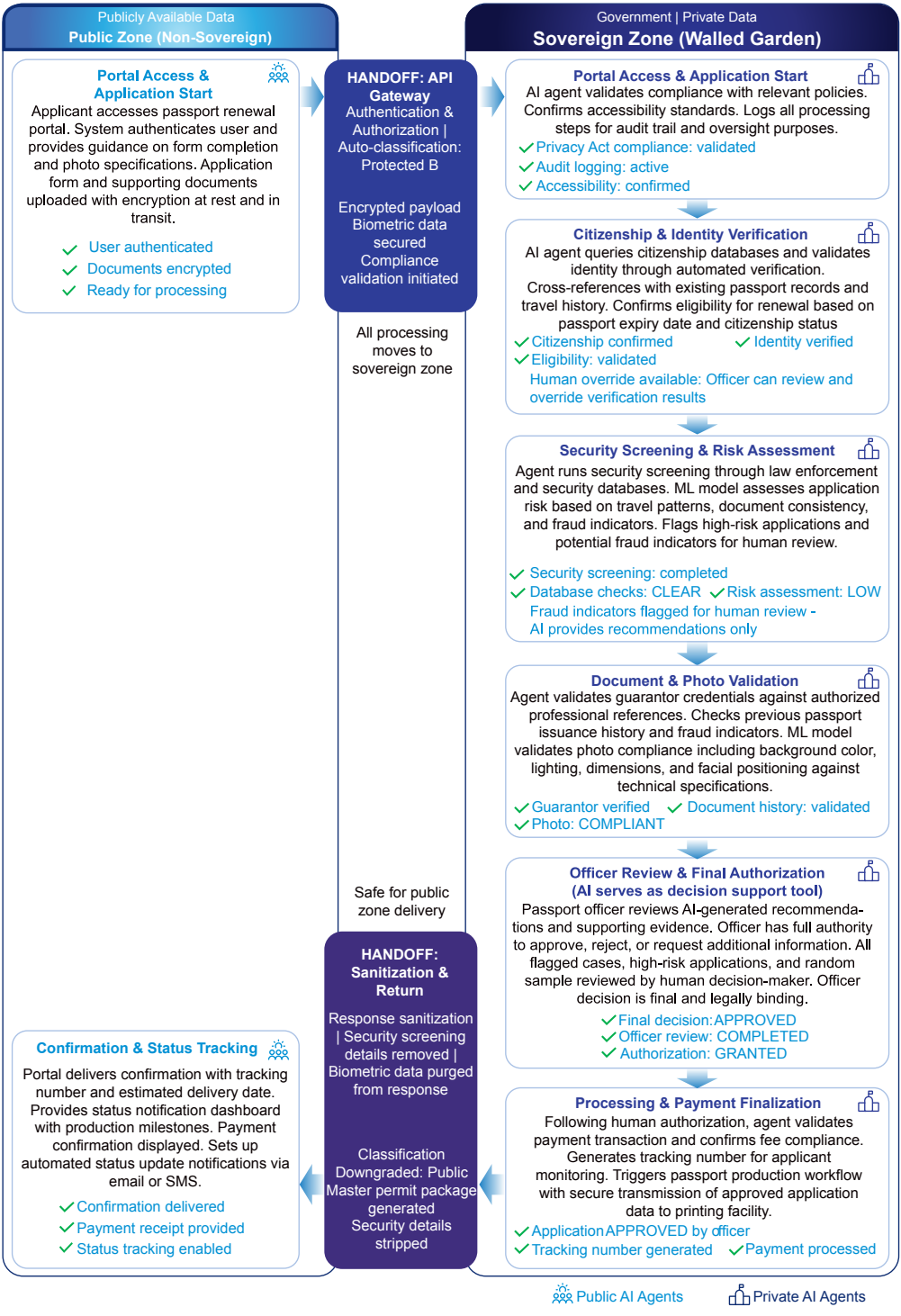
This is precisely why a Sovereign Data and AI architecture is so critical. Instead of relying on unlearning, this approach is built on prevention. It is designed to keep your data and the fine-tuned model private from the start. This requires ensuring the model is deployed in a certified sovereign zone where your fine-tuned models are protected, as depicted in the architecture above.

In the above figure, public data is leveraged to deliver a base pre-trained LLM (1) that operates in the non-sovereign/public zone. A complete set of agentic AI capabilities can be delivered in this environment. On the private zone side, the base model is fine-tuned with private data (2), which in turn provides a customized LLM that includes domain or industry specifics that may be a differentiator for your business. This LLM (3) can be leveraged by agentic AI operating in the private zone, and the data is not supplied back to the LLM operating in the public zone.

Notably, if you control the infrastructure on which the model is deployed, you can keep it private. If the model is hosted in the public cloud, you require assurances from both the public cloud provider and the model provider (if they are different) as to the sovereignty of your data.

Agentic AI in the Sovereign Context: A Use Case

If we place agentic AI within the sovereign context, we can use an example that's familiar to citizens of many nations: applying for a new passport. This example highlights the need for both private and public datasets, and demonstrates how agentic AI can navigate both environments, with fine-tuned models operating in the sovereign/private world working alongside models deployed in the non-sovereign/public zone. When these environments work together, the end customer is the ultimate beneficiary, enjoying a greatly enhanced experience.



Passport Processing Use Case Featuring Sovereign Zones and Non-Sovereign Zones

Step 1: Portal Access and Application Start (Public Zone)
The applicant begins by accessing a passport renewal portal. The system authenticates the user and provides guidance on completing and submitting the application. Passport information and supporting documents are uploaded with encryption both at rest and in transit. At this stage, the statuses include user authentication, document encryption, and readiness for processing.

Step 2: Handoff—API Gateway
The API Gateway handles authentication and authorization, auto classifying the data as protected. The payload is encrypted, biometric data is secured, and compliance validation is initiated.

Step 3: Compliance and Policy Validation (Sovereign Zone)
The Government AI Agent validates compliance with the relevant privacy and information regulations and policies.

The system confirms language service capability and accessibility standards, logging all processing steps for audit trail and compliance purposes. The statuses at this point include compliance validation, active audit logging, and confirmed accessibility.

Step 4: Citizenship and Identity Verification (Sovereign Zone)
The Government AI Agent queries the citizenship database to match the identity from the submitted passport application. It cross-references existing passport records to confirm eligibility based on nationality and other criteria. The statuses include confirmed citizenship, available match override if needed, and validated eligibility.

Step 5: Security Screening and Risk Assessment (Sovereign Zone)
The Government AI Agent conducts security screenings through law enforcement databases, utilizing travel patterns and risk factors. Machine learning models assess application risk based on travel patterns and cross-check watchlists, then alert for manual review if necessary. The statuses include completed security screening and a risk assessment categorized as low, medium, or high.

Step 6: Document and Photo Validation (Sovereign Zone)
The Government AI Agent validates guarantor credentials through a database lookup, checks previous passport history for issues or travel fraud indicators, and utilizes machine learning models to authenticate the photo against government ID records and databases. The statuses include validated guarantor credentials and verified document integrity.

Step 7: Officer Review and Final Authorization (Sovereign Zone)
An expert human agent reviews all information flagged by the system, using AI as a decision support tool. The human agent grants final authorization based on the comprehensive review of all validated information. This workflow ensures that sensitive personal data is securely handled, validated, and processed in compliance with privacy regulations, maintaining a clear separation between public and sovereign zones.

While specific use cases may vary, and this is a simplified example, it highlights how the engagement of agentic AI interacts across sovereign and non-sovereign zones while handling personally identifiable information as part of a hybrid deployment. Implementing and managing the deployment of agentic AI requires a broader consideration of how digital agents and human workforces work in concert. Agentic AI performs tasks using its built-in logic, while human oversight ensures successful outcomes.

The next chapter will dig more deeply into how digital and human workforces must work in concert to realize AI's potential in the enterprise.

Read the following feature to find out how the General Council of the Judiciary uses a trusted EIM system to securely consolidate both public and private information—to improve the delivery of its services to Spanish citizens.

Case Study

General Council of the Judiciary

PoderJudicial.es

> *Analytics help us measure the success of our services and the public site's overall performance, equipping us with the tools we need to present users with a relevant and responsive experience, supported by multimedia content.*

The General Council of the Judiciary (Consejo General del Poder Judicial or CGPJ) was established by the Spanish Constitution in 1978 as the constitutional body that governs the Judiciary of Spain. The CGPJ wanted to combine its systems into an online portal to provide citizens with personalized access to the information and services they need.

The new portal would support a variety of communication channels in multiple languages. On the back end, the system would be required to integrate all corporate services of the Judiciary Council to streamline collaboration, provide integrated services such as online applications, allow for the secure management of information, and comply with current regulations around transparency, accessibility, multilingualism, Law 11/2007, and more.

An e-government solution was selected as the basis for the CGPJ website and judiciary extranet, providing the Council with a technologically sound and manageable platform for the future. The multilingual portal supports a substantial number of hits and is readily scalable. The web publishing process is more efficient; self-service capabilities have significantly reduced the time it takes to publish up-to-date information.

The system went live internally with 6,500 active users and 5,400 messages exchanged on its forums. Members of the Judiciary can participate and collaborate using the system's virtual environments, 45 communities of practices, and shared files. Secure access to integrated applications and services is provided through single sign-on and identity management. The system is customizable, allowing users to personalize and configure their working environment.

The Fast Five Download

1. **Deploy Agentic AI to Drive Enterprise Value.**
   Accelerate productivity and adaptability by adopting agentic AI applications that autonomously perceive, plan, decide, and act—enabling automation of complex workflows and reducing dependency on manual intervention.

2. **Leverage Private, Domain-Specific Data to Differentiate.**
   Achieve business advantage by fine-tuning AI models with your organization's proprietary internal data, empowering agentic AI to solve domain-specific challenges that generic models cannot and building a secure, high-quality data foundation.

3. **Implement Sovereign AI Architectures to Protect IP and Privacy.**
   Safeguard your enterprise's sensitive data and intellectual property by deploying AI models within secure, sovereign environments—ensuring compliance, data privacy, and full control over your AI assets.

4. **Focus AI Initiatives on Targeted, Learning-Capable Systems.**
   Maximize ROI by directing agentic AI toward specific, well-understood business processes, and invest in systems that learn and adapt over time—avoiding generic solutions and minimizing disruptive organizational changes.

5. **Champion Human-AI Collaboration for Sustained Impact.**
   Ensure ongoing value by establishing standards for human oversight and alignment, starting with simple agentic tasks, and cultivating effective human-machine collaboration that evolves with your business needs.

Chapter Nine

The Management of EAI Applications

In today's enterprise, the management of AI applications is no longer about deploying a single model—it's about orchestrating a symphony of intelligent agents operating across public and sovereign zones, private clouds and open networks, and multitudes of workflows. This is Enterprise Artificial Intelligence and managing this complexity demands more than technical prowess; it requires a sophisticated organizational approach rooted in solid business processes, change management, and governance. As noted by recent research, companies falter in their application of AI not because the models are inadequate but because their structures, owners, and workflows aren't ready for it.

In this chapter, we lay out the key principles that ensure your organization can not only deploy agentic AI—systems that reason, plan, act, and collaborate—but also manage them in a way that aligns with strategic goals, risk frameworks, and human-centred governance.

These four principles define the right conditions for the successful deployment of enterprise agentic AI systems:

1. **Organizational Model for Agentic EAI Deployments**: Ensuring that ownership and accountability, along with roles and responsibilities, are clear.
2. **Developing Agentic EAI Applications**: Adopting a structured approach to prioritizing and building out capabilities for the organization.
3. **Collaboration between Human and Agentic EAI Workforces**: Ensuring that your teams embrace and adopt AI with clarity of role and purpose.
4. **Performance Management and Measurement**: Closing the feedback loop by measuring outcomes and performance-managing your agentic AI workforce.

As we dive into each of these principles, you'll find frameworks, best practices and real-world considerations to build and operate enterprise AI at scale. From defining the model of the organization, to designing workflows that humans and agents share, to measuring value and adapting continuously—this chapter equips you to move from isolated AI experiments to enterprise-grade deployments. Let's begin by exploring how the organizational model sets the foundation for accountable and scalable AI applications.

1. An Organizational Model for Agentic AI Deployments

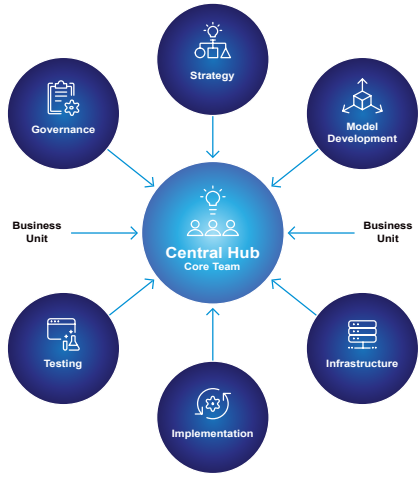
How to Select the Right Model

Enterprises seeking to drive AI adoption, and more specifically, deliver agentic AI capabilities, must make a critical decision about how to manage their AI applications. Several common models exist, each with distinct positive and negative attributes, but the most crucial aspect is selecting the right one.

The following examples outline four models that work in various organizations depending on the industry and level of regulation: Centralized Model (AI Center of Excellence/CoE), Hub-and-Spoke Model, Federated Model, and Hybrid Model.

The Centralized Model

In this model, a centralized team holds deep competency and is responsible for driving strategy, model development, infrastructure, implementation, testing, and governance. This ensures consistency and control, along with unified governance; however, it can absolve business units of accountability and ownership for driving outcomes from their AI adoption. Many organizations new to adopting technology, as well as those in regulated industries and government, find this model attractive.

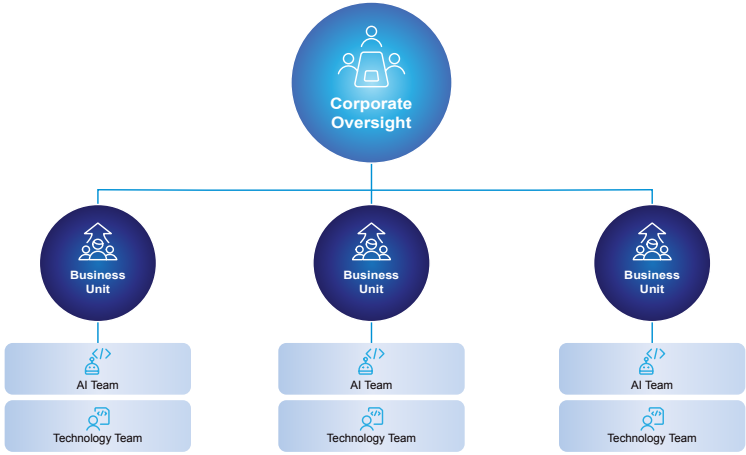


The Centralized Model

The Hub-And-Spoke Model

In this model, a small group at the center sets the strategy and provides tools and frameworks, while the different business units act as spokes to execute projects within their domain. This model is inherently more agile and attractive to organizations that have technology competency in other business units. It is also more agile and scalable for the organization to drive multiple projects in parallel. One point of contention with this model is the question of who owns, trains, and fine-tunes the LLM. Generally, this is owned by the hub, and the business units are responsible for the agentic AI applications.

The Hub-And-Spoke Model



The Federated Model

The Federated Model

In this model, there is no centralized function, and each business unit has a group responsible for operating its own AI systems and technology. In some cases, a small team may provide corporate oversight. Generally, this model offers complete control for the business units, allowing them to drive faster implementation; however, this comes at the expense of governance and security risks. This model would be most useful for extremely mature organizations.

Hybrid Model

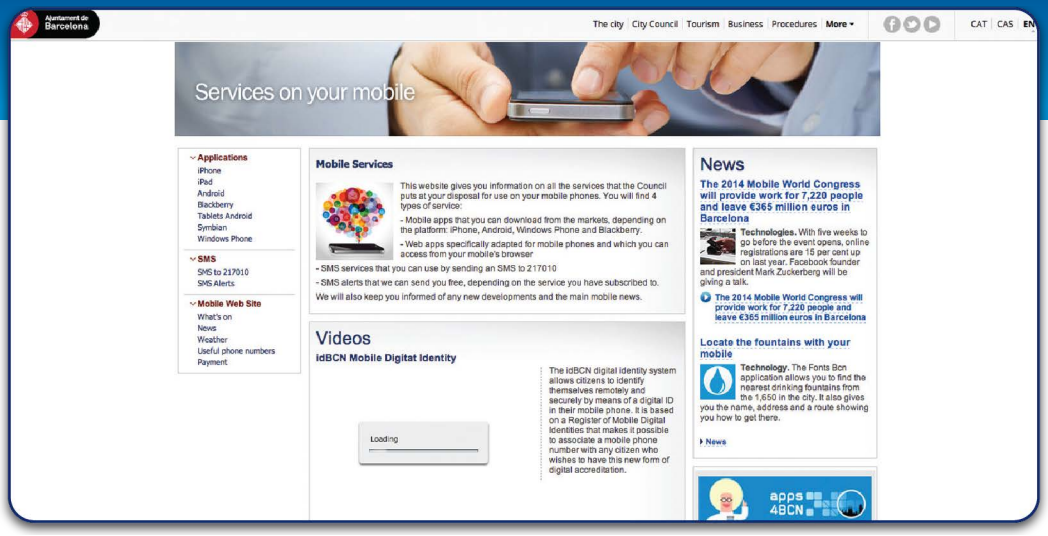
Hybrid models blend components from the other approaches. The key advantage lies in being able to leverage economies of scale by having standard services that teams can utilize, coupled with giving autonomy to business units to deliver.

Ultimately, selecting the right model depends on the organization's specific needs. Success requires understanding how you want your teams to work and what guardrails you wish to put in place for your users. This clarity is critical to building scalable, outcome-focused agentic AI applications.

In the following case study, the City of Barcelona has implemented a Hub-and-Spoke model to make data and services available to all citizens from any device and any location, improving access to services and the overall quality of life for its citizens.

Case Study

City of Barcelona



The City of Barcelona—Citizen Services Are "One Tap Away"

The City of Barcelona is the second largest city in Spain, with over a million and a half inhabitants. Fulfilling its vision of transformation into a smart city, the municipal government is relying on mobile and cloud-based e-government solutions to facilitate citizen engagement with administrative processes and city services.

The goals of implementing an e-government system have been clear: to make data and services available to all citizens from any device and any location as a means to improve the quality of life for all citizens. A first step toward achieving this was making City Council and other data available in digital format, while promoting the reuse of this information to stimulate economic growth through opportunities for innovation.

To standardize its information, the City needed to consolidate its infrastructure based on interoperable and open standards and decommission its legacy systems. The City opted to migrate its solutions to the cloud. A content management system hosted in the cloud provides an alternative that is reliable, flexible, and produces economic gains in the long run. The result was the first Barcelona Open Data site with 510 datasets. The solution, based on the principles of mobility, smart cities and administration, information systems and innovation, supports 150 portals with over 4 million user visits and more than 65 million pages generated each month.

Is Your Organization Ready?

The AI hype sparked a race to adopt, driven by a fear of being left behind. But the truly innovative organizations didn't slam the accelerator—they tapped the brakes. They understood that while data may be the fuel for the AI engine, flooring it without direction doesn't get you farther; it only risks burning out before you reach your destination.

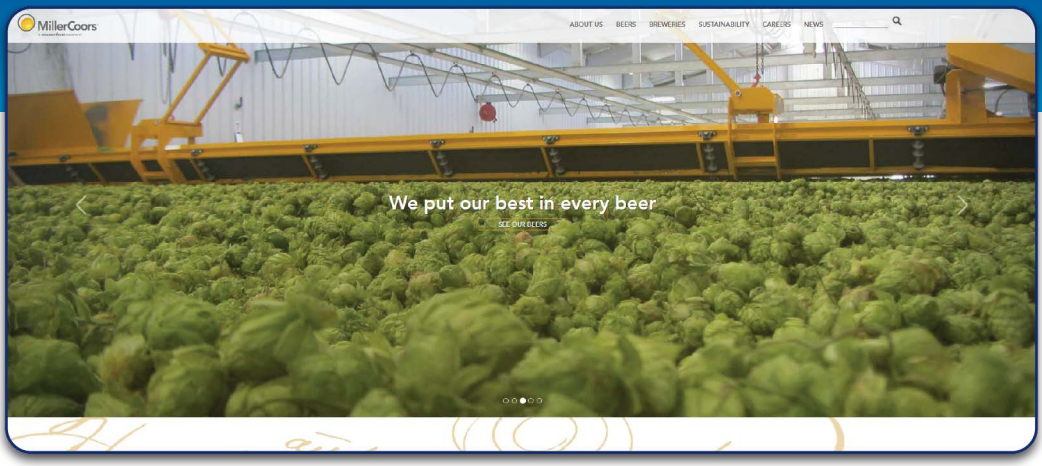
The organizations that took time to learn, plan, and prepare have achieved far greater success. By ensuring their data was ready and governance was in place, they knew how they would use AI before accelerating—a critical step those who sped off from the starting line missed.

Even Microsoft eased off the accelerator when they rolled out Copilot across their organization. As one of the first organizations to deploy at scale, they divided their implementation into distinct phases—from a limited early access rollout for specific groups, to more focused groups, to ultimately a full rollout by cohort. They shared: "We divided our adoption along two vectors: internal organizations like legal or sales and marketing, and regions like North America or Europe. Different cohorts have different focuses, but the strategy is similar."[62] This cohort-specific approach has been cited by other organizations as the key to their AI deployment success as they sought to enable specific groups and users with technology specific to their needs, thereby driving adoption.

MillerCoors acts as the focal point or Hub-and-Spoke of its supply chain by overseeing its suppliers directly in the following case study.

Case Study

MillerCoors



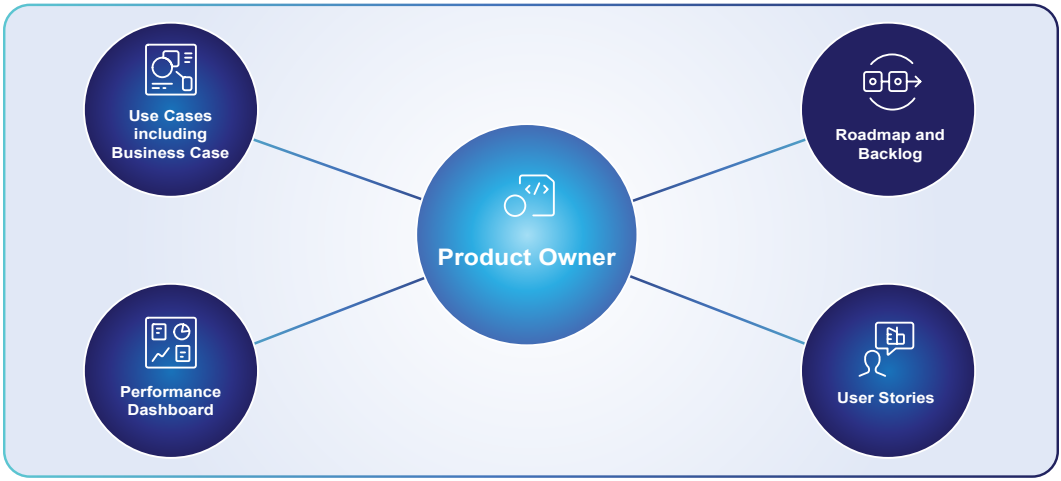
MillerCoors

MillerCoors is a joint venture of the U.S. operations of SABMiller and Molson Coors. With more than 450 years of combined brewing heritage, MillerCoors boasts an impressive portfolio of industry-leading beers. With nearly 30 percent of U.S. beer sales, MillerCoors is the second-largest beer company in the United States. The company operates eight major breweries, as well as several craft breweries.

Miller Brewing (a legacy company of MillerCoors) found its distributor-to-retail supply chain was falling short of the industry standard and, more importantly, user expectations. The company needed to modernize and standardize their inefficient and document intensive processes to remain competitive in their complex and consumer-driven market.

Using B2B Managed Services, Miller Brewing connected more than 400 distributors with 25 different business systems into a cohesive EDI (Electronic Data Interchange) platform. Doing so enabled their entire distributor network to conduct business with any retailer that required an EDI capability.

B2B Managed Services provides the technical foundation for a seamless, end-to-end EDI platform for all of MillerCoors' supplier and banking connections. Critical documents are received, processed, and seamlessly exchanged to deliver efficiencies, cost savings and, of course, beer. In just one year, the business transformation eliminated 1.2 million hours of labor for distributors and 1.3 million hours for retailers, for a total of 2.5 million labor hours removed from the distributor-to-retailer supply chain. The time savings translates to an estimated re-allocation of 1,200 full-time equivalent (FTE) resources to other tasks, freeing up potentially $50 million in labor savings.



Broad Scope of the Product Owner

2. Developing Agentic EAI Applications

Start Small, Keep it Simple

Beyond a cohort-specific deployment approach, a core principle for successful AI implementation is to start small and keep it simple. Underlying this is a ruthless focus on driving business outcomes. Technology for technology's sake is a nice concept, and can certainly be fun for technology teams, but it is not a winning strategy with AI.

Starting small means picking a use case and working with a part of your business that understands the technology and its potential, and has good, documented business processes, good data quality, and can drive adoption. The cultural impact of having change agents and champions that can drive adoption should not be underestimated. In our case, this was selecting our Human Resources team. With a strong technology orientation across that team, they were keen to embrace the transformation and their role as both business and product owner.*

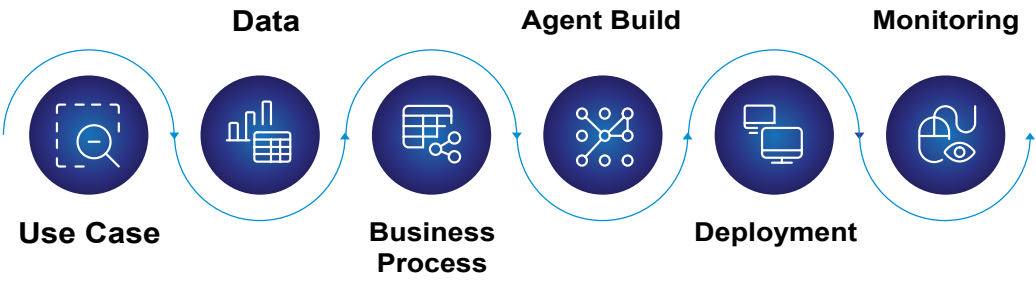
Product Owners play a vital role in designing and implementing specific AI use cases. Ensuring they can act as change agents and champions for agentic AI adoption is as critical as ensuring they have the right skills for the role. The broader scope of the Product Owner role is shown above.

* For reference, the Scaled Agile Framework defines product owner as "the voice of the customer and the business, managing and prioritizing the Team Backlog, aligning the team's work with strategy and stakeholder needs, and helping maintain both business and technical integrity of the solution."[63]

The Importance of Good Processes and Data to Drive Agentic AI Applications

With a team and target use case defined, a deep understanding of the data and business process becomes the key to guiding the agent's development and behavior. The process is outlined below.

Lifecycle Management Approach for Agentic AI



The Lifecycle of Agentic AI

Building on the **use case**, the process begins with an analysis of **the data** and **business processes**. This analysis directly informs the development of the agentic AI application.

This development phase, often driven by the Product Owner, is typically a collaboration between IT and the specific business unit. To lower the barrier to entry, many agentic frameworks now use low-code/no-code approaches, allowing non-developers to contribute.

Following the **agent build**, the application moves to **deployment**. This step requires a standardized approach to ensure the proper governance and guardrails are in place for the organization. Finally, the process is completed with ongoing **monitoring** to manage performance.

An agent's success often hinges on a unified understanding of its role, the data and processes it uses, and its inputs and outputs. Beyond that, carefully documenting its expected behaviors is critical to success. The best way to achieve this is to start small. This means beginning with simple, discrete-function agents and avoiding complex scenarios with numerous edge cases. As these simple agents start delivering value, more complicated scenarios can be tackled through either a series of orchestration flows or more complex agents.

3. Collaboration between Human and Agentic AI Workforces

Treating Digital Agents as an Extension of Your Workforce

Should digital agents be managed by Human Resources, just like human employees? This question is certainly a topic of debate as agentic AI applications become more mainstream. In their report about the agentic organization, McKinsey & Company examined how companies leverage human employees and digital agents to drive outcomes and results:

> "As agents take on execution, people will increasingly define goals, make trade-offs, and steer outcomes. This will change how companies plan for a hybrid workforce, whom they hire (or borrow), how they deploy human or AI talent, and how they measure success. HR systems not only track human employees but also are a repository of agents and agentic workflow."[64]

One effective approach that some organizations are undertaking is building job descriptions for their agents (see below). We've adopted this practice internally, with our teams creating job descriptions during the initial development process that are similar to those we publish for human roles. This ensures that as we move into the deployment and measurement phase, we know the expectations. Culturally, this has also helped our team better understand their own roles in relation to these new digital agents.

Human Job Description: HR Operations Specialist

Role Summary
The HR Operations Specialist is responsible for managing and resolving employee HR tickets, with a focus on benefits selection, onboarding, and policy guidance. This role works in tandem with an Agentic AI assistant to ensure timely, accurate, and personalized support.

Key Responsibilities

- Review and validate employee-submitted benefit selection requests.
- Provide personalized guidance based on employee eligibility, location, and role.
- Escalate complex or exception-based cases to HR leadership.
- Collaborate with the AI agent to monitor ticket queues and prioritize urgent cases.
- Audit benefit selections for compliance with internal policies and regulatory requirements.
- Train and calibrate the AI agent by reviewing its recommendations and feedback loops.

Skills & Qualifications

- 3+ years in HR operations or benefits administration.
- Strong understanding of enterprise HRIS systems and benefits platforms.
- Excellent communication and decision-making skills.
- Comfortable working alongside AI agents and digital workflows.

Collaboration with AI Agent

- Oversee and approve benefit recommendations generated by the agent.
- Provide context and nuance for edge cases the agent flags as ambiguous.
- Participate in continuous improvement of agentic workflows and training data.

Agentic AI Agent Job Description: HR Ticket Resolution Agent

Role Summary
The HR Operations Specialist is responsible for managing and resolving employee HR tickets, with a focus on benefits selection, onboarding, and policy guidance. This role works in tandem with an Agentic AI assistant to ensure timely, accurate, and personalized support.

Key Responsibilities

- Automatically classify and route incoming HR tickets using natural language understanding.
- Retrieve and analyze employee data (e.g., tenure, location, job level) to recommend appropriate benefits packages.
- Generate personalized benefits summaries and FAQs for employees.
- Flag tickets requiring human judgment or policy exceptions.
- Learn from human feedback and update decision models accordingly.
- Maintain audit logs and traceability for all actions taken.

Capabilities

- Integrate with enterprise HRIS, payroll, and benefits systems using secure, auditable and approved APIs.
- Use policy documents and historical ticket data to inform decisions.
- Operate 24/7 with real-time response capabilities.
- Continuously improve via feedback-driven calibration and model tuning.

Collaboration with Human

- Send benefit recommendations to the HR Operations Specialist for approval.
- Receive feedback on rejected or modified recommendations to refine future outputs.
- Alert the human to anomalies, missing data, or policy conflicts.

Governance & Oversight

- All actions are logged, and subject to review by automated Audit Agents and HR specialist teams.
- The system operates with autonomy but under continuous monitoring and auditability and undergoes periodic audits to validate compliance and model performance.

Step	Agentic AI Assistant	Human Specialist
1. Ticket Received	Classifies the ticket as "Benefits Selection" and extracts relevant employee data.	Monitors queue and reviews flagged tickets.
2. Recommendation	Suggests a benefits package based on policy rules and employee profile.	Reviews recommendation for accuracy and context.
3. Communication	Sends summary to employee with links to enrolment forms and FAQs.	Follows up with employee if clarification or escalation is needed.
4. Exception Handling	Flags tickets with missing data or policy conflicts.	Resolves exceptions and updates agentic training data.
5. Audit & Feedback	Logs actions and learns from human feedback.	Audits agentic decisions and provides feedback for improvement.

How the Human and the Agentic AI Assistant Work Together to Select Benefits for an Employee

The agentic AI evolution is not about replacing people with automation—it's about redefining how humans and AI work together as complementary partners. Across industries, leading organizations are redesigning roles and workflows to integrate AI into editorial, creative, and strategic functions. Rather than viewing AI as a threat, they're embracing it as a catalyst for efficiency and innovation. The distinction lies in mindset: success favors the enterprises that approach AI adoption with purpose and foresight—retraining teams, redesigning processes, and embedding AI where it amplifies human capability.

At its core, this transformation shifts AI from an emotional flashpoint to an operational advantage. Creative professionals—writers, editors, designers—are not being replaced; their capacity is being elevated. Enterprise AI now accelerates research, produces initial drafts, and automates routine production, creating time and space for people to focus on what they do best: shaping strategy, safeguarding brand integrity, and exercising human judgment where it matters most.

In the feature below, AI and Human Agents and existing workflows orchestrate secure flows between public and private datasets within a private cloud, automating claims, protecting sensitive information, and enforcing compliance. This pattern unifies public cloud agility with on-premises governance and end-to-end data integrity.

Case Study

Clerk of the Circuit Court, A U.S. County

The Clerk of the Circuit Court in one U.S. county oversees a complex judicial ecosystem—maintaining court records, securing evidence, collecting fines, and managing documentation across 24 municipalities and unincorporated areas. For decades, paper-based systems created bottlenecks: clerks manually verified citations, judges relied on manila folders, and every data entry step slowed the pace of justice. The challenge wasn't just inefficiency—it was scale. As population growth accelerated, the volume of traffic cases threatened to overwhelm staff capacity and delay court outcomes.

By introducing AI-driven automation inside a governed case management platform, the County transformed its courtroom operations. Agentic AI now monitors case status, validates records, and routes documents securely across systems—while human clerks remain in the loop to approve exceptions and verify edge cases. Judges can instantly retrieve digital case histories, access integrated state traffic databases, and review prior citations through a unified dashboard.

Behind the scenes, AI agents connect the County's in-car ticketing system, document repositories, and court databases—automating the capture, classification, and validation of information. Sensitive data never leaves the County's private cloud, and every decision point is logged for audit and compliance. What once required manual data entry now happens in seconds, freeing clerks to focus on higher-value tasks and reducing the risk of human error.

With this hybrid AI model—combining agentic automation with human oversight—the Clerk's office has modernized its entire information ecosystem. The outcome: faster case processing, stronger data integrity, and full alignment with state mandates for information sharing. It's a blueprint for responsible AI in government—showing how intelligent systems and human judgment can work side by side to deliver more trusted, efficient public service.

4. Performance Management and Measurement

Measuring the Success of Your Agentic AI Application

Measuring outcomes is at the heart of whether an agentic AI application succeeds or fails. Therefore, these measurements must be clearly defined upfront in a job description that outlines the agent's objective, tasks, and metrics. This 'job description,' created while developing the business case, is the key to setting the proper scope for the agent's role.

Today, there is no universally defined or adopted standard for KPIs for agentic EAI applications, although there are standards across many countries and regulatory bodies around AI (ethics, transparency, risk, etc.). In the absence of a universal standard, organizations can leverage the many frameworks in the public domain, either adopting one directly or adapting it, depending on their specific implementation.

A framework proposed in the *International Journal of Scientific Research and Modern Technology* looked at "five vital dimensions –Model Quality, System Performance, Business Impact, Human-AI Interaction, and Ethical and Environmental Considerations." On the Model Quality dimension, the paper examined accuracy, precision, task completion, hallucination, and output. Operational Key Performance Indicators (KPIs) were focused on latency, throughput, and resource utilization. Business Impact assessed ROI, cost savings, productivity improvements, and market impact. Human-AI Interaction was examined in terms of user satisfaction, trust, adoption, and engagement. Finally, in terms of Ethical and Environmental Considerations, the paper examined bias, fairness, transparency, environmental impact, and ethical drift.[65]

While all of these KPIs may not be relevant to every agentic AI deployment, it's important for teams to adopt a holistic approach to selecting the different dimensions. After the relevant KPIs are determined, they can be formalized into a scorecard. This approach mirrors the one successfully used for Robotic Process Automation (RPA), where scorecards were key to driving automation and efficiency. The same rigor should be applied here, with daily assessments against the agent's key dimensions.

Equally important is having a defined remediation framework and process. Not all enterprise AI applications will be successful, and for those that fail, this framework is essential to understanding the root cause and making a data-driven decision about whether to invest in a fix or decommission it. This process directly supports a "fail fast" culture—a shift that many organizations struggle with. Teams must be taught to accept that it is better to decommission a failing project than to force something to work that will never achieve its anticipated outcome.

It's also important to remember that EAI thrives on secure, contextual data, not just quantity. By connecting structured systems, unstructured content, and inter-organizational flows across the EIM Cloud, organizations can train and deploy agents that act responsibly, trace their decisions, and meet compliance requirements by design. In the next chapter, we'll examine the evolution from Agentic AI to AGI.

The Fast Five Download

1. **Choose the Right Organizational Model for AI Deployment.**
   Selecting an appropriate deployment model—Centralized, Hub-and-Spoke, Federated, or Hybrid—is foundational for successful agentic AI adoption. The model should clarify ownership, accountability, and governance, balancing control with agility based on your industry's needs and regulatory environment.

2. **Adopt a Phased and Cohort-Based Rollout Strategy.**
   Rushed AI adoption often leads to missteps. Successful organizations roll out agentic AI applications in deliberate phases targeting specific business units or regions. This cohort-driven approach ensures readiness, maximizes user adoption, and tailors support to each group's unique requirements.

3. **Start Small, Focus on Business Value, and Build from Success.**
   Begin with simple, well-defined use cases, prioritizing business units with mature processes and strong data quality. Empower change agents such as Product Owners to drive adoption and iterate based on early wins before scaling to more complex scenarios.

4. **Integrate Digital Agents into Workforce Planning and Management.**
   Treat AI agents as an extension of your workforce. Define clear roles and expectations for digital agents, adopting HR practices like job descriptions and performance objectives to ensure alignment between human and AI team members, and to foster organizational understanding and acceptance.

5. **Implement Rigorous Performance Measurement and Remediation.**
   Success hinges on clearly defined KPIs across multiple dimensions (model quality, business impact, human-AI interaction, ethics, and system performance). Develop scorecards for agents, regularly assess outcomes, and be prepared to remediate or retire underperforming applications. Embrace a culture that learns from failures and iterates quickly.

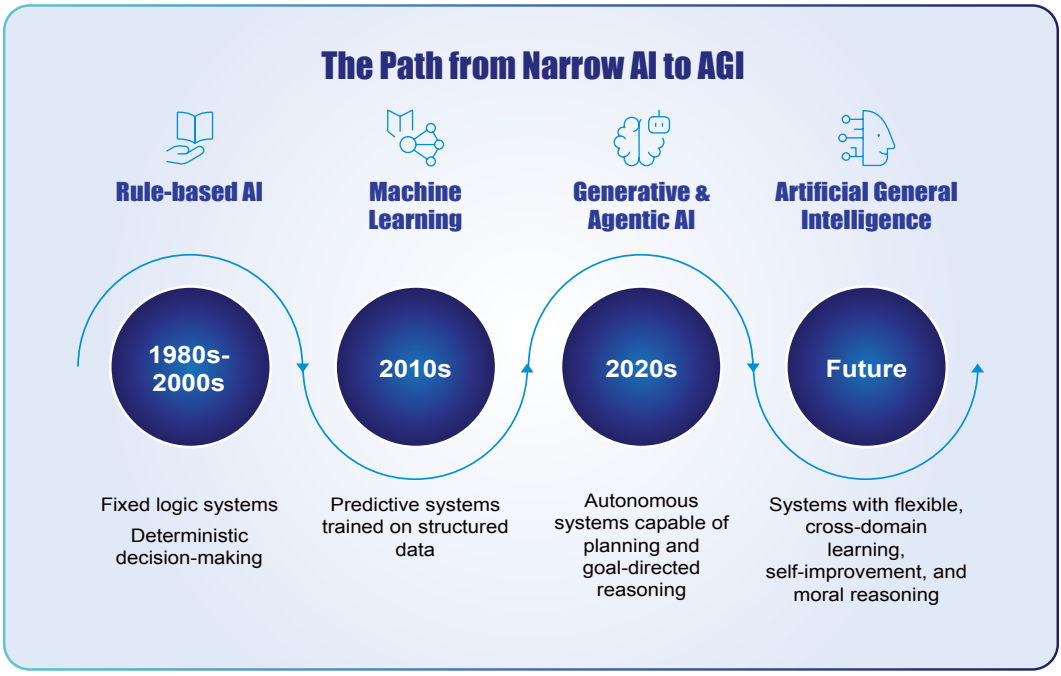
Chapter Ten

The Creation of AGI from Agentic AI

As we have explored in this book, the story of AI is a story about aspiration and innovation—the desire to create systems that can compute and comprehend, respond and reason. Agentic AI shows us a glimpse of what is possible and moves us towards the frontier models that pave the way to Artificial General Intelligence (AGI). AGI will extend EAI's trajectory towards systems capable of human-like generalization, learning across domains, forming abstract concepts, and acting with autonomy.

Enterprises looking to deploy intelligent systems at scale must plan for the governance, orchestration, and lifecycle management of agent networks, not just individual models. As these frameworks evolve, they serve as building blocks on the path from agentic AI toward broader, more adaptive cognitive systems—systems that will challenge traditional architectural, operational, and governance models.

This chapter explores the shift from agentic AI—systems that pursue goals and learn with human guidance—toward the promise of AGI, a form of intelligence capable of human-like understanding, reasoning, and adaptation across diverse contexts. It highlights the technical and ethical foundations required for this transition and explores the ongoing debate about whether AGI will arise from scaling up current models or from breakthroughs in new architectures, reasoning abilities, and emotional intelligence.



The Path from Narrow AI to AGI

Agentic AI: The Bridge Towards AGI

While agentic AI can perform task-specific actions, it has domain constraints and cannot learn across domains. Its reasoning is contextual but not conceptual; it cannot abstract principles or generalize learning. In contrast, AGI can learn, reason, and adapt across a broad range of tasks. AGI approaches the flexible intelligence characteristic of human cognition.

The transition from agentic AI to AGI is not simply a matter of more data, but of architectural approach. Researchers debate whether AGI will emerge from scaling current foundation models or require a new method of reasoning, experience, and emotional intelligence. Two different approaches are dominating the early thinking on this topic:

1. Scaling Hypothesis: Predicts that AGI will emerge from continued scaling of today's large language and multimodal models, without requiring new algorithms. In *Scaling Laws for Neural Language Models*, the authors explain the relationship between model performance and three factors: model size, dataset size, and compute capacity, "Our results strongly suggest that larger models will continue to perform better and will also be much more sample efficient than has been previously appreciated. Big models may be more important than big data. In this context, further investigation into model parallelism is warranted. Deep models can be trained using pipelining, which splits parameters depth-wise between devices, but eventually requires increased batch sizes as more devices are used."[66]

2. Discontinuity Hypothesis: Predicts that AGI will not emerge simply by scaling up existing LLMs or neural architectures, but will require fundamentally new paradigms, architectures, or forms of cognition. Some experts argue that scaling neural networks will not deliver AGI because they lack structured reasoning, causal models, and compositional generalization—essential features of human cognition. Gary Marcus, for example, has asserted the importance of symbols over neural networks in furthering AI:

> "Symbols [computer-internal encodings, like strings of binary bits, that stand for complex ideas] still far outstrip current neural networks in many fundamental aspects of computation. They are much better positioned to reason their way through complex scenarios, can do basic operations like arithmetic more systematically and reliably, and are better able to precisely represent relationships between parts and wholes (essential both in the interpretation of the 3-D world and the comprehension of human language). They are more robust and flexible in their capacity to represent and query large-scale databases. Symbols are also more conducive to formal verification techniques, which are critical for some aspects of safety and ubiquitous in the design of modern microprocessors. To abandon these virtues rather than leveraging them into some sort of hybrid architecture would make little sense."[67]

In all likelihood, the path from agentic AI to AGI will not be a simple one, but instead a mix of model and capability expansion, driven by improvements in data quality, model interpretability, the availability of compute, and leveraging symbolic reasoning beyond traditional neural networks.

The Role of Agentic AI and Enterprise Orchestration

As agentic AI deployments mature, they provide a first step in enabling hybrid approaches towards the development of AGI. With agentic AI, complex human-level tasks are naturally decomposable and can be distributed. Specialized agents can be used for functions such as planning, researching, coding, verifying, simulating, and managing. The agents perform discrete functions and can operate in parallel and collaborate, reducing the cognitive and computational burden on any single model.

In parallel, specialized agents can be improved independently and reused across tasks. Agents can also adopt distinct learning approaches, leveraging reinforcement learning for optimization, symbolic reasoning for logic, or unsupervised learning for discovery. This modularity enables the creation of a hybrid learning system.

In combination with the agents, the orchestration layer provides a central coordination mechanism. The orchestrator handles task management by decomposing and assigning tasks, scheduling, and allocating resources. It also manages communication by routing context between agents, and provides oversight by validating outputs, monitoring performance, and managing the system lifecycle.

Crucially, the orchestration layer also enables learning orchestration, enabling the entire agentic system to improve over time based on distributed experiences. Yet, it is essential to recognize that orchestration alone does not equate to cognition; many current systems lack long-term planning, persistent memory, reasoning, and model-based causal understanding. From a design perspective, the orchestrator should evolve from a simple task scheduler into a meta-controller with core capabilities such as goal management, dynamic resource and role allocation across agents, reflective error and feedback loops, and continuous evaluation/assurance pipelines. This modular, orchestrated approach forms a viable foundation for training hybrid AGI systems

In the following feature, find out how a Portuguese municipality has improved productivity and cut operational costs using AI-driven automation.

Case Study

A Portuguese Municipality

As part of the urban agglomeration of Greater Lisbon, the municipality employs a workforce of over one thousand employees. For the public sector organization, managing the growing complexity of digital operations was problematic. Fragmented systems and manual workflows made it difficult to classify and prioritize requests, track interventions, or maintain accurate records. Data existed, but insight did not. Without integrated oversight, teams were forced into reactive decision-making and struggled to maintain compliance across evolving regulatory standards. The result was a lack of transparency and accountability—an obstacle that modern AI governance models are uniquely designed to overcome.

To address this, the organization established a unified, AI-driven management framework capable of orchestrating workflows, classifying requests, and predicting service demand through pattern recognition. By introducing structured governance and intelligent automation, it gained real-time visibility into performance, resource allocation, and compliance adherence. Instead of manually managing processes, the enterprise now operates through a self-optimizing system that learns from each interaction. Agentic AI components continuously analyze performance data, refine workflows, and flag emerging inefficiencies—paving the way for adaptive service management aligned with enterprise strategy.

These developments represent more than operational improvement; they signal a step toward AGI-like enterprise intelligence. With AI now embedded across service management, the system not only responds to user requests but anticipates them—analyzing context, predicting outcomes, and coordinating across teams. As these agentic systems evolve, they form the foundation of an organization capable of learning, reasoning, and improving at scale. What began as an effort to streamline IT operations has become a model for how intelligent governance, human oversight, and adaptive AI can coexist—creating an enterprise where automation doesn't replace people but empowers them to think and act with greater intelligence.

By the Numbers: The Impact of Intelligent Governance

- **60% faster request resolution** after replacing manual workflows with AI-driven classification and prioritization.
- **Up to 40% reduction in operational costs** through automation of contract, asset, and service management.
- **100% visibility** into performance metrics and compliance adherence across all service domains.
- **50% fewer process errors** due to automated validation, audit trails, and real-time anomaly detection.
- **Continuous learning loop** established: agentic AI systems now refine workflows autonomously based on data trends and feedback.
- **Cross-functional collaboration** improved across departments, replacing silos with transparent, adaptive workflows.

Data as an Enabler to AGI: Fueling Cognitive Scale

The foundation of the evolution to AGI remains data, where data quality, diversity, and governance are the primary enablers. Agentic AI thrives on structured and semi-structured data within defined operational boundaries. AGI, however, requires a richer and more representative dataset capable of supporting higher-order reasoning. This is why the need for data is only growing in importance as technology evolves.

Data for AGI must capture context, causality, and ethics. This requires data frameworks, federated data-sharing models, and sovereign data infrastructures that ensure responsible access and use. The OECD AI Principles (2019) and ISO/IEC 42001:2023 standard both emphasize that AI systems should operate under well-defined data governance mechanisms ensuring fairness, accountability, and traceability.

Privacy-enhancing technologies also play a critical role. As AI moves closer to general cognition, maintaining data ethics and integrity becomes as essential as performance metrics.

Governance and Ethics: Aligning Autonomy with Accountability

As agentic AI systems become more independent, questions of control, accountability, and oversight are key, as we reviewed in Chapter 4. However, the challenge increases as we approach AGI, which has a level of autonomy beyond human capability. Ethical frameworks for enterprise AI have historically focused on fairness, transparency, and explainability. However, as systems begin to make complex decisions, it will be important to ensure that AI systems' goals remain consistent with human values.

As discussed in Chapter 6, international governance efforts are converging around this challenge. The EU Artificial Intelligence Act (2024) establishes tiered risk categories for AI and mandates strict oversight for high-risk applications. The UNESCO Recommendation on the Ethics of Artificial Intelligence (2021) calls for human rights-based governance, while NIST AI RMF (2023) introduces trustworthiness as a measurable element. These initiatives ensure that AI systems remain subject to human intent and oversight even as their capabilities expand.

From a policy perspective, AGI could enable a new level of autonomy, in which systems might adapt or self-improve in unpredictable ways. Anticipating this, researchers in AI safety are looking into new standards. Again, this needs to happen in parallel with the technology evolution so that, once AGI is ready, the standards are prepared as well.

The Enterprise Relevance of AGI-Like Systems

As enterprises deploy increasingly autonomous and interconnected agentic AI systems, many are already encountering early signs of Artificial General Intelligence in practice—though not in name. What we call "AGI-like" systems are emerging organically across organizations: intelligent agents that learn from multiple data sources, coordinate decisions across departments, and adapt their behavior based on shifting objectives or external context. These aren't isolated tools; they're self-optimizing networks of intelligence, continuously refining how work gets done.

The shift is subtle but profound. Where once automation replaced narrow, repetitive tasks, agentic AI now integrates reasoning, planning, and self-correction. A financial services team might deploy agents that analyze customer sentiment, predict churn, and autonomously generate retention strategies—activities that span marketing, risk, and compliance in a unified feedback loop. In manufacturing, AI systems can already interpret sensor data, reallocate supply chain resources, and flag ethical sourcing risks before human teams intervene. The line between specialized automation and enterprise-scale cognition is blurring rapidly.

This evolution carries immense strategic opportunity—but also risk. Without effective governance, enterprises may find themselves managing systems that learn and act beyond their intended design. As noted by Gartner, over 80 percent of organizations pursuing AI at scale cite governance and transparency as their biggest obstacles to adoption.[68]

Managing AGI-like systems requires new models of accountability and oversight. Traditional IT management was built for static systems; modern intelligence ecosystems demand adaptive governance—where oversight mechanisms evolve alongside the AI itself. Explainability, auditability, and feedback loops must become design features, not afterthoughts. And, as these systems begin to reason across domains, human judgment must remain in the loop—not to slow decisions, but to steer them.

In this sense, AGI is not a distant horizon but a growing enterprise reality. The organizations that will lead in this era are those that recognize intelligence as infrastructure—something to be governed, integrated, and continuously improved, just like data or cybersecurity. The result is not machines that replace human capability, but intelligent systems that amplify it—scaling enterprise insight, accelerating transformation, and building a foundation of trust for whatever comes next.

In the feature below, a top South African university is using an AI-powered automated service desk to transform student experiences and ensure business continuity when crisis hits.

Case Study

A South African University

> *The value of machine learning is phenomenal in our student community, as evidenced by the wide use of our virtual agents and knowledge articles. Without machine learning and AI there is absolutely no way we could support our end users with the few dedicated agents we have.*
>
> Change and Configuration Manager, University in South Africa

One of Africa's top universities produces research to find solutions for pressing issues. The University teaches in the classroom, online, and embedded in communities. Faced with unprecedented scale and digital inequality, the university set out to transform how it delivered education and support in an increasingly hybrid world. With a student population exceeding 130,000 and only a handful of dedicated support agents, manual processes were no longer sustainable. Limited access to devices and connectivity deepened the digital divide, while non-technical departments struggled to adapt to remote workflows. The challenge wasn't simply technological—it was structural. The institution needed an intelligent operating model capable of supporting both academic and administrative continuity while empowering every student to participate fully in a connected ecosystem.

To meet this challenge, the university re-engineered its digital service framework around automation, governance, and intelligence. AI-driven systems were introduced to classify requests, predict demand, and route tasks automatically, allowing a small team to manage massive volumes of support interactions in real time. When COVID hit, machine learning capabilities accelerated adaptation during the global shift to remote learning—automating VPN access, provisioning laptops, and optimizing connectivity support for thousands of students. Agentic AI became the invisible backbone of the university's digital infrastructure, orchestrating workflows across departments and extending intelligence to non-IT functions such as enrollment, student services, and library operations. Each system learned from interactions, improving accuracy, responsiveness, and fairness across the institution.

What began as a crisis response evolved into a model for AGI-ready education—one where adaptive intelligence enhances both scale and equity. Today, service request volumes have increased dramatically, yet efficiency and transparency have improved in equal measure. AI not only supports staff and students—it collaborates with them, learning from patterns, context, and feedback to anticipate needs and streamline decision-making. The university's transformation demonstrates how intelligent governance and agentic automation can bridge human and digital capability, laying the foundation for an academic ecosystem where intelligence is distributed, collaborative, and continually self-improving.

Defining the Future of AGI: Beyond the Technical Horizon

The pursuit of AGI is as much a philosophical and social journey as it is a technical one. While some view it as the logical outcome of scaling current architectures (Scaling Hypothesis), others see it as a redefinition of intelligence itself, a step toward systems that possess intentionality, moral reasoning, and self-awareness (Discontinuity Hypothesis).

If agentic AI represents the automation of action, AGI represents the automation of understanding. Future AI systems must not only think and learn but also align with collective human values, which is a challenge that will define the next decade of enterprise AI policy and innovation. The transition from agentic AI to AGI is not solely about machines surpassing human capability; it is about how human and machine intelligence evolve together.

As AI systems become more capable, they will also reshape the roles of the human workforce. And for this reason, human oversight must remain a priority—from a policy and governance perspective as well as an execution and operations perspective. Roles that are commonplace today may no longer be required, but equally new roles will emerge. These could range from training and managing the agentic AI capabilities, to ensuring data quality and governance, to leveraging AI to create new products and capabilities that are not envisaged today. With each shift in technology comes new opportunities, and AGI will be no different.

The future of work will not be defined by human replacement, but by human–machine partnership. Designing effective collaboration models between human specialists and generalist AI systems means clearly defining roles, authority, and accountability within shared workflows. It also means investing in continuous training and digital fluency so teams understand how to question, interpret, and guide AI outcomes responsibly. In a world where AI can learn faster than its creators, sustaining trust and ethical oversight becomes the anchor—ensuring that intelligence serves humanity's goals, not the other way around.

In this chapter, we explored the evolution from agentic AI to the possibility of AGI, which would exhibit human-like reasoning, learning, and adaptability across diverse contexts. This transition will involve not just scaling data but also integrating improved data quality, model interpretability, and symbolic reasoning, paving the way for hybrid EAI systems that can tackle complex tasks through specialization and collaboration.

Looking ahead and considering that AGI is not the replacement of human intelligence, but its next great amplifier, data that is managed and governed in EIM will play a crucial role as an enabler of AGI. It will provide the foundational knowledge necessary for these advanced systems to learn, make sound decisions, and adapt in increasingly complex and dynamic environments. Investments made today in agentic AI will be valuable in the evolution to AGI.

In the following feature, find out how a Mexican retail analytics provider transforms sales data into actionable insights to boost revenues.

Case Study

A Mexican Retail Analytics Company

> *Using AI we have achieved a quantum leap in performance and dramatically reduced query response times. Our clients now have the critical data they need at their fingertips to optimize their sales revenues.*

Manager Director, Retail Analytics Company

The company delivers an AI-powered analytics platform that enables retailers to optimize sales performance and decision-making. Serving over 130 leading consumer brands across Latin America, the cloud-based system unifies sales and inventory data, analyzes purchasing behavior in real time, and generates predictive insights to guide smarter, faster operational decisions.

The company set out to solve one of commerce's most persistent challenges: balancing supply and demand with precision. In a world where consumer preferences shift by the minute, the ability to synchronize sales, inventory, and pricing decisions is critical. Yet, legacy systems built on traditional databases struggled to scale with the volume and velocity of data being generated. As transaction loads soared, the company found its architecture strained—queries slowed, insights lagged, and the ability to make real-time adjustments faded. For businesses depending on timely intelligence, this was more than a technical bottleneck; it was an existential risk to competitiveness.

To move beyond reactive reporting, the company reimagined its analytics platform through the lens of AI. Machine learning and adaptive algorithms now process billions of records daily, identifying emerging demand patterns and optimizing distribution at scale. The introduction of AI-powered simulation tools enabled predictive pricing strategies that once took hours to calculate to be executed in seconds. These systems learn continuously from historical data, testing new variables, and refining elasticity models across thousands of products and regions. The result is a platform that doesn't just describe what happened—it anticipates what will happen next, transforming static analytics into a living, learning system of intelligence.

This evolution marks a shift from analytics to cognition—a step toward enterprise-level AGI. By embedding reasoning, prediction, and self-optimization into its operations, the company has built a digital nervous system capable of adjusting in real time to market behavior. Every new transaction becomes a learning signal, strengthening the feedback loops that guide future strategy. With each iteration, the system grows more attuned to human decision-making—amplifying, not replacing it. What began as a search for faster insights has evolved into a glimpse of the cognitive enterprise: one where intelligence is distributed, collaborative, and continuously self-improving.

The Fast Five Download

1. **Agentic AI as an Enterprise Foundation.**
   Agentic AI serves as a crucial stepping stone towards AGI by enabling task decomposition, specialization, and collaboration among autonomous agents. This modular approach lays the groundwork for more flexible, scalable, and human-like intelligence systems.

2. **Competing Paths to AGI.**
   The transition to AGI is shaped by two dominant hypotheses: the Scaling Hypothesis (AGI emerges from scaling current models) and the Discontinuity Hypothesis (AGI requires fundamentally new architectures and reasoning). Executives should monitor both trajectories for strategic planning and investment.

3. **Data Strategy is Critical.**
   Progress toward AGI will be driven by data quality, diversity, and governance. Organizations must prioritize robust data frameworks, privacy-enhancing technologies, and compliance with evolving international standards to fuel advanced AI capabilities.

4. **Governance and Ethics at the Core.**
   As AI systems become more autonomous, aligning their actions with human values is essential. Executives must champion strong governance, ethical oversight, and risk management frameworks to anticipate regulatory requirements and societal expectations.

5. **Prepare for Workforce and Policy Shifts.**
   The evolution from agentic AI to AGI will redefine workforce roles and policy landscapes. Proactive investment in talent, change management, and ongoing human oversight will be vital to harness AGI's potential while mitigating risks.

Chapter Eleven

The Future of EAI and Operations Management

Often overlooked, operations management plays a vital role within the enterprise by supporting all business units and driving business growth. As operations practices have transformed over time, AI has become pivotal in this realm. In this chapter, we will explore the evolution of enterprise AI and operations management, and how understanding it is essential for maximizing the benefits of agentic AI deployments.

Earlier in this book, we examined the convergence of trusted data and AI in delivering innovative experiences and operationalizing agentic AI. We also considered its effects on the workforce and within the organization, and strategies for managing and maintaining an AI workforce.

Clear and specific job descriptions and measurable KPIs for both human and digital workforces are essential for success. Assigning the digital workforce simple logic and small, well-defined tasks allows them to operate efficiently. When multiple digital agents work together, they can handle more complex tasks. Meanwhile, humans retain oversight, enabling them to quickly identify and address issues or anomalies. This approach is like conducting an orchestra: when each instrument plays its part, the conductor can easily detect if one is out of tune, ensuring a harmonious performance.

The pages ahead focus on all aspects of EAI-driven operations management—essentially, how to keep your infrastructure, platforms, data, human workforce and now, digital agents, in harmony 24/7.

Discover how a global leader in healthcare technology was able to improve their operations by implementing a sophisticated automated predictive maintenance platform that leverages advanced AI and machine learning algorithms.

Case Study

A Global Leader in Healthcare

> *Our predictive maintenance system, built on vast amounts of data and advanced AI models, allows us to detect and address potential issues before they impact clinical operations. This improves the reliability of our equipment and enhances patient outcomes and satisfaction.*
>
> Principal Architect, Service

A health technology organization faced mounting challenges maintaining its advanced medical imaging systems—MRI and CT scanners that are vital to patient diagnosis and care. A single MRI unit can log over a million events and produce 200,000 sensor readings each day, spanning tens of thousands of data points. Yet, in such a complex and tightly regulated environment, medical devices take years to develop and certify. While they generate vast amounts of operational data, that data was never structured to enable predictive maintenance.

The transition was not only technical, but also operational, because the organization had to rethink existing processes. It required the integration of massive datasets from medical devices, advanced analytics, and machine learning models to predict and prevent potential failures before they could disrupt patient care.

Improving patient health care is the organization's top priority. Using AI, they are able to process complex datasets efficiently and identify patterns that indicate imminent issues, allowing them to take preventive action well in advance. The company has integrated more than 200 data streams—real-time logs, error reports, and performance metrics—into a single data warehouse holding over a decade of history and 1.5 petabytes of continuously refreshed information. Predictive models now mine this vast dataset to spot anomalies early, enabling proactive maintenance and reducing costly equipment downtime by 30 percent. The system has led to 50 percent of CT service cases being diagnosed and resolved remotely, and an 84 percent first-time fix rate for onsite equipment issues—enhancing the company's service efficiency and improving overall patient care outcomes.

Defining the Future of AGI: Beyond the Technical Horizon

The future of operations management will fundamentally hinge on the adoption of AI and its transformative impact on operational experiences. Several key factors are crucial:

1. **Transitioning from Reactive to Autonomous Operations**
   Being reactive is no longer an option in the operations domain. Cyber threats, as well as network and technology complexity, demand 24/7 autonomous operations that detect and act on issues before they impact customers.

2. **Evolution of Operations Management**
   Over the past two decades, operations has undergone major transformations, becoming far more efficient through advances in data collection, management, and analysis.

3. **Core Elements of AI in Operations**
   EAI operations depend on five key components: data utilization, intelligence formulation, decision-making processes, human intervention within the operational loop, and a comprehensive feedback lifecycle. This holistic approach enables operations teams to navigate the transition from manual to automated methodologies effectively.

4. **Application of AI in Network and Security Operations**
   Agentic AI has the potential to transform network and security operations. Later in this chapter, we'll explore practical use cases that show how agentic AI enhances operational effectiveness.

5. **Transformational Impacts on Operations Metrics**
   The transitions described bring deep changes to core operations metrics such as Mean Time to Restore (MTTR), service availability levels, outage numbers, incident numbers, and the ability to achieve Five Nines availability (when technology and services are up and running 99.999% of the time, the gold standard in operations). Adopting AI will bring significant changes and benefits to each of these areas.

Now that we've introduced them, we can look at each of the five transitions in detail.

1. From Reactive to Autonomous Operations

The size and scale of networks and enterprise operations have made manual and reactive monitoring things of the past. Historically, operations teams responded to issues as they arose, leading to a predominantly reactive operational posture. However, in recent years, operations leaders have been striving to enhance their teams' capabilities, transitioning towards a more proactive approach. This involves not only understanding potential incidents but also identifying and mitigating these issues before they escalate into significant outages. Modern monitoring tools have advanced significantly, enabling the detection of minimal changes in operations, latency, or performance metrics related to specific services or applications. These tools are designed to provide early warnings of potential problems. Similar to fire alarms, they allow teams to act before a minor issue becomes a widespread disruption.

Despite these advancements, a substantial segment of operational practices remains heavily reactive. The evolution towards autonomous operations marks a significant shift in this paradigm. With the integration of EAI, operations teams can attain a more granular understanding of system dynamics, including the complex correlations between various activities and events that contribute to incidents. This deeper insight is crucial for not only enhancing the proactive capabilities of teams but also for implementing self-healing mechanisms within operations. Such autonomous capabilities enable systems to automatically address certain issues, thus alleviating the operational workload.

As a result, operations teams can redirect their focus to higher-priority tasks and preventive measures that are essential for mitigating the occurrence of incidents. The adoption of EAI provides a transformative opportunity to redefine how operations are managed, shifting from a primarily reactive stance to a more strategic and proactive framework that is essential in today's dynamic operational environment.

2. The Evolution of Operations Management

Operations management has traditionally been associated with teams working in dark operational centers, constantly monitoring screens for critical alerts. However, the reality of operations management has significantly evolved. In its early stages, operations relied heavily on manual monitoring and troubleshooting of critical events. The introduction of automation through scripting represented a significant advancement, enabling teams to automate specific tasks, enhance repeatability, and reduce human error.

With the advent of artificial intelligence and the adoption of agentic AI, operations management can now leverage more sophisticated analytical capabilities. EAI tools can effectively assemble and analyze vast amounts of data, facilitating root cause analysis by identifying anomalies and detecting changes in data patterns. This process enables operators to correlate different datasets, which has become increasingly essential in identifying root causes of issues. The ability to quickly pinpoint these causes is critical to minimizing operational downtime.

Furthermore, EAI enhances predictive analytics within operations. By examining trends, activities, timelines, and the relationships between various symptoms, causes, and effects, AI facilitates the forecasting of operational challenges and outcomes. This marks a significant shift in how operations management is approached today and suggests a future wherein operations management will be radically different.

The evolving landscape also necessitates changes in the skillsets required for operations management. There is a growing trend of developers joining operations teams in roles such as Site Reliability Engineers (SREs). These professionals utilize their technical expertise to address incidents, identify root causes, and develop solutions to these issues in real time, thereby preventing issues from recurring. A blend of domain expertise and programming proficiency, augmented by AI, is becoming increasingly pervasive across operations.

Today's operations center also serves as the primary training ground for applying enterprise AI and cutting-edge technologies to solve high-stakes challenges. Organizations that successfully position their operations centers as critical hubs of innovation and talent development are better equipped to attract, train, and retain top performers. These centers become the proving grounds where future leaders hone their development and problem-solving skills, ensuring a robust pipeline of talent ready to take on leadership roles within the organization.

As operations management continues to evolve, it serves as a valuable training ground for senior developers in product and technology companies. These individuals gain firsthand experience with incidents affecting customers and operations, allowing them to apply this knowledge in product development roles. Ultimately, this understanding of advanced operations management will significantly inform their future contributions to the field.

Operations, once viewed as an antiquated, round-the-clock function focused solely on monitoring issues, has evolved into the central nervous system of the organization—a true center of excellence for innovation.

A South African retailer is doing just this—analyzing data on how its teams use AI to best adapt its processes and optimize performance.

Case Study

Leading Retailer of Consumer Goods in Africa

> *With AI integrated in our product testing processes, it takes literally two seconds to understand where we are per sprint, per release, per feature level, for every application we test in our omnichannel space.*

SQA Manager

With thousands of stores across South Africa and in seven other countries, this leading retailer of consumer goods in Africa manages a massive portfolio of digital omnichannel applications. The company also has a strong online shopping presence for its grocery, home, and clothing businesses, including a mobile app for ultra-fast local delivery of groceries.

Keeping physical stores replenished and digital applications running smoothly is vital in a highly competitive market. Under constant time-to-market pressure, the retailer integrated AI into their process to speed up product testing and release. The AI-enabled acceleration of test-case creation has opened the way for the retailer to adopt in-sprint and in-release automation. This has enabled them to automate much earlier in its two-week sprints, driving a massive increase in automation coverage from about 65% to about 95%.

In just eight weeks, across almost twenty applications tested in omnichannel, the retailer has completed four to five releases a week. They've cut cycle times by 43 percent, increased release frequency 60x, and improved test coverage with faster insights to speed time to market. With performance outcomes like these, the retailer is investigating the potential of applying AI across additional business functions.

3. Core Components of AI-Driven Operations

As organizations evolve their operations and adopt advanced AI capabilities, several foundational layers must be addressed.

A. The Data Layer

Building a unified and accessible data layer is critical. Traditional operations often suffered from fragmented data—spread across multiple systems, service management tools, and organizational silos. Bringing these datasets together, and enabling AI agents to operate across them, dramatically improves visibility and detection capabilities. For example, integrating security and network operations allows security logs to be analyzed alongside network data. This broader dataset enables teams to identify and resolve issues or incidents more effectively by seeing the full picture in real time.

B. The Intelligence Layer

This is where language models, machine learning, and generative and agentic AI platforms operate. Within this layer, correlations are drawn, knowledge is built, and AI applications begin to work alongside human analysts. Generative AI enhances situational understanding and supports faster, more informed responses within the operations center. Agentic AI applications enable autonomous operations.

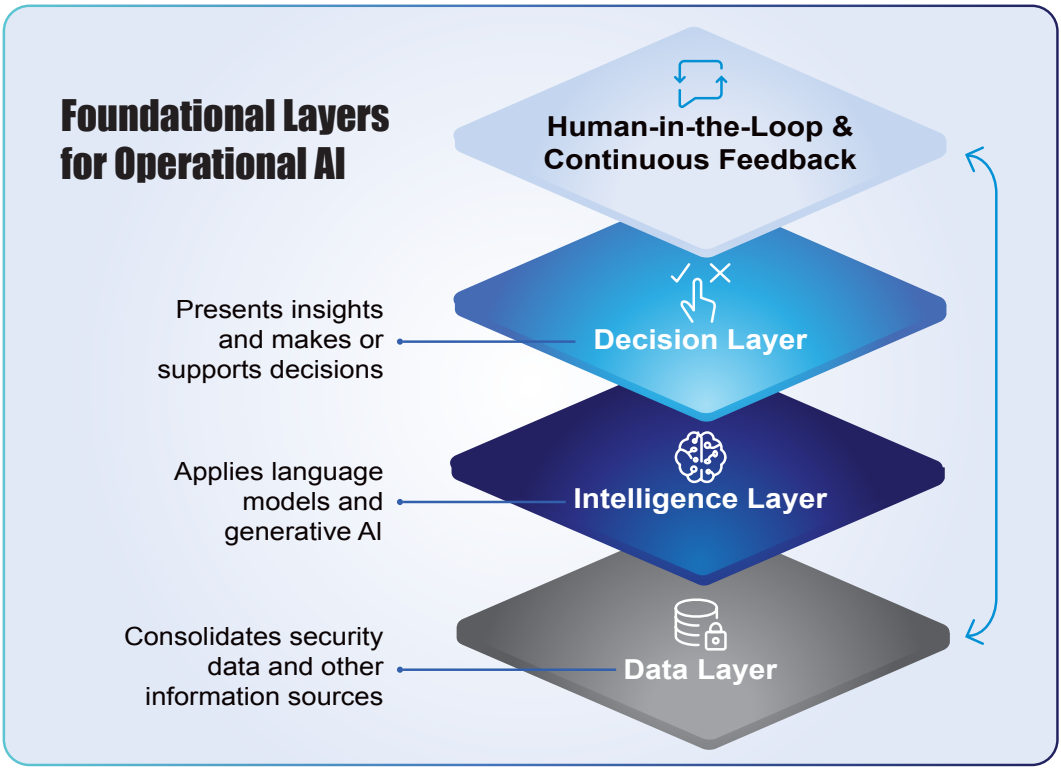
C. The Decision Layer

Analyzing data is one thing—making decisions based on it is another. In the early stages of AI adoption, most operations centers have preferred to have AI present insights while leaving the final decisions to human operators. As maturity grows, organizations are beginning to allow AI systems to make certain predefined or low-risk decisions autonomously. Over time, as AI models and governance structures evolve, these systems will handle more complex, repeatable decisions.

D. Human-in-the-Loop and Continuous Feedback

Even in AI-driven environments, humans remain essential. Their evolving role centers on oversight, contextual understanding, strategy, high-stakes judgement calls, and AI system improvement.

Equally critical is the feedback loop. As incidents are resolved and root causes identified, feeding this information back into the system ensures continuous learning, which in turn makes recovery faster each time or reduces MTTR. This minimizes repeat incidents and strengthens consistency in response. When operations teams address root causes effectively, incident volume drops—freeing time for proactive, innovative AI work that enhances resilience and efficiency across the operations center. Working together, these key components enable the AI-driven operations required to effectively support agentic AI.



Foundational Layers to Address

4. Agentic AI in Network and Security Operations

The role of the Network Operations Center (NOC) operator is one of high stress and tight deadlines and often involves searching for a needle in a haystack. Success is measured by how much time a task takes. Before the introduction of agentic AI, NOC operators would need to find correlation or similar issues in vast databases, so they could locate repeat issues and data that would help solve the issue at hand. The example below demonstrates the benefits of partnership with an agentic AI application. The agent can help search the database to better pinpoint past issues, glean learnings, and then help the operator resolve the current issue not in hours, but minutes.

5. Transformational Impacts on Enterprise Operations

Consider this: It's 2:47 AM when a global e-commerce NOC detects database latency spikes hammering their payment processing. The monitoring system automatically fires the alert, but agentic AI changes everything.

From Hours to Minutes with AI Agents

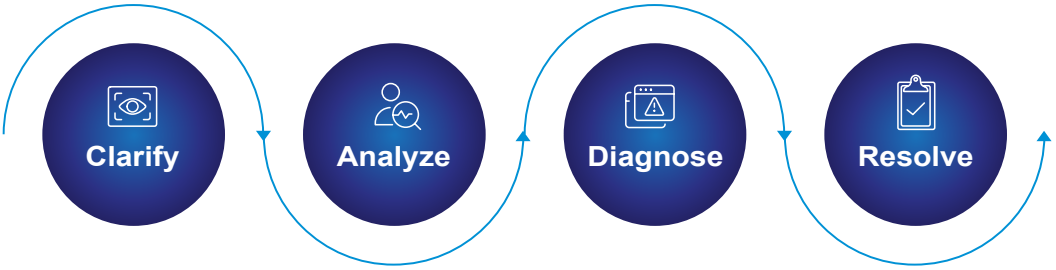
Clarify: The AI agent immediately performs automated event correlation across the flood of alerts, distinguishing between the actual cause (a batch job conflict) and all the symptom events (latency spikes, timeout errors, queue backups). Instead of 20 confusing alerts, the operator sees one clear picture: "Database conflict detected; likely root cause identified."

Analyze: The AI agent queries security logs, network telemetry, application traces, and change management databases, while simultaneously searching through years of historical incident data in a vector database. In seconds, it finds 847 similar patterns and flags an 89 percent match to two past incidents, based on how the symptoms, timing, and system behaviors line up. It surfaces the smoking gun: change ticket CHG-45209 modified a batch job schedule that's now running during peak transaction times.

Diagnose: The AI doesn't just find correlations; it pinpoints the root cause by cross-referencing the batch job timing with transaction volume patterns and shows exactly when things went wrong. It presents the diagnosis: "Batch job 'user_analytics_aggregation_v2' conflicting with real time payment processing same pattern as incidents #3421 and #11203."

Resolve: Here's where the human comes back in. The AI agent offers three resolution options based on what has actually worked before, ranked by success rate and risk. The operator reviews them, considers the context (it's 2:52 AM, outside maintenance windows), and makes the call: suspend the batch job and set up automatic rollbacks if things go sideways. The AI executes the approved actions while maintaining continuous monitoring.

Total time from alert to resolution: 14 minutes. Without agentic AI, the same process would have taken over four hours.



Agentic AI Reduces Time to Resolution

The agentic AI handled the heavy lifting at each stage—including automated correlation, intelligent analysis, precise diagnosis, and guided resolution—but the human stayed in control where it mattered most: approving the fix. That drove a meaningful reduction in MTTR. Not only that, but every incident handled this way enriches the historical database, making future responses even sharper.

Every operations center is measured through a range of key performance indicators (KPIs). Traditional metrics typically focus on service availability—with many organizations striving for Five Nines (99.999%) uptime, as well as incident volume, including the number and severity of major and minor incidents. Other core measures include MTTR, recovery time objective (RTO), and recovery point objective (RPO).

While these metrics are important, they remain largely reactive. They assess how well a team responds to disruptions rather than how effectively it prevents them. As AI becomes embedded in operations, organizations must begin to incorporate proactive metrics. For example:

- How many incidents were detected or mitigated by AI before they escalated?
- How quickly did agentic AI systems identify early indicators of failure or compromise?
- What percentage of total incidents are being managed autonomously by AI agents?

Measuring the impact of agentic AI separately helps organizations understand the true transformational effect of adoption. Success should be reflected in measurable improvements such as:

- A reduction in the total number of incidents, particularly major ones
- Faster time to identify and restore from incidents
- Greater operational resilience driven by predictive monitoring and automated response

Generative and agentic AI bring the capabilities to find the needle in the haystack—uncovering root causes quickly and enabling earlier intervention.

The evolution of operations must progress hand in hand with the adoption of AI. Too often, organizations focus on deploying AI models while neglecting to modernize their operations centers. A team relying on manual monitoring and traditional workflows cannot keep pace with an enterprise moving toward intelligent, AI-augmented operations.

Moreover, as threat actors increasingly use AI to automate and amplify cyberattacks, security operations centers must evolve in parallel, leveraging AI to maintain parity and defend at machine speed. This transformation is not optional; it is essential for maintaining competitiveness, resilience, and trust in the era of AI-driven enterprise operations.

In this new era, the ability to effectively manage organizational data is what will ultimately empower you to get the most out of AI. Leveraging enterprise AI to manage, govern, and continually optimize data operations is essential. As operations centers evolve into nerve centers of innovation and resilience, data stewardship and strategy must remain at the core of every executive agenda. Enterprises that treat data not only as a resource, but as a strategic asset—and apply AI to maintain its health and availability—will be best positioned to unlock the full transformative potential of AI at scale.

A major manufacturer is unlocking the power of data for insights into its processes to cut costs and reduce its reliance on manual work in the following case study.

Case Study

North Star BlueScope Steel

North Star BlueScope Steel

A subsidiary of Australia-based BlueScope, North Star BlueScope Steel produces and supplies hot-rolled steel bands for coil processors, cold-rolled strip producers, pipe and tubers, original equipment manufacturers and steel service centers. Founded in 1997, the company is the largest scrap steel recycler in Ohio, recycling nearly 1.5 million tons of scrap steel every year.

North Star BlueScope Steel needed a more efficient tool to help it more accurately understand its costing data and workflow, so the company could use it to engage with customers, conduct market-based analysis, and build purchasing breakdowns. The technology would have to eliminate the manually intensive process and collect data automatically from a variety of sources—including databases and the company's electric arc furnaces (EAF)—allowing it to reallocate staff and save on resources, all while better meeting customers' needs.

The company opted to use intelligent data and analytics to automatically access, blend, explore and analyze data. The solution allows North Star BlueScope Steel to apply algorithms to extracted information to generate a final monthly report, reducing their reliance on manual work. Using data and analytics, the company can compare month-to-month data to analyze how events such as plant delays and bottlenecking might affect profitability. Embracing the IoT, the company hopes to integrate analytics into data points coming directly from its instruments, to analyze electricity consumption, weather patterns, material usage and steel prices for a better idea of future needs and sales potential.

The Fast Five Download

1. **Drive the Shift to Autonomous Operations.**
   Lead your organization to move beyond reactive monitoring by investing in AI-powered, self-healing systems that proactively prevent incidents and optimize performance.

2. **Champion Human-AI Collaboration.**
   Ensure your teams are equipped to work alongside AI—establish governance frameworks, empower human oversight, and create continuous feedback loops to maximize both safety and innovation.

3. **Elevate Operations Centers to Innovation Hubs.**
   Transform your operations center from a traditional support function into a strategic engine for enterprise innovation and talent development, making it a focal point for AI adoption and experimentation.

4. **Make AI Adoption a Board-Level Priority.**
   Treat the integration of AI into operations as a critical competitive differentiator. Allocate executive attention and resources to accelerate adoption, strengthen security, and build organizational trust.

5. **Redefine Success Metrics for the AI Era.**
   Move beyond traditional, reactive KPIs. Implement new metrics that track AI's impact—such as incidents prevented, response speed, and autonomous actions—to accurately measure value and drive continuous improvement.

Endnotes

[1] Foundry Research sponsored by OpenText, "MarketPulse Survey: The Role of GenAI in Modernizing Content Management," May 2025.

[2] Philip Miller, "Unlocking Unstructured Data: Fueling AI with Insights," *Dataversity*, June 3, 2025, https://www.dataversity.net/articles/unlocking-unstructured-data-fueling-ai-with-insights/.

[3] Ibid.

[4] "More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI Applications by 2026," *Gartner Press Release*, October 11, 2023, www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026.

[5] "AI Governance Software Spend Will See 30% CAGR From 2024 to 2030," *Forrester Blog*, November 13, 2024, www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/.

[6] McKinsey & Company, "The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value," *QuantumBlack by McKinsey*, May 30, 2024, www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024.

[7] Ibid.

[8] Accenture, "New Accenture Research Finds that Companies with AI-Led Processes Outperform Peers," *Accenture*, October 10, 2024, https://newsroom.accenture.com/news/2024/new-accenture-research-finds-that-companies-with-ai-led-processes-outperform-peers.

[9] "What is Artificial Intelligence (AI)?" *International Organization for Standardization*, January 31, 2024, https://www.iso.org/artificial-intelligence/what-is-ai?.

[10] Melissa Russell, "How can I learn artificial intelligence?" *Harvard*, April 8, 2025, https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence.

[11] Sofia Samoili, Montserrat Lopez Cobo, Blagoj Delipetrev, Fernando Martinez-Plumed, Emilia Gomez Gutierrez, and Giuditta De Prato, "AI Watch, Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy for the AI Landscape," *Publications Office of the European Union,* 2021.

[12] Ibid.

[13] Tim Mucci and Cole Stryker, "What is artificial superintelligence?" IBM, July 22, 2025, https://www.ibm.com/think/topics/artificial-superintelligence.

[14] Arend Hintze, "Understanding the four types of AI, from reactive robots to self-aware beings," *The Conversation,* November 13, 2016, https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616

[15] A. M. Turing, "Computing Machinery and Intelligence," *Mind*, Volume LIX, Issue 236, October 1950, https://doi.org/10.1093/mind/lix.236.433.

[16] J. McCarthy, M. L. Minsky, N. Rochester, & C.E. Shannon, "A proposal for the Dartmouth summer research project on artificial intelligence," Dartmouth College, 1955, https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904.

[17] Ben Lutkevich, "What is AI Winter? Definition, History and Timeline," *Tech Target*, August 26, 2024, https://www.techtarget.com/searchenterpriseai/definition/AI-winter.

[18] D. Crevier, *AI: The tumultuous history of the search for artificial intelligence,* Basic Books, 1993.

[19] Ibid.

[20] S.J. Russell & P. Norvig, *Artificial intelligence: A modern approach,* 4th ed., Pearson, 2021.

[21] Yann LeCun, Yoshua Bengio, and Geoffrey Hinton, "Deep learning," *Nature,* 521(7553), 436–444, 2015, https://doi.org/10.1038/nature14539.

[22] Melissa Russell, "How can I learn artificial intelligence?" *Harvard*, April 8, 2025, https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence.

[23] "Gartner Survey Reveals GenAI Attacks Are on the Rise," *Gartner Inc.*, September 22, 2025, https://www.gartner.com/en/newsroom/press-releases/2025-09-22-gartner-survey-reveals-generative-artificial-intelligence-attacks-are-on-the-rise.

[24] Akshay Joshi, Giulia Moschetta, and Ellie Winslow, "Global Cybersecurity Outlook 2025 Insight Report," World Economic Forum in Collaboration with Accenture, January 2025, https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

[25] Shuli Jiang, Swanand Ravindra Kadhe, Yi Zhou, Ling Cai, and Nathalie Baracaldo, "Forcing Generative Models to Degenerate Ones: The Power of Data Poisoning Attacks," Cornell University, arXiv:2312.04748, December 7, 2023, https://arxiv.org/abs/2312.04748.

[26] B. Biggio, B. Nelson, and P. Laskov, "Poisoning Attacks Against Support Vector Machines," *Proceedings of the 29th International Conference on Machine Learning (ICML)*, 2012.

[27] Tianyu Gu, Brendan Dolan-Gavitt, and Siddharth Garg, "BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain," Cornel University, arXiv:1708.06733, March 11, 2019, https://arxiv.org/abs/1708.06733.

[28] Ian J. Goodfellow, Jonathon Shlens, and Christian Szegedy, "Explaining and Harnessing Adversarial Examples," Cornell University, arXiv:1412.6572, March 20, 2015, https://arxiv.org/abs/1412.6572.

[29] Wencheng Yang, Song Wang, Di Wu et al, "Deep Learning Model Inversion Attacks and Defenses: A Comprehensive Survey," Cornell University, arXiv:2501.18934, April 30, 2025, https://arxiv.org/abs/2501.18934.

[30] Ninareh Mehrabi, Fred Morstatter, Nripsuta Saxena, Kristina Lerman, and Aram Galstyan, "A Survey on Bias and Fairness in Machine Learning," Cornell University, arXiv:1908.09635, January 25, 2022, https://arxiv.org/abs/1908.09635.

[31] ISO/IEC 27001:2022, "Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements," International Organization for Standardization.

[32] Sandeep Kumar Jangam, "Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices," *International Journal of AI, BigData, Computational and Management Studies,* 4(3), 82–91, 2023, https://ijaibdcms.org/index.php/ijaibdcms/article/view/242/.

[33] Qiang Yang, Yang Liu, Tianjian Chen, and Yongxin Tong, "Federated Machine Learning: Concept and Applications," *ACM Digital Library*, January 28, 2019, https://dl.acm.org/doi/10.1145/3298981.

[34] European Parliament & Council, "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data – Article 17 (Right to erasure), 2016, https://eur-lex.europa.eu/eli/reg/2016/679/oj.

[35] Scott Rose, Oliver Borchert, Stu Mitchell, and Sean Connelly, "Zero Trust Architecture," *NIST Special Publication 800-207*, August 2020, https://doi.org/10.6028/NIST.SP.800-207.

[36] Alexey Kurakin, Ian Goodfellow, and Samy Bengio, "Adversarial Machine Learning at Scale," Cornell University, arXiv:1611.01236, February 11, 2017, https://arxiv.org/abs/1611.01236.

[37] Yusuke Uchida, Yuki Nagai, Shigeyuki Sakazawa, and Shin'ichi Satoh, "Embedding Watermarks into Deep Neural Networks," Cornell University, arXiv:1701.04082, April 20, 2017, https://arxiv.org/abs/1701.04082.

[38] Forrester. "AI Governance Software Spend Will See 30 % CAGR From 2024 to 2030." *Forrester Research*, November 13, 2024, https://www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/.

[39] "Information Governance Reference Model," EDRM, http://www.edrm.net/projects/igrm.

[40] "Key Regulatory and Industry Initiatives," *Capgemini*, https://web.archive.org/web/20141105171058/https://www.worldpaymentsreport.com/kriis#Heat-Map-of-KRIIs-Global-and-Regional.

[41] Gartner, Inc., "Gartner Poll Finds 55% of Organizations Have an AI Board," Press Release, June 26, 2024, https://www.gartner.com/en/newsroom/press-releases/2024-06-26-gartner-poll-finds-55-percent-of-organizations-have-an-ai-board

[42] Ibid.

[43] Alex Edquist, Liz Grennan, Sian Griffiths, and Kayvaun Rowshankish, "Data ethics: What it means and what it takes," *McKinsey & Company*, September 23, 2022, https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes.

[44] James Moor, "What is Computer Ethics?" *Metaphilosophy*, 16(4), 266–275, 1985, https://doi.org/10.1111/j.1467-9973.1985.tb00173.x.

[45] Unesco, "Recommendation on the Ethics of Artificial Intelligence," UNESCO.org, 2022, https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence.

[46] Ibid.

[47] Ibid.

[48] OECD, "Recommendation of the Council on Artificial Intelligence," OECD/LEGAL/0449, 2019.

[49] European Commission, "Regulation (EU) 2024/1689 on Artificial Intelligence," 2024.

[50] NIST, "Artificial Intelligence Risk Management Framework (AI RMF 1.0)," *NIST Special Publication AI 100-1*, 2023.

[51] Dario Maisto, "From Digital Sovereignty Platforms To Sovereign Cloud Platforms: Three Reasons For A Title Change," *Forrester Blogs*, August 11, 2025, www.forrester.com/blogs/from-digital-sovereignty-platforms-to-sovereign-cloud-platforms-three-reasons-for-a-title-change.

[52] McKinsey & Company, "Future-Proofing the IT Function Amid Global Trends and Disruptions," *McKinsey Digital*, June 11, 2024, www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/future-proofing-the-it-function-amid-global-trends-and-disruptions.

[53] Sébastien Bubeck, Varun Chandrasekaran, Ronen Eldan et al, "Sparks of artificial general intelligence: Early experiments with GPT-4," Cornell University, April 13, 2023, https://arxiv.org/abs/2303.12712.

[54] Aditya Challapally, Chris Pease, Ramesh Raskar, et al., "The GenAI Divide: State of AI in Business 2025," *MIT NANDA*, July 2025, https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf.

[55] Mark J. Barrenechea, Tom Jenkins, and David Fraser, *The Anticipant Organization*, OpenText Corporation, 2022.

[56] Ibid.

[57] Ibomoiye Domor Mienye, Nobert Jere, George Obaido, Oyindamola Omolara Ogunruku, Ebenezer Esenogho and Cameron Modisane, "Large language models: an overview of foundational architectures, recent trends, and a new taxonomy," *Discover Applied Sciences*, 7, 1027, September 2, 2025, https://link.springer.com/article/10.1007/s42452-025-07668-w.

[58] Ruei-Shan Lu ,Ching-Chang Lin , and Hsiu-Yuan Tsao, "Empowering Large Language Models to Leverage Domain-Specific Knowledge in E-Learning," *Applied Sciences*, 14(12), 5264, June 18, 2024, https://doi.org/10.3390/app14125264.

[59] Qizheng Zhang, Changran Hu, Shubhangi Upasani et al. "Agentic Context Engineering: Evolving Contexts for Self-Improving Language Models," arXiv preprint arXiv:2510.04618, 2025, https://www.arxiv.org/pdf/2510.04618.

[60] Lingrui Mei, Jiayu Yao, Yuyao Ge et al, "A survey of context engineering for large language models," Cornell University, arXiv:2507.13334, July 21, 2025, https://arxiv.org/abs/2507.13334.

[61] A. Feder Cooper, Christopher A. Choquette-Choo, Miranda Bogen et al. "Machine Unlearning Doesn't Do What You Think: Lessons for Generative AI Policy, Research, and Practice," SSRN, February 6, 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5060253.

[62] K. Boyd, "Microsoft 365 Copilot for executives: Sharing Our Customer Zero Deployment and adoption journey at Microsoft," *Microsoft Inside Track Blog*, December 5, 2024, https://www.microsoft.com/insidetrack/blog/copilot-for-microsoft-365-for-executives-sharing-our-internal-deployment-and-adoption-journey-at-microsoft/.

[63] Product owner. Scaled Agile Framework, February 25, 2025, https://framework.scaledagile.com/product-owner.

[64] Alexander Sukharevsky, Alexis Krivkovich, Arne Gast, et al, "The agentic organization: Contours of the next paradigm for the AI era," *McKinsey & Company,* September 26, 2025, https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-agentic-organization-contours-of-the-next-paradigm-for-the-ai-era.

[65] V.L. Sunkara, "KPIs for AI agents and Generative AI: A rigorous framework for evaluation and Accountability," *International Journal of Scientific Research and Modern Technology*, 22–29, 2024, https://doi.org/10.38124/ijsrmt.v3i4.572.

[66] Jared Kaplan, Sam McCandlish, Tom Henighan et al, "Scaling Laws for Neural Language Models," Cornell University, arXiv:2001.08361, January 23, 2020, https://arxiv.org/abs/2001.08361.

[67] Gary Marcus, "Deep learning is hitting a wall,"*Communications of the ACM*, 65(8), 36–43, 2022, https://nautil.us/deep-learning-is-hitting-a-wall-238440/.

[68] Annette Zimmermann and Danielle Casey, "Emerging Tech Impact Radar: Generative AI," *Gartner,* February 14, 2025.

Glossary

Agentic Artificial Intelligence: Agentic AI refers to the framework of artificial intelligence systems designed to function as autonomous agents. Unlike models that simply respond to a prompt, an agent can perceive its environment, create a multi-step plan, make independent decisions, and use tools to actively work toward a specific goal.

In an enterprise context, these agents are a powerful engine for productivity with data serving as fuel. They can be given access to private enterprise datasets and internal tools, allowing them to automate complex workflows that previously required human judgment. Agentic AI is powered by a 'digital brain'—a single, competent model that can process decades of human responses.

AI Agent: A specific software system designed for a defined task that can autonomously perceive its environment, plan and reason about tasks, and take actions to achieve specific goals. It operates with a degree of independence (but usually within human-set constraints), learns or adapts over time, uses tools or external data sources when needed, and supports decision-making with minimal direct supervision. AI agents are the "building blocks" of the framework of "agentic AI".

AI-Driven Analytics: The application of artificial intelligence and machine learning to automate data collection, preparation, and analysis. By uncovering patterns and generating insights in real or near real time, it helps organizations predict outcomes, identify trends, and make faster, more informed decisions.

AI-Ready Platform/Stack: A technology environment built to support the development, deployment, and scaling of artificial intelligence applications. It combines scalable infrastructure, strong data governance, and modular tools—such as APIs, model management, and integration pipelines—to make AI projects faster, more reliable, and easier to move from experimentation to production.

Air Gap: A network security measure implemented on one or more computers. It aims to ensure that a secure computer network is physically set apart from any unsecured networks within range. Unsecured networks can include the internet or other local area networks. Often, this method is used in high-security environments, like the military. This term is also sometimes referred to as an air wall, or as air gapping.

Analytics: The systematic process of collecting, processing, and interpreting data in order to identify patterns, trends, and insights. In computing, analytics is used to support decision-making, optimize performance, and predict future outcomes through techniques such as statistical analysis, data visualization, and machine learning.

Anticipant: An anticipant refers to an expectant individual, who is able to foresee wide-ranging possible events and outcomes. These individuals minimize risks associated with potential events and outcomes. An anticipant will make necessary changes in advance or create protocols which can be implemented when needed. They're prepared for almost anything.

Application Programming Interface (API): A set of software rules and protocols that enable two applications to communicate with each other. APIs provide a structured way for AI systems to connect programmatically with external models, datasets, or other software components.

Artificial General Intelligence (AGI): AGI represents advanced intelligence capable of redefining not just sectors but entire societies. It refers to AI that possesses the capacity to understand, learn, and apply knowledge across a wide range of tasks, much like a human being. Despite its vast capabilities, AGI is ultimately still shaped by the quality and scale of its training data.

Artificial Intelligence (AI): Technology that empowers machines or software to perform tasks normally requiring human intelligence—things like learning, reasoning, perception, problem-solving, decision-making, natural language understanding, and recognizing patterns. AI systems mimic or simulate cognitive functions of the human mind by using algorithms, large datasets, and computational power. Because AI encompasses a wide variety of methods (from machine learning to neural networks and deep learning), its applications can range from analyzing speech and text to making predictions, translating languages, generating creative content, or optimizing complex processes.

Artificial Narrow Intelligence (ANI): Refers to AI systems designed and trained to perform specific tasks or solve defined problems—often at or above human capability—but without general reasoning ability or understanding beyond their programmed domain.

Artificial Superintelligence (ASI): A hypothetical form of AI that surpasses human intelligence across all domains—including reasoning, creativity, social understanding, and strategic decision-making—and would be capable of outperforming the best human minds in every field.

Audit: A systematic examination and evaluation of systems, processes, or data in computing to ensure accuracy, security, compliance, and proper operation. Audits may review logs, access controls, configurations, and policies to detect irregularities, confirm adherence to standards, and identify areas for improvement.

Audit Trails: Chronological records that track system activities, including user actions, data changes, and access events. They provide transparency, support regulatory compliance, and help with security investigations by showing who did what, when, and how within a system.

Auditable Access: The capability of a system to log and review who accessed resources, when, and how. It provides accountability and compliance by ensuring access activity can be verified and traced if needed.

Automation: The use of technology to perform tasks with minimal or no human intervention. In computing, automation streamlines repetitive or rule-based processes—such as software deployment, system monitoring, or data processing—to improve efficiency, consistency, and reliability.

Big Data: Extremely large and complex data sets that require advanced tools and analytics to process and extract insights.

Bots: Software programs designed to automate tasks, often by simulating human activity. In computing, bots can perform a wide range of functions, from helpful activities such as customer support chatbots, search engine indexing, and workflow automation, to malicious uses like spamming, credential stuffing, or spreading malware. Bots typically operate at high speed and scale, making them powerful tools for both legitimate and harmful purposes.

Business Intelligence (BI): The technologies, tools, and practices that collect, integrate, and analyze business data to support decision-making. BI platforms transform raw data into dashboards, reports, and visualizations, helping organizations identify trends, measure performance, and make more informed strategic choices.

Business Process Management (BPM): Refers to aligning processes with an organization's strategic objectives, designing and implementing process-centric tools or architectures, and determining measurement systems for effective process management.

California Consumer Privacy Act (CCPA): A data privacy law enacted in California in 2020 that gives residents greater control over their personal information. CCPA requires businesses to disclose what data they collect, how it is used, and with whom it is shared, while granting consumers rights to access, delete, and opt out of the sale of their data.

Change Management: A broader discipline that focuses on the human and organizational side of change, ensuring that new systems, processes, or technologies are adopted successfully. While configuration management deals with technical consistency, change management addresses communication, training, and stakeholder alignment to minimize resistance and maximize value from change initiatives.

Cloud/The Cloud: A model of computing that delivers on-demand access to shared resources—such as servers, storage, databases, networking, software, and analytics—over the internet. The cloud allows users and organizations to scale resources quickly, pay only for what they use, and access services without maintaining physical hardware or infrastructure on-site.

CloudOps: Short for Cloud Operations, CloudOps focuses on managing and optimizing applications and infrastructure running in cloud environments. It extends DevOps principles into the cloud, emphasizing scalability, performance monitoring, security, and cost efficiency across dynamic, distributed systems.

Compliance (in technology): The practice of ensuring that systems, processes, and data management meet established laws, regulations, standards, and internal policies. In tech, compliance often covers areas like data privacy (e.g., GDPR, CCPA), cybersecurity, accessibility, and industry-specific rules, helping organizations reduce risk, maintain trust, and avoid legal or financial penalties. (See also: Data Security; Cybersecurity; Data Privacy).

Configuration Management: The process of systematically handling changes to a system to maintain its integrity, consistency, and traceability throughout its lifecycle.

Content Lifecycle Management (CLM): The combination of document management, records management, workflow, archiving, and imaging into a fully integrated solution to effectively manage the lifecycle of content, from creation through to archiving and eventual deletion.

Content Management System (CMS): A software platform that allows users to create, edit, organize, and publish digital content—usually for websites—without needing extensive technical skills. CMS platforms like WordPress, Drupal, or Adobe Experience Manager provide templates, workflows, and integrations that make managing online content more efficient and collaborative. A CMS manages website content for publishing, while an enterprise content management (ECM) system manages all organizational information across its lifecycle for governance, compliance, and business processes.

Contextual Intelligence: The ability of systems, organizations, or individuals to interpret data, events, or behaviors within their surrounding context and act appropriately. In technology, it refers to AI's use of real-time signals—such as location, behavior, preferences, or timing—to deliver more relevant insights, recommendations, and actions. In media and marketing, contextual intelligence powers personalization and customer journey orchestration by ensuring every interaction is timely, meaningful, and aligned with customer needs.

Customer Relationship Management (CRM): A strategy and set of software tools that help businesses manage interactions with current and potential customers. CRM systems centralize customer data, track sales and communications, and support marketing, service, and relationship-building to improve retention and drive growth.

Cybersecurity: The practice of protecting systems, networks, software, and data from digital attacks, unauthorized access, or damage. It encompasses technologies, processes, and policies that safeguard confidentiality, integrity, and availability, helping organizations defend against threats like malware, phishing, ransomware, and insider risks. (See also: Data Security; Compliance; Data Privacy).

Data Driven: The use of data analytics and insights to inform business decisions and strategies.

Data Lake: A centralized storage repository that holds vast amounts of raw data in the data's native format, whether structured, semi-structured, or unstructured. Unlike traditional databases or data warehouses, data lakes allow organizations to store data first and organize or analyze it later, supporting big data analytics, machine learning, and real-time insights.

Data Mapping: The process of matching data fields from one system, format, or database to another to enable integration, migration, or analysis. Effective data mapping ensures consistency and accuracy, making it possible to consolidate information across platforms, support compliance, and prepare data for analytics or machine learning.

Data Privacy: The discipline of managing and protecting personal information to ensure it is collected, stored, and used in ways that respect individuals' rights and expectations. Data privacy focuses on transparency, consent, and legal compliance, ensuring that organizations handle sensitive data responsibly while maintaining user trust. (See also: Data Security; Cybersecurity; Compliance).

Data Protection Impact Assessment (DPIA): A process required under regulations like GDPR to identify and minimize risks to personal data before starting a project that involves its collection or processing. A DPIA evaluates how data will be used, assesses potential impacts on privacy, and documents safeguards to ensure compliance and protect individuals' rights.

Data Residency: The physical or geographic location where an organization's data is stored and processed. Often driven by legal, regulatory, or business requirements, data residency ensures that information remains within specific jurisdictions, which can impact compliance, security, and performance.

Data Security: The set of practices, technologies, and policies used to protect digital information from unauthorized access, corruption, or loss. It encompasses measures such as encryption, access controls, backups, and monitoring to safeguard the confidentiality, integrity, and availability of data across its lifecycle. (See also: Cybersecurity; Compliance; Data Privacy).

Data Silos: Isolated collections of data that are controlled by one department, system, or platform and are not easily accessible to others within an organization. Data silos limit collaboration, reduce visibility, and can create inefficiencies or inconsistencies, making it harder to gain a unified view of information across the business.

Data Sovereignty: The principle that digital data is subject to the laws and governance structures of the country or region where it is collected, stored, or processed. It ensures that data handling complies with local regulations—such as GDPR in the EU or data localization laws elsewhere—affecting how organizations manage storage, security, and cross-border transfers.

Data Warehouse: A structured storage system optimized for querying and reporting on curated data. Unlike data lakes, which hold raw inputs, data warehouses store cleaned, organized, and integrated data—typically from multiple sources—making it easier for businesses to run analytics, generate dashboards, and support decision-making.

Deep Learning: A specialized branch of machine learning that relies on deep neural networks—multi-layered structures of interconnected "neurons" whose weights and parameters can be adjusted through training. This approach excels at extracting patterns and insights from unstructured data such as images, text, audio, and video, making it the backbone of many modern AI applications like image recognition, language translation, and speech processing.

DevOps: A set of practices that combines software development (Dev) and IT operations (Ops) to shorten development cycles, improve collaboration, and deliver updates more reliably. By automating testing, integration, and deployment, DevOps helps teams release software faster while maintaining quality.

Digital Governance: The framework of policies, roles, processes, and standards that guide how an organization manages its digital assets, technologies, and data. It ensures accountability, compliance, security, and alignment with business goals while balancing innovation with risk management in digital operations.

Digital Workforce: A collection of automated software systems, known as "digital workers" (such as AI agents, bots, and virtual assistants), that perform tasks traditionally done by humans.

E-commerce: The buying and selling of goods or services over the internet, including activities such as online shopping, electronic payments, digital marketplaces, and mobile commerce. E-commerce enables businesses to reach customers directly through websites, apps, and platforms, transforming how products are marketed, purchased, and delivered.

Edge Computing: A distributed computing architecture in which processing power, storage, and data analysis are located nearer to where data is generated—on devices, gateways, or local "edge" servers—rather than centralized in remote cloud data centers. This approach improves response time, reduces latency and bandwidth usage, and enables real-time or near-real-time applications, particularly in IoT, autonomous systems, and environments where speed or local decision-making matters.

Electronic Data Interchange (EDI): A standardized method for exchanging business documents—such as purchase orders, invoices, and shipping notices—electronically between organizations, eliminating manual data entry and improving speed, accuracy, and consistency in transactions.

Encryption: The process of converting data into a coded format using algorithms and cryptographic keys to prevent unauthorized access. In computing, encryption ensures that only authorized parties with the correct key can decrypt and read the information, protecting sensitive data during storage or transmission.

Enterprise AI (EAI): The disciplined application of artificial intelligence within an organization to solve real business problems, improve decision-making, and automate work securely and at scale. It is not a separate category of intelligence, but the governed deployment of existing AI capabilities—including machine learning, natural language processing, computer vision, automation, and generative AI—within a structured data and compliance environment. Enterprise AI depends on trusted information, sovereign data controls, lifecycle management (MLOps and LLMOps), hybrid or sovereign cloud infrastructure, and secure orchestration layers to ensure AI operates responsibly, transparently, and reliably across the business.

Enterprise Content Management (ECM): An ECM is a platform that stores, manages, and delivers enterprise-level content. This includes documents, images, videos, and other forms of content that are important to an organization. An ECM platform should seamlessly integrate with crucial enterprise applications and systems (such as enterprise resource planning, customer relationship management, human capital management, and supply chain management solutions) to accelerate business processes and leverage the data they generate. ECM includes cloud content management that can be rapidly deployed to allow organizations to store, manage, and collaborate with digital content in the cloud.

Enterprise Information Management (EIM): Enterprise Information Management solutions manage the creation, capture, use, and eventual lifecycle of structured and unstructured information. They are designed to help organizations extract value from their information, secure that information, and meet the growing list of compliance requirements.

Enterprise Resource Planning (ERP): An integrated software system that manages core business processes—such as finance, supply chain, manufacturing, human resources, and customer relations—within a unified platform. ERP centralizes data and workflows across departments, improving efficiency, collaboration, and decision-making while providing a single source of truth for the organization.

Extraterritorial Access: The ability of governments, organizations, or entities to reach and demand access to data stored outside their own national jurisdiction. In technology and data governance, extraterritorial access raises concerns about sovereignty, privacy, and compliance, as it allows laws such as the U.S. CLOUD Act or similar frameworks to compel disclosure of data stored abroad.

FinOps: Short for Cloud Financial Operations, FinOps is a framework for managing cloud costs through collaboration between engineering, finance, and business teams. It ensures that organizations gain financial accountability, optimize spending, and make informed trade-offs between performance and cost in cloud environments.

Foundational Models: Large deep learning models trained on massive amounts of unstructured, unlabeled data, designed to perform a wide variety of tasks either directly or by being fine-tuned for specific applications. Foundation models can also be used for generative or nongenerative purposes (for example, classifying user sentiment as negative or positive based on call transcripts).

General Data Protection Regulation (GDPR): A comprehensive data privacy and protection law enacted by the European Union in 2018. GDPR governs how organizations collect, process, store, and share personal data, emphasizing transparency, user consent, and individual rights, with significant penalties for non-compliance.

Generative AI (GenAI): AI systems that create new, original content using machine learning models. Models such as ChatGPT, Claude, Gemini, and DeepSeek are trained on public data sources like websites, news, Reddit, and Wikipedia. While GenAI models are useful for generating general insights, they are limited to general-purpose tasks. This is because they lack access to the private, real-time, and enterprise-centric data required for specific business use cases.

Geopolitics: The study of how geographical factors—such as location, resources, physical terrain, population, and economic or demographic trends—influence political power, foreign policy, and decision-making among states or other political actors. It examines how control over territory, strategic regions, and geographic features shapes relationships, conflicts, and cooperation on a global stage.

Graphical User Interface (GUI): A visual interface that allows users to interact with software or devices through graphical elements such as windows, icons, buttons, and menus, rather than text-based commands. GUIs make technology more intuitive and accessible by enabling point-and-click navigation, drag-and-drop actions, and visual feedback.

Human-in-the-Loop (HITL): An approach to artificial intelligence and automation where humans remain actively involved in the system's decision-making or training process. HITL is used to provide oversight, improve accuracy, correct errors, and handle edge cases, ensuring that automated systems align with human judgment, ethics, and real-world context.

Hyperscaler: A large cloud service provider—such as Amazon Web Services (AWS), Microsoft Azure, or Google Cloud—that delivers massive-scale computing, storage, and networking services across global data centers. Hyperscalers are known for their ability to scale resources up or down instantly, support multi-tenant workloads, and provide the backbone for cloud-native, AI, and data-intensive applications.

Identity and Access Management (IAM): A security framework that ensures the right individuals have the appropriate access to the right resources at the right time. It manages digital identities, authentication, and permissions across systems and applications to protect sensitive data and maintain compliance.

Identity Management (IdM): A core component of Identity and Access Management (IAM) focused on creating, maintaining, and retiring user identities and their attributes. While IAM oversees both identity and access controls, IdM specifically handles user identity lifecycle tasks such as provisioning accounts, updating user roles, and ensuring identity data is accurate and secure.

Infrastructure-as-a-Service (IaaS): A cloud computing model that delivers virtualized computing resources—such as servers, storage, and networking—over the internet on a pay-as-you-go basis. IaaS allows organizations to scale infrastructure quickly without investing in physical hardware, supporting flexibility, cost efficiency, and rapid deployment.

Intelligence Layer: The analytical and decision-making tier within a technology stack that transforms raw data into actionable insights. Often powered by AI, machine learning, or advanced analytics, the intelligence layer sits above data storage and processing systems, enabling personalization, predictions, and automation that drive smarter business outcomes.

Internet of Things (IoT): Refers to a network of physical devices—such as sensors, appliances, vehicles, and machinery—that are connected to the internet and can collect, share, and act on data, enabling automation, monitoring, and smarter decision-making in real time.

Interoperability: The capacity of different systems, applications, or platforms to exchange and use data seamlessly. By relying on common standards and protocols, interoperability reduces technical barriers and allows diverse systems to work together efficiently.

Key Performance Indicators (KPIs): Quantifiable metrics used to evaluate how effectively an organization, team, or process is achieving its objectives. KPIs track progress toward strategic goals, guide decision-making, and can range from financial measures like revenue growth to operational ones like customer retention or system uptime.

Kubernetes: An open-source platform for automating the deployment, scaling, and management of containerized applications. Originally developed by Google, Kubernetes orchestrates clusters of containers—handling scheduling, load balancing, and failover—so applications run reliably and efficiently across cloud, on-premises, or hybrid environments.

Large Language Models (LLMs): A type of foundation model built with deep learning that's pre-trained on enormous text corpora using self-supervised methods. These models process inputs in the form of "tokens" (pieces of words or characters), learn the statistical relationships among them, and use those relationships to understand, generate, summarize, or transform human-language text. Because of their size and architecture (often transformer based), LLMs can perform many language tasks "out of the box," but can also be fine-tuned or guided via prompt-engineering for specific applications. Examples of LLMs include GPT-4 and Meta's Llama models.

Large Language Model Operations (LLMOps): A specialized extension of MLOps focused on the unique lifecycle requirements of large language models. LLMOps manages how foundation models are selected, fine-tuned, deployed, monitored, and governed, including prompt-management, safety controls, access governance, hallucination mitigation, and cost efficiency. It ensures LLMs operate securely with enterprise data, comply with policy and regulatory requirements, and deliver reliable performance. In the enterprise, LLMOps is essential for scaling generative AI responsibly while protecting data integrity and trust.

Legacy Platforms: Outdated or older technology systems, software, or infrastructure that remain in use despite being superseded by newer alternatives. Legacy platforms may still support critical business operations but often present challenges such as limited compatibility, higher maintenance costs, security vulnerabilities, and difficulty integrating with modern solutions.

Machine Learning (ML): A field of artificial intelligence that focuses on developing algorithms and models that enable systems to learn from data and improve their performance over time without being explicitly programmed. ML is used to identify patterns, make predictions, and support decision-making in applications such as recommendation engines, fraud detection, image recognition, and natural language processing.

Machine Learning Operations (MLOps): A disciplined framework for managing the end-to-end lifecycle of machine learning models in production. MLOps brings DevOps principles to AI, ensuring models are developed, deployed, monitored, and governed reliably at scale. It encompasses data pipelines, model versioning, performance monitoring, bias and drift detection, security controls, and auditability. The goal of MLOps is to operationalize AI responsibly—delivering consistent outcomes, reducing risk, and enabling continuous improvement across enterprise systems.

Managed Services: Outsourced IT operations and responsibilities provided by a third-party service provider. In computing, managed services typically include proactive monitoring, maintenance, security, updates, and support for infrastructure, applications, or cloud environments. This approach allows organizations to reduce the burden on internal teams, ensure system reliability, and access specialized expertise while focusing on core business activities.

Metadata: Any set of terms, words, symbols, and numbers embedded within a document to allow record-management functions such as classification, search, historical tracking (date created, modified, retrieved), user identification (authors and editors of each refinement), and a variety of other items related to its characteristics.

Microservices: An architectural approach to software development in which applications are structured as a collection of small, independent services that communicate through APIs. Each microservice focuses on a specific business function, can be developed and deployed independently, and scales separately. This design improves flexibility, resilience, and maintainability compared to monolithic architectures.

Middleware Layer: Software that acts as a bridge between operating systems, databases, and applications, enabling them to communicate and share data efficiently. The middleware layer provides common services such as messaging, authentication, API management, and transaction processing—simplifying integration and interoperability across complex systems.

Modernization (in software): The broader process of updating legacy systems, applications, or infrastructure to take advantage of modern technologies, architectures, and practices. While migration often focuses on relocating existing systems, modernization may involve refactoring, replatforming, or redesigning to improve scalability, agility, and long-term business value.

Monolithic Architecture: A traditional software design where all components of an application—such as the user interface, business logic, and data management—are tightly integrated and deployed as a single unit. While simpler to build initially, monolithic systems can be harder to scale, update, or adapt compared to composable alternatives.

Multi-Cloud: A cloud strategy in which an organization uses services from two or more cloud providers simultaneously. This approach helps reduce vendor lock-in, increase resilience, optimize performance, and meet regulatory or geographic requirements by distributing workloads across multiple platforms such as AWS, Microsoft Azure, and Google Cloud.

Multi-Region Model: A cloud computing architecture in which applications and data are deployed across multiple geographic regions offered by a cloud provider. This model improves availability, performance, and disaster recovery by distributing workloads closer to end users and ensuring redundancy if one region experiences outages or latency issues.

Multiverse: A complex system where multiple interconnected business models, content formats, and revenue streams coexist.

Natural Language Processing (NLP): A field of artificial intelligence that enables computers to understand, interpret, and generate human language. NLP combines linguistics, machine learning, and computational techniques to support applications such as chatbots, translation, sentiment analysis, and voice recognition.

Optical Character Recognition (OCR): Technology that converts printed or handwritten text in scanned documents or images into machine-readable digital text, enabling search, editing, and automated processing.

Orchestration Layer: A management layer in computing that automates the coordination, scheduling, and execution of complex tasks across multiple systems, applications, or services. The orchestration layer ensures that components work together seamlessly by handling workflows, resource allocation, scaling, and dependencies. It is commonly used in cloud environments, containerized applications, and microservices to streamline operations and reduce manual intervention.

Orchestrator: A system, tool, or human that coordinates and manages multiple components or processes so they work together to execute complex tasks. (See also: Query Router for Sovereign Data/AI Context).

Permissions: Management of who can access a computer or network. The Access Control List (ACL) is the set of data associated with a file, directory, or other resource that defines the permissions that users, groups, processes, or devices have for accessing it.

Personal Information Protection and Electronic Documents Act (PIPEDA): Canada's federal privacy law governing how private-sector organizations collect, use, and disclose personal information in the course of commercial activities. PIPEDA grants individuals rights to access and correct their data, requires organizations to obtain meaningful consent, and mandates safeguards to protect personal information.

Personally Identifiable Information (PII): Any data that can be used to identify an individual, either on its own or when combined with other information. Examples include names, addresses, phone numbers, email addresses, Social Security or passport numbers, and financial or health records. In computing and data privacy, protecting PII is critical to complying with regulations and safeguarding individuals from identity theft or misuse.

Platform: A computing environment that provides the underlying infrastructure, software, and tools needed for applications or services to run. Platforms can include operating systems, cloud environments, or application frameworks that support development, deployment, and integration. They serve as the foundation on which users, developers, or organizations build and manage digital solutions.

Platform-as-a-Service (PaaS): A cloud computing model that provides developers with a ready-to-use platform—including infrastructure, operating systems, and development tools—for building, testing, and deploying applications. PaaS abstracts away hardware and system management, allowing teams to focus on coding and innovation while ensuring scalability, security, and integration with other cloud services.

Privacy: The protection and proper handling of user data to ensure individuals maintain control over how their personal information is collected, used, shared, and stored in computing environments. Privacy safeguards prevent unauthorized access or misuse of data and are guided by legal, ethical, and regulatory standards. (See also: Personally Identifiable Information [PII]).

Privacy-by-Design: A framework that embeds privacy and data protection principles directly into the design and operation of technologies, processes, and systems. It emphasizes proactive measures—such as minimizing data use, safeguarding by default, and ensuring transparency—so privacy is not an afterthought but a core design principle.

Private Cloud: A cloud computing environment dedicated to a single organization, offering exclusive access to infrastructure, resources, and services. Private clouds can be hosted on-premises or by a third-party provider and are designed to deliver greater control, security, and customization compared to public cloud environments. (See also: Public Cloud).

Process Management: The automation of business processes using a rule-based expert system that invokes the appropriate tools and supplies necessary information, checklists, examples, and status reports to the user.

Prompt Engineering: The practice of crafting, refining, and optimizing input prompts to steer a generative AI model toward producing accurate, relevant, and useful outputs. Effective prompt engineering improves the efficiency, consistency, and reliability of AI systems, enabling them to perform tasks such as summarization, translation, coding, or creative generation with higher quality. As AI models grow more capable, prompt engineering has become a key discipline for aligning outputs with user intent and business goals.

Public Cloud: A cloud computing model in which infrastructure, resources, and services are owned and operated by a third-party provider and delivered over the internet. Public cloud environments are shared among multiple organizations (tenants) but keep data and workloads logically separated. They offer scalability, flexibility, and cost efficiency, with common examples including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud. (See also: Private Cloud).

Query Router: Intelligent function that leverages a rules engine to determine how to route sovereign and non-sovereign data based on the request of an agentic AI workflow.

Real-Time Analytics: The process of collecting, processing, and analyzing data immediately as it is generated, allowing organizations to gain insights and make decisions without delay. In computing, real-time analytics supports use cases such as fraud detection, personalized recommendations, system monitoring, and live performance tracking. (See also: Analytics).

Reasoning AI: AI systems that perform logical thinking, step-by-step planning, problem solving, and decision making using structured or unstructured data, going beyond pattern recognition to draw conclusions and solve complex problems.

Recommendation Engines: Software systems that analyze data and user behavior to suggest relevant products, services, or content. In computing, recommendation engines use techniques such as machine learning, collaborative filtering, or content-based filtering to personalize user experiences, commonly seen in e-commerce, streaming platforms, and digital publishing.

Repository: A storage location, often managed with tools like GitHub or GitLab, where a codebase and its history of changes are kept. While the codebase refers to the actual code itself, the repository also tracks revisions, branches, and contributions, enabling teams to manage and collaborate on the code effectively.

Return on Investment (ROI): A performance metric that measures the profitability or efficiency of an investment, calculated by comparing the net gain or benefit to its cost. In computing and business contexts, ROI is used to evaluate the value of technology initiatives, projects, or purchases by quantifying financial returns relative to the resources invested.

Rights and Permissions: Identifies the circumstances under which a particular asset may be used. For instance, it indicates who legally owns the asset, in what mediums it may be used (web, print, T5) and the financial liabilities incurred to include the asset.

Robotic Process Automation (RPA): Software technology that automates structured, rule-based business tasks by mimicking human actions within digital systems. RPA interacts with applications, forms, and data just as a user would—clicking, typing, copying, and moving information—but does so with speed, consistency, and accuracy. It is commonly used to streamline high-volume administrative processes such as data entry, invoice processing, and records management. In the enterprise, RPA becomes even more powerful when combined with AI and workflow orchestration, enabling both task automation and intelligent decision support at scale.

Rules Engine: A system that makes decisions and applies logic to workflows based on predefined business rules.

Scalability: The ability of a system, application, or infrastructure to handle increasing workloads or demand by adding resources such as processing power, memory, or storage. In computing, scalability ensures consistent performance and reliability as usage grows and can apply to scaling up (vertical scaling) or scaling out (horizontal scaling).

Sentiment Analysis Tools: Software applications that use natural language processing, machine learning, or statistical methods to identify and categorize opinions or emotions expressed in text, speech, or other data. These tools help organizations determine whether sentiment is positive, negative, or neutral, and are commonly used in areas such as customer feedback, social media monitoring, and market research.

Structured Data: Data that resides in fixed fields within a record or file. Relational databases and spreadsheets are examples of structured data.

Unstructured Data: Data that does not reside in fixed locations. Free form text in a word processing document is a typical example.

Workflow Automation: A subset of automation that focuses on coordinating and executing a series of tasks or processes across systems, applications, or teams. Workflow automation maps out the steps in a business or technical process and uses automation to ensure they are carried out in the correct sequence with minimal manual input.

Zero-Party Data: Information willingly shared by users, such as preferences or intentions, collected through surveys or quizzes.

Zero-Trust: A security framework that assumes no user, device, or system should be trusted by default, whether inside or outside an organization's network. In computing, zero-trust requires continuous verification of identity, strict access controls, and monitoring of all activities to minimize risk and protect sensitive data.

Works Cited

Agrawal, A., Gans, J., and Goldfarb, A. "Prediction Machines: The Simple Economics of Artificial Intelligence." *Harvard Business Review Press*, 2022.

"AI Governance Framework: Transparency, Explainability, and Contestability (TEC)." *AI-Governance.eu*, 2024. https://ai-governance.eu/ai-governance-framework/tec/. (Accessed Oct. 2025).

"AI Governance Software Spend Will See 30% CAGR From 2024 to 2030." *Forrester Blog*, Nov. 13 2024. www.forrester.com/blogs/ai-governance-software-spend-will-see-30-cagr-from-2024-to-2030/. (Accessed Oct. 2025).

Barrenechea, Mark J. and Tom Jenkins. *Digital Financial Services*. OpenText Corporation, 2016.

Barrenechea, Mark J. and Tom Jenkins. *Digital Manufacturing*. OpenText Corporation, 2018.

Barrenechea, Mark J. and Tom Jenkins. *e-Government or Out of Government*. OpenText Corporation, 2014.

Barrenechea, Mark J. and Tom Jenkins. *Enterprise Information Management: The Next Generation of Enterprise Software*. OpenText Corporation, 2013.

Barrenechea, Mark J., Jenkins, Tom, and David Fraser. *The Anticipant Organization*. OpenText Corporation, 2022.

Biggio, B., Nelson, B. and P. Laskov. "Poisoning Attacks Against Support Vector Machines." *Proceedings of the 29th International Conference on Machine Learning (ICML)*, 2012.

Boyd, K. "Microsoft 365 Copilot for executives: Sharing Our Customer Zero Deployment and adoption journey at Microsoft." *Microsoft Inside Track Blog*, December 5, 2024. https://www.microsoft.com/insidetrack/blog/copilot-for-microsoft-365-for-executives-sharing-our-internal-deployment-and-adoption-journey-at-microsoft/. (Accessed Oct. 2025).

Bubeck, Sébastien, Chandrasekaran, Varun, Eldan Ronen et al. "Sparks of artificial general intelligence: Early experiments with GPT-4." Cornell University, *arXiv:2303.12712*, April 13, 2023. https://arxiv.org/abs/2303.12712. (Accessed Oct. 2025).

Challapally, Aditya, Pease, Chris, Raskar, Ramesh et al. "The GenAI Divide: The State of AI in Business 2025." *MIT NANDA Report*. MIT Sloan School of Management, July 2025. https://mlq.ai/media/quarterly_decks/v0.1_State_of_AI_in_Business_2025_Report.pdf. (Accessed Oct. 2025).

Crevier, Daniel. *AI: The tumultuous history of the search for artificial intelligence*. Basic Books, 1993.

"Cyber Risks Associated with Generative Artificial Intelligence." *Monetary Authority of Singapore (MAS)*, Circular No. TRPD-G01-2024, Aug. 2024. https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/trpd/cyber-risks-associated-with-generative-artificial-intelligence.pdf. (Accessed Oct. 2025).

Daugherty, Paul, Ghosh, Bhaskar, Narain, Karthik, et al. "A new generative era of AI for everyone." *Accenture*, 2023.

"Data Sovereignty as Your Foundation Layer." *Katonic Blog*, 13 Oct. 2025. https://www.katonic.ai/blog/building-your-ai-stack-data-sovereignty-as-your-foundation-layer. (Accessed Nov. 2025).

"Deepfake and AI Phishing Statistics (2024)." *ZeroThreat.ai*. ZeroThreat, 2024. https://zerothreat.ai/blog/deepfake-and-ai-phishing-statistics. (Accessed Oct. 2025).

Edquist, Alex, Grennan, Liz, Griffiths, Sian et al. “Data ethics: What it means and what it takes.” *McKinsey & Company*, September 23, 2022. https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/data-ethics-what-it-means-and-what-it-takes. (Accessed Oct. 2025).

European Commission. Regulation (EU) 2024/1689 on Artificial Intelligence, 2024.

European Parliament & Council. “Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data.” *Article 17* (Right to erasure), 2016. https://eur-lex.europa.eu/eli/reg/2016/679/oj. (Accessed Oct. 2025).

Cooper, A. Feder, Choquette-Choo, Christopher A., Bogen, Miranda et al. “Machine Unlearning Doesn’t Do What You Think: Lessons for Generative AI Policy, Research, and Practice.” *SSRN*, February 6, 2025. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5060253. (Accessed Oct. 2025).

Foundry Research sponsored by OpenText. “MarketPulse Survey: The Role of GenAI in Modernizing Content Management.” May 2025.

“Gartner Poll Finds 55% of Organizations Have an AI Board.” *Gartner, Inc. Press Release*, 26 June 2024. https://www.gartner.com/en/newsroom/press-releases/2024-06-26-gartner-poll-finds-55-percent-of-organizations-have-an-ai-board

“Gartner Says More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI-Enabled Applications by 2026.” *Gartner Inc. Press Release*., 11 Oct. 2023. www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026. (Accessed Oct. 2025).

“Gartner Survey Reveals GenAI Attacks Are on the Rise.” *Gartner Inc.*, September 22, 2025. https://www.gartner.com/en/newsroom/press-releases/2025-09-22-gartner-survey-reveals-generative-artificial-intelligence-attacks-are-on-the-rise. (Accessed Oct. 2025).

Goodfellow, Ian J., Shlens, Jonathon and Christian Szegedy. “Explaining and Harnessing Adversarial Examples.” Cornell University*, arXiv:1412.6572*, March 20, 2015. https://arxiv.org/abs/1412.6572. (Accessed Oct. 2025).

Gownder, J. P., “The Artificial Intelligence Pathway to the Future of Work.” *Forrester Research*, June 2023.

Gu, Tianyu, Dolan-Gavitt, Brendan and Siddharth Garg. “BadNets: Identifying Vulnerabilities in the Machine Learning Model Supply Chain.” *Cornel University, arXiv:1708.06733*, March 11, 2019. https://arxiv.org/abs/1708.06733. (Accessed Oct. 2025).

Hintze, Arend. “Understanding the four types of AI, from reactive robots to self-aware beings.” *The Conversation*, November 13, 2016. https://theconversation.com/understanding-the-four-types-of-ai-from-reactive-robots-to-self-aware-beings-67616. (Accessed Oct. 2025).

“How we built our multi-agent research system.” *Anthropic*, 2024. https://www.anthropic.com/engineering/multi-agent-research-system. (Accessed Oct. 2025).

“Information Governance Reference Model.” *EDRM*. http://www.edrm.net/projects/igrm. (Accessed Oct. 2025).

International Organization for Standardization. “Artificial Intelligence Standards Portfolio.” ISO/IEC JTC 1/SC 42, 2023.

International Organization for Standardization. “Information Security, Cybersecurity and Privacy Protection—Information Security Management Systems—Requirements.” ISO/IEC 27001:2022.

International Organization for Standardization. “What is Artificial Intelligence (AI)?” January 31, 2024. https://www.iso.org/artificial-intelligence/what-is-ai?. (Accessed Oct. 2025).

Jangam, Sandeep Kumar. “Importance of Encrypting Data in Transit and at Rest Using TLS and Other Security Protocols and API Security Best Practices.” *International Journal of AI*, BigData, Computational and Management Studies, 4(3), 82–91, 2023. https://ijaibdcms.org/index.php/ijaibdcms/article/view/242/. (Accessed Oct. 2025).

Jenkins, Tom. *Behind the firewall: Big Data and the Hidden Web: The Path to Enterprise Information Management*. OpenText Corporation, 2012.

Jenkins, Tom. *Enterprise Content Management: What You Need to Know*. OpenText Corporation, 2004.

Jenkins, Tom. *Managing Content in the Cloud: Enterprise Content Management 2.0*. OpenText Corporation, 2011.

Jiang, Shuli, Kadhe, Swanand Ravindra, Zhou, Yi et al. “Forcing Generative Models to Degenerate Ones: The Power of Data Poisoning Attacks.” Cornell University, *arXiv:2312.04748*, December 7, 2023. https://arxiv.org/abs/2312.04748. (Accessed Oct. 2025).

Joshi, Akshay, Moschetta, Giulia and Ellie Winslow. “Global Cybersecurity Outlook 2025 Insight Report.” World Economic Forum in Collaboration with Accenture, January 2025. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf. (Accessed Oct. 2025).

Kandogan, Eser, Bhutani, Nikita, Zhang, Dan et al. “Orchestrating Agents and Data for Enterprise: A Blueprint Architecture for Compound AI.” *arXiv Preprint*, 10 Apr. 2025. https://arxiv.org/abs/2504.08148. (Accessed Nov. 2025).

Kaplan, Jared, McCandlish, Sam, Henighan, Tom et al. “Scaling Laws for Neural Language Models.” Cornell University, *arXiv:2001.08361*, January 23, 2020. https://arxiv.org/abs/2001.08361. (Accessed Oct. 2025).

“Key Regulatory and Industry Initiatives.” *Capgemini*. https://web.archive.org/web/20141105171058/https://www.worldpaymentsreport.com/kriis#Heat-Map-of-KRIIs-Global-and-Regional. (Accessed Oct. 2025).

“Key Terms for AI Governance.” *International Association of Privacy Professionals (IAPP)*, 2024. https://iapp.org/resources/article/key-terms-for-ai-governance/. (Accessed Oct. 2025).

Kourinian, Arsen and Mayer Brown. “Addressing Transparency & Explainability When Using AI Under Global Standards.” Bloomberg Law, 2024. https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2024/01/addressing-transparency-and-explainability-when-using-ai-under-global-standards.pdf. (Accessed Oct. 2025).

Kurakin, Alexey, Goodfellow, Ian and Samy Bengio. “Adversarial Machine Learning at Scale.” Cornell University, *arXiv:1611.01236*, February 11, 2017. https://arxiv.org/abs/1611.01236. (Accessed Oct. 2025).

LeCun Yann, Bengio, Yoshua, and Geoffrey Hinton. “Deep learning.” *Nature*, 521(7553), 436–444, 2015. https://doi.org/10.1038/nature14539, (Accessed Oct. 2025).

Lu, Ruei-Shan, Lin, Ching-Chang and Hsiu-Yuan Tsao. “Empowering Large Language Models to Leverage Domain-Specific Knowledge in E-Learning.” *Applied Sciences, 14(12), 5264*, June 18, 2024. https://doi.org/10.3390/app14125264. (Accessed Oct. 2025).

Lutkevich, Ben. “What is AI Winter? Definition, History and Timeline.” *Tech Target*, August 26, 2024. https://www.techtarget.com/searchenterpriseai/definition/AI-winter. (Accessed Oct. 2025).

Marcus, Gary. “Deep learning is hitting a wall.” *Communications of the ACM*, 65(8), 36–43, 2022. https://nautil.us/deep-learning-is-hitting-a-wall-238440/. (Accessed Oct. 2025).

Maisto, Dario. “From Digital Sovereignty Platforms To Sovereign Cloud Platforms: Three Reasons For A Title Change.” *Forrester Blogs*, August 11, 2025. www.forrester.com/blogs/from-digital-sovereignty-platforms-to-sovereign-cloud-platforms-three-reasons-for-a-title-change/. (Accessed Oct. 2025).

McCarthy, J., Minsky, M. L., Rochester N. et al. “A proposal for the Dartmouth summer research project on artificial intelligence.” Dartmouth College, 1955. https://ojs.aaai.org/aimagazine/index.php/aimagazine/article/view/1904. (Accessed Oct. 2025).

Mienye, I.D., Jere, N., Obaido, G. et al. “Large language models: an overview of foundational architectures, recent trends, and a new taxonomy.” *Discov Appl Sci 7*, 1027, 2025. https://doi.org/10.1007/s42452-025-07668-w. (Accessed Oct. 2025).

McKinsey & Company. “Future-Proofing the IT Function Amid Global Trends and Disruptions.” *McKinsey Digital*, June 11, 2025. www.mckinsey.com/capabilities/mckinsey-digital/our-insights/tech-forward/future-proofing-the-it-function-amid-global-trends-and-disruptions. (Accessed Oct. 2025).

McKinsey & Company. “The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.” *QuantumBlack* by McKinsey, May 30, 2024. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024. (Accessed Oct. 2025).

Mehrabi, Ninareh, Morstatter, Fred, Saxena, Nripsuta et al. “A Survey on Bias and Fairness in Machine Learning.” Cornell University, *arXiv:1908.09635*, January 25, 2022. https://arxiv.org/abs/1908.09635. (Accessed Oct. 2025).

Mei, Lingrui, Yao, Jiayu, Ge Yuyao et al. “A survey of context engineering for large language models.” Cornell University, *arXiv:2507.13334*, July 21, 2025. https://arxiv.org/abs/2507.13334. (Accessed Oct. 2025).

Miller, Philip. “Unlocking Unstructured Data: Fueling AI with Insights.” *Dataversity*, June 3, 2025. https://www.dataversity.net/articles/unlocking-unstructured-data-fueling-ai-with-insights/. (Accessed Oct. 2025).

Moor, James. “What is Computer Ethics?” *Metaphilosophy*, 16(4), 266–275, 1985, https://doi.org/10.1111/j.1467-9973.1985.tb00173.x. (Accessed Oct. 2025).

“More Than 80% of Enterprises Will Have Used Generative AI APIs or Deployed Generative AI Applications by 2026.” *Gartner Inc. Press Release*, October 11, 2023. www.gartner.com/en/newsroom/press-releases/2023-10-11-gartner-says-more-than-80-percent-of-enterprises-will-have-used-generative-ai-apis-or-deployed-generative-ai-enabled-applications-by-2026. (Accessed Oct. 2025).

Mucci, Tim and Cole Stryker. “What is artificial superintelligence?” *IBM*, July 22, 2025. https://www.ibm.com/think/topics/artificial-superintelligence. (Accessed Oct. 2025).

“New Accenture Research Finds that Companies with AI-Led Processes Outperform Peers.” *Accenture*, October 10, 2024. https://newsroom.accenture.com/news/2024/new-accenture-research-finds-that-companies-with-ai-led-processes-outperform-peers. (Accessed Oct. 2025).

NIST. “Artificial Intelligence Risk Management Framework (AI RMF 1.0).” *NIST Special Publication AI 100-1*, 2023.

Organisation for Economic Co-operation and Development. “Recommendation of the Council on Artificial Intelligence.” *OECD/LEGAL/0449*, 2019.

O’Grady, Michael, and Michele Goetz, et al. “Global Commercial AI Software Governance Market Forecast, 2024 to 2030.” *Forrester Research*, November 1, 2024.

“Predicts 2025: Data and Analytics Strategy—Unlocking Value with AI and Governance.” *Gartner Inc.*, 2024.

Product owner. *Scaled Agile Framework*, February 25, 2025. https://framework.scaledagile.com/product-owner. (Accessed Oct. 2025).

Rabot, M. “Winning in the Autonomous AI Agents Race?” *Medium*, April 4, 2025. https://rabot.medium.com/winning-in-the-autonomous-ai-agents-race-a0c03d52acad. (Accessed Oct. 2025).

Rose, Scott, Borchert, Oliver, Mitchell, Stu et al. “Zero Trust Architecture.” *NIST Special Publication* 800-207, August 2020. https://doi.org/10.6028/NIST.SP.800-207. (Accessed Oct. 2025).

Rowe, Adam. “MIT finds 95% of Enterprise AI Pilots Fail to Deliver Revenues,” *Tech.co*, August 20, 2025. https://tech.co/news/mit-enterprise-ai-pilots-fail-revenues. (Accessed Oct. 2025).

Russell, Melissa. “How can I learn artificial intelligence?” *Harvard*, April 8, 2025. https://extension.harvard.edu/blog/how-can-i-learn-artificial-intelligence/#What-is-Artificial-Intelligence. (Accessed Oct. 2025).

Russell, S.J. and P. Norvig. *Artificial intelligence: A modern approach.* 4th ed., Pearson, 2021.

Sanchez, Jarvy. “Enterprise AI Architecture | Components & Best Practices.” *Leanware*, August 28, 2025. https://www.leanware.co/insights/enterprise-ai-architecture. (Accessed Nov. 2025).

Samoili, S., López Cobo, M., Delipetrev, B. et al. “AI Watch, Defining Artificial Intelligence 2.0: Towards an operational definition and taxonomy for the AI Landscape.” *Publications Office of the European Union*, 2021.

Semba, Kurt. “Artificial Intelligence, Real Consequences: Confronting AI’s Growing Energy Appetite.” *Extreme Networks*, August 15, 2024. https://www.extremenetworks.com/resources/blogs/confronting-ai-growing-energy-appetite-part-1. (Accessed Oct. 2025).

Singla, Alex, Sukharevsky, Alexander, Yee Lareina et al. *The State of AI: How Organizations Are Rewiring to Capture Value.* McKinsey & Company, 2025.

Stanford University. *AI Index Report 2025.* Stanford Institute for Human-Centered Artificial Intelligence, 2025.

Sukharevsky, Alexander, Krivkovich, Alexis, Gast, Arne et al. “The agentic organization: Contours of the next paradigm for the AI era.” *McKinsey & Company*, September 26, 2025. https://www.mckinsey.com/capabilities/people-and-organizational-performance/our-insights/the-agentic-organization-contours-of-the-next-paradigm-for-the-ai-era#/. (Accessed Oct. 2025).

Sunkara, V.L. “KPIs for AI agents and Generative AI: A rigorous framework for evaluation and accountability.” *International Journal of Scientific Research and Modern Technology*, 3(4), 22–29, 2024. https://doi.org/10.38124/ijsrmt.v3i4.572. (Accessed Oct. 2025).

Tegmark, M. *Life 3.0: Being human in the age of Artificial Intelligence*. Vintage Books, A Division of Penguin Random House LLC, 2018.

“The State of AI in Early 2024: Gen AI Adoption Spikes and Starts to Generate Value.” *McKinsey & Company*, May 30 2024. https://www.mckinsey.com/capabilities/quantumblack/our-insights/the-state-of-ai-2024. (Accessed Oct. 2025).

“Towards a Unified Agent with Foundation Models.” *Reddit — r/MachineLearning*, 2024. https://www.reddit.com/r/MachineLearning/comments/155wa2p/r_towards_a_unified_agent_with_foundation_models/. (Accessed Oct. 2025).

Turing, A. M. “Computing Machinery and Intelligence.” *Mind*, Volume LIX, Issue 236, October 1950. https://doi.org/10.1093/mind/lix.236.433. (Accessed Oct. 2025).

Uchida, Yusuke, Nagai, Yuki, Sakazawa, Shigeyuki et al. “Embedding Watermarks into Deep Neural Networks.” Cornell University, *arXiv:1701.04082*, April 20, 2017. https://arxiv.org/abs/1701.04082. (Accessed Oct. 2025).

Unesco. “Recommendation on the Ethics of Artificial Intelligence.” UNESCO.org, 2022. https://www.unesco.org/en/articles/recommendation-ethics-artificial-intelligence. (Accessed Oct. 2025).

University of Michigan College of Engineering. “Up to 30% of the Power Used to Train AI Is Wasted—Here’s How to Fix It.” *Michigan Engineering News*, November 12, 2024. https://news.engin.umich.edu/2024/11/up-to-30-of-the-power-used-to-train-ai-is-wasted-heres-how-to-fix-it/. (Accessed Oct. 2025).

“What is Artificial Intelligence (AI)?” *International Organization for Standardization*, January 31, 2024. https://www.iso.org/artificial-intelligence/what-is-ai?

Wharton School of the University of Pennsylvania. “The Hidden Cost of AI: Energy Consumption.” *Knowledge@ Wharton*, April 25, 2024. https://knowledge.wharton.upenn.edu/article/the-hidden-cost-of-ai-energy-consumption/. (Accessed Oct. 2025).

Yang, Wencheng, Wang, Song, Wu, Di et al. “Deep Learning Model Inversion Attacks and Defenses: A Comprehensive Survey.” Cornell University, *arXiv:2501.18934*, April 30, 2025. https://arxiv.org/abs/2501.18934. (Accessed Oct. 2025).

Yang, Qiang, Liu, Yang, Chen, Tianjian et al. “Federated Machine Learning: Concept and Applications.” *ACM Digital Library*, January 28, 2019. https://dl.acm.org/doi/10.1145/3298981. (Accessed Oct. 2025).

Zhang, Qizheng, Hu, Changran, Upasani, Shubhangi et al. “Agentic Context Engineering: Evolving Contexts for Self-Improving Language Models.” *arXiv preprint arXiv:2510.04618*, 2025. https://www.arxiv.org/pdf/2510.04618. (Accessed Oct. 2025).

Zimmermann, Annette and Danielle Casey. *Emerging Tech Impact Radar: Generative AI.* Gartner, 2025.

Index

A

Adversarial (evasion) attacks, 72

Agentic Artificial Intelligence, 8, 196

AI Agent, 19, 33, 49, 106, 119, 124-125, 131, 137, 144-145, 159, 161, 163, 183-188, 195-199, 209-210

AI ethics, 104

AI governance, 14, 33, 62, 66, 84, 100-107, 109, 112, 114, 168, 192, 194, 206-208

AI model lifecycle, 72-74, 80-81

AI Winter, 44-45, 53, 193, 208

AI-driven Analytics, 102, 196

AI-driven operations, 67, 79, 112, 183

AI-Ready Platform, 196

Air Gap, 196

Algorithms, 37, 45-47, 50, 52-53, 73, 98, 104, 141, 166, 174, 177, 190, 197, 200, 202

Amazon Web Services (AWS), 9, 201, 203-204

Analytics, 13, 15, 19, 21, 26-27, 36, 41, 48, 59, 64, 69-70, 75, 78, 93, 99, 101-102, 133-134, 138, 141, 146, 173-174, 178, 181, 190, 196-199, 201, 204, 209

Anthropic, 140, 207

Anticipant, 4, 195-196, 206

Application management, 13

Application Programming Interface (API), 24, 26-27, 33, 40, 50, 93, 96, 124-127, 144-145, 159, 192-193, 196, 202-203, 207-209

Archive, 9, 15, 26-27, 31-32, 93, 130

Archiving, 26, 32, 70, 74, 130, 198

Artificial General Intelligence (AGI), 7, 29, 34, 37-38, 74, 115, 132, 135, 162, 164-175, 179, 194-196, 206

Artificial Intelligence (AI), 1-5, 7-22, 24-82, 84, 86-91, 93-99, 101-131, 133-163, 165-167, 170-181, 183-212

Artificial Intelligence and Data Act (AIDA), 97

Artificial Narrow Intelligence, 37, 40, 197

Artificial Superintelligence, 37-38, 192, 197, 209

ASR Nederland, 84, 86

Audit, 19, 22, 29, 34, 66, 99, 107, 110-114, 121, 124, 126, 131, 144-145, 159, 161, 169, 197

Audit Trails, 99, 107, 113, 131, 169, 197

Auditability, 19, 34, 62, 83, 93-94, 106-107, 159, 171, 202

Auditable Access, 197

Automation, 8, 18, 23, 27, 33, 35, 40-41, 55-56, 70, 79, 88, 94, 99, 102, 111-113, 118-120, 141, 148, 160-162, 167-173, 180-182, 197, 200-201, 204-205

Autonomous operations, 179-180, 183, 191

B

Backdoor attacks, 72-73, 81

Bias exploitation attacks, 72-73

Big Data, 26, 166, 197-198, 208

Bots, 197, 199

BRZ, 129-130

Bundesrechenzentrum, 129-130

Business Intelligence (BI), 19-21, 48, 64, 122-123, 141, 197

Business Process Management (BPM), 197

C

California Consumer Privacy Act (CCPA), 197-198

Center of Excellence (CoE), 151, 181

Centralized Model, 151

Change Management, 136, 149, 175, 186, 197

ChatGPT, 11, 55, 135, 201

City of Barcelona, 152-153

Claude, 11, 44-45, 201

Client/Server, 25

Cloud, 3-5, 8-9, 15, 26-27, 40, 46, 53, 57, 71, 75, 93-99, 102, 117, 119-120, 129-131, 143, 149, 153, 160-162, 174, 194, 198, 200-204, 208

CloudOps, 198

COBOL, 24, 27

Cognitive Computing, 3, 8, 10

Cognitive Computing Era, 3, 8

Cognitive Era, 15, 26-27, 33, 74

Cohere, 140

Compliance, 2, 4, 10-11, 15-16, 19, 23, 26-32, 42, 46, 56, 62, 66, 74-79, 82, 92-104, 107-120, 124-126, 131, 140, 144-145, 148, 159-162, 168-171, 175, 197-201

Configuration Management, 9, 197-198

Consumer Privacy Protection Act (CPPA), 97

Content Lifecycle Management (CLM), 198

Content Management System (CMS), 25, 153, 198

Contextual Intelligence, 29, 36, 52, 198

Continuous feedback, 61, 66, 183-184, 191

Copilot, 154, 195, 206

COVID-19 Pandemic, 8

Customer Experience (CX), 35, 124

Customer Relationship Management (CRM), 17, 42, 88, 93, 140-141, 198

Cybersecurity, 7, 12-13, 42, 67, 69-71, 74, 78-82, 102-103, 171, 193, 198-199, 207-208

D

Data Driven, 198

Data exfiltration, 72, 107

Data governance, 7, 10, 24, 29, 34, 62, 70, 81-83, 87, 93, 100, 107, 109, 114, 170, 196, 200

Data Lake, 26, 141, 198-199

Data lifecycle, 74-75, 78, 82

Data Mapping, 72, 198

Data poisoning attacks, 72-73, 193, 208

Data Privacy, 48, 124, 148, 197-199, 201, 203

Data Protection Impact Assessment (DPIA), 199

Data Protection Tribunal, 97

Data quality, 30, 34, 53, 56, 58, 63, 66, 136, 156, 163, 166, 170, 173, 175

Data Residency, 99, 131, 199

Data Security, 74, 97, 119, 198-199

Data Silos, 199

Data Sovereignty, 11, 16, 96-97, 117, 199, 206

Data Warehouse, 139, 141, 178, 198-199

Deep learning, 37, 45, 53, 193, 195, 197, 199-200, 202, 208, 211

Deepfake Attacks, 81

Deepfakes, 68

DevOps, 198-199, 202

Digital Asset Management (DAM), 88-89

Digital Charter Implementation Act (Bill C-27), 97

Digital Governance, 84, 199

Digital Personal Data Protection Act (DPDP), 97

Digital Revolution, 8

Digital Workforce, 177, 199

DIRKS methodology, 92

Discontinuity Hypothesis, 166, 173, 175

DNB Finans, 121-123

Drones, 57

Dual data architecture, 119, 124

E

E-commerce, 185, 199, 205

e-Government, 111, 128, 130, 134, 147, 153, 206

Edge Computing, 200

Encryption, 75, 78, 82, 97, 107, 113, 117, 145, 199-200

Energy, 2, 5, 23, 30, 34, 69-70, 141, 210-211

Enterprise Artificial Intelligence (EAI), 1-5, 7-14, 16-22, 24-42, 44-50, 52-66, 68-78, 80-91, 93-99, 101-117, 119-137, 139-158, 160-167, 170-181, 183-212

Enterprise Content Management (ECM), 76-77, 108, 130, 198, 200, 208

Enterprise Information Management (EIM), 11, 15-17, 23, 26-34, 39, 43, 55-57, 69, 75, 83, 88, 91-102, 108-110, 115, 119, 133, 137-138, 145, 162, 173, 200, 206, 208

Enterprise Resource Planning (ERP), 17, 22, 42, 88, 93, 113, 129-130, 140, 200

Enterprise Risk Management (ERM), 106

Ethical AI, 104-105

EU AI Act, 103, 109, 114

EU Data Act, 96

European Union, 92, 103, 192, 201, 210

Explainability, 62, 94, 105, 107, 109, 170-171, 206, 208

Extranet, 29, 34, 108, 147

Extraterritorial Access, 200

F

FAA, 97

Facebook, 45, 122

FDA 21 CFR Part 11, 97

Federated learning, 75

Federated Model, 151-152

Feedback loop, 58, 61, 66, 136, 150, 159, 167, 171, 174, 183, 191

Fine-tuning, 58, 103, 124, 126, 139-140, 143, 148

FinOps, 200

Firewall, 2, 11, 16-17, 26, 33, 78, 115, 139, 208

Five Nines, 179, 187

FOIPPA, 97

Foundational Models, 46, 63, 200

FTC, 97

G

Gartner, 101, 171, 192-195, 207, 209, 211

General Council of the Judiciary (Consejo General del Poder Judicial or CGPJ), 145-147

General Data Protection Regulation (GDPR), 11, 62, 75, 82, 96, 113, 198-199, 201

Generative AI (GenAI), 13, 16, 29, 33-36, 41, 45-46, 50, 52-53, 68, 71, 74, 81, 107, 115-118, 132-136, 139, 142, 183, 192-195, 200-207, 209-211

Geopolitics, 201

Google Cloud, 9, 201, 203-204

Google Gemini, 45, 135, 201

Graphical User Interface (GUI), 52, 201

Guideline B-10, 97

H

HBO, 88-89

Healthcare, 48, 109, 119, 121, 177-178

Hidden web, 16-17, 26, 208

HIPAA, 26, 97

Hub-and-Spoke Model, 151-152

Human agent, 145, 160

Human Resources, 156, 158, 200

Human workforce, 145, 173, 177

Human-generated content, 12, 18, 22

Human-in-the-Loop (HITL), 183-184, 201

Hybrid Model, 117, 129, 151-152

Hype cycles, 53

Hyperscale infrastructure, 3, 8

Hyperscaler, 9, 16, 117, 120, 201

I

IDC, 16

Identity and Access Management (IAM), 78, 201

Identity Management (IdM), 71, 147, 201

Immutable storage, 75, 82

Informatica, 10

Information governance, 23, 42, 84-85, 93, 95, 113, 194, 207

Infrastructure-as-a-Service, 119, 143, 201

Insider threat, 71

Intelligence Layer, 15, 183-184, 201

International Journal of Scientific Research and Modern Technology, 162, 195, 210

International Organization for Standardization (ISO), 37, 62, 66, 75, 82, 92, 95, 103, 110, 114, 170, 192-193, 207, 211

Internet, 5, 16, 29, 33-34, 59, 64, 108, 196, 198-199, 201, 204

Internet of Things (IoT), 59, 64, 190, 200-201

Interoperability, 27, 96, 201, 203

Intranet, 25, 28-29, 34, 88

ISO 15489, 92

ISO/IEC 27001:2022, 75, 82, 193, 207

ISO/IEC 38505, 62

ISO/IEC 42001, 62, 66, 110, 170

iTAC Software AG, 63-64

K

Karlsruhe Institute of Technology (KIT), 133-134

Key Performance Indicators (KPIs), 162-163, 177, 187, 191, 195, 202, 210

Knorr-Bremse Group, 59

Kubernetes, 141, 202

L

LANXESS, 76

Large Language Models (LLMs), 16, 45, 50, 55, 58, 71-74, 135-136, 140, 166, 195, 202, 208-209

Law 11/2007, 147

Legacy Platforms, 202

Legal sovereignty, 117

Lifecycle management, 18, 31, 40, 64, 83, 93-94, 108, 157, 164, 198, 200

M

Machine Learning (ML), 23, 27, 37, 41, 44-45, 53, 141-145, 172, 174, 177-178, 183, 193-203, 205-209, 211

Machine-generated content, 12

Mainframe Era, 24

MAN Diesel & Turbo, 31-32

Managed Services, 12, 155, 202

Marketing, 49-50, 59, 76-77, 88-89, 141, 154, 171, 198

Massachusetts Institute of Technology (MIT), 136, 195, 206, 210

McKinsey & Company, 158, 192, 194-195, 207, 209-210

Mean Time to Restore (MTTR), 179, 183, 187

Metadata, 17-18, 22, 24-27, 29, 33-34, 56, 83, 88-89, 93-99, 121, 134, 140, 202

Metro Vancouver, 110-111

Microservices, 26, 202-203

Microsoft, 9, 25, 154, 195, 201, 203-204, 206

Microsoft Azure, 9, 201, 203-204

Middleware Layer, 203

MillerCoors, 154-155

MOBIS Parts Australia Pty Ltd., 20

Model Context Protocol (MCP), 49-50

Model inversion attacks, 72-73, 81, 193, 211

Model poisoning, 72

Model training, 18, 30, 58, 75, 120, 126

Modernization, 92, 113, 203

Monolithic Architecture, 202-203

Multi-Agent AI Model, 119, 131

Multi-Cloud, 102, 120, 203

Multi-factor Authentication (MFA), 78, 127

Multi-Region Model, 203

Multimodal AI, 46

Multiverse, 203

N

NANDA initiative, 136

National Institute of Standards and Technology (NIST) AI Risk Management Framework (RMF), 78, 103, 107-114, 170, 194, 209-210

Natural Language Processing (NLP), 37, 41, 53, 200, 202-203, 205

Network Operations Center (NOC), 184-185

Neural network, 45, 73, 166, 194, 197, 199, 210

Non-Sovereign / Public Zone, 143

North Atlantic Treaty Organization (NATO, 11

North Star BlueScope Steel, 190

O

Office of the Superintendent of Financial Institutions (OSFI), 97

OpenAI, 45, 135, 140

Operational sovereignty, 117

Operations management, 7, 43, 176-177, 179-181

Orchestration Layer, 40, 167, 200, 203

Orchestrator, 167, 203

Organisation for Economic Co-operation and Development (OECD) / OECD AI Principles, 103-104, 109, 114, 170, 194, 209

P

PC and Desktop Publishing Era, 25

Permissions, 17, 33-34, 83, 90-92, 94, 98-99, 201, 203, 205

Perplexity, 11

Personal Information Protection and Electronic Documents Act (PIPEDA), 95, 97, 203

Personalization, 42, 61, 64, 198, 201

Personally Identifiable Information (PII), 124-125, 145, 203-204

PHIPA, 97

Phishing, 68, 198, 206

PIPL, 97

Platform-as-a-Service (PaaS), 119, 143, 204

Pre-Web, 24

Predictive maintenance, 58, 121, 177-178

Privacy-by-Design, 107, 204

Private Agent, 126

Private Cloud, 119, 149, 160-161, 204

Private Data / Datasets, 16, 34, 55, 58, 60, 69, 73-74, 81, 131, 139-140, 142-144, 160

Process Management, 197, 204

Prompt Engineering, 126, 204

Prompt injection, 72, 107

Proprietary data, 11, 66, 140

Public Agent, 125

Public chatbots, 11

Public Cloud, 57, 117, 129, 131, 143, 160, 204

Public Data / Datasets, 11, 16-17, 33-34, 50, 55, 58, 97, 117, 124-125, 143, 201

Q

Query Router, 124, 127, 203-204

R

Ransomware, 71, 74-75, 198

Real-Time Analytics, 204

Reasoning AI, 204

Recommendation Engines, 39, 202, 205

Red team, 80, 82

Remediation framework, 162

Remote work, 8

Repository, 11, 17, 26, 50, 92-93, 111, 158, 161, 198, 205

Retention and lifecycle management, 83, 93

Retrieval-augmented generation (RAG), 18, 27, 49-50, 58, 124, 126

Return on Investment (ROI), 66, 99, 123, 141, 148, 162, 205

Right to be forgotten, 75

Right to erasure, 75, 194, 207

Rights and Permissions, 205

Robotic Process Automation (RPA), 41, 162, 205

Rules Engine, 11, 204-205

S

Sales, 20-21, 49, 76-77, 89, 154-155, 173-174, 190, 198

Salesforce, 10-11

Sarbanes-Oxley Act, 26

Scalability, 51, 141, 198, 203-205

Scaling Hypothesis, 166, 173, 175

Sentiment Analysis Tools, 205

Small Language Model (SLM), 11, 139

Social engineering, 68, 71

Sovereign / Private Zone, 124, 126, 131, 143

Sovereign cloud, 3, 9, 40, 93, 98, 120, 194, 200, 208

Sovereign Data Sources, 124, 126

Sovereignty, 2, 11, 13, 16, 55, 60, 96-99, 116-117, 119-120, 125, 142-143, 194, 199-200, 206, 208

Structured Data, 16, 24, 170, 200, 205

T

T-Systems, 108

Technological sovereignty, 117

The Big Data, Multimedia, and Mobile Era, 26

The Cloud, 9, 15, 57, 94, 97, 153, 174, 198, 200, 208

The CLOUD Act, 97

Transactional or business-network data, 18

Transparency, Explainability, and Contestability (TEC), 107, 206

Turing, Alan / Turing Test, 44-45, 192, 210

U

UBS, 27-28

United Nations (UN), 11, 104

United Nations Educational, Scientific and Cultural Organization (UNESCO) / UNESCO Recommendation on the Ethics of Artificial Intelligence, 104, 170, 194, 210

Unlearning, 140, 142-143, 195, 207

Unstructured Data, 11, 16-17, 27, 60, 102, 121, 192, 199, 204-205, 209

V

Validation, 58, 73, 112, 124-125, 144-145, 161, 169

W

Web 1.0, 24-25

Web 2.0 and the Collaboration Era, 26

Workflow Automation, 70, 197, 205

World Economic Forum, 71, 193, 208

Z

Zero Trust, 194, 210

Zero-Party Data, 205

Enterprise Artificial Intelligence: Building Trusted AI with Secure Data

There have been moments in technology history when everything changed at once. The arrival of the web. The rise of cloud computing. The mobile revolution. Each wave transformed how businesses operate, how industries compete, and how people live and work.

But none of those shifts compare to the rise of AI in the Cognitive Era—not in speed, not in scale, and certainly not in consequence.

Artificial intelligence has moved from the periphery of enterprise strategy to its core. It is no longer a research initiative or an experimental add-on. It is the new engine of productivity, innovation, and competitive advantage.

Enterprise Artificial Intelligence: Building Trusted AI with Secure Data reveals why the next era of innovation belongs to organizations that treat information as their most strategic asset. Drawing on decades of experience in secure, governed information management, we show how enterprises and governments can build AI that doesn't just perform—but is governed and secure.

From hyperscale clouds to sovereign data policies, this book explores how to balance speed with responsibility, automation with accountability, and intelligence with integrity. Because success won't be decided by who builds the smartest systems—but by who builds the ones we can trust.

The future of enterprise is intelligent. The future of intelligence is governed. And the work begins now.

11.25 |243-000119-001