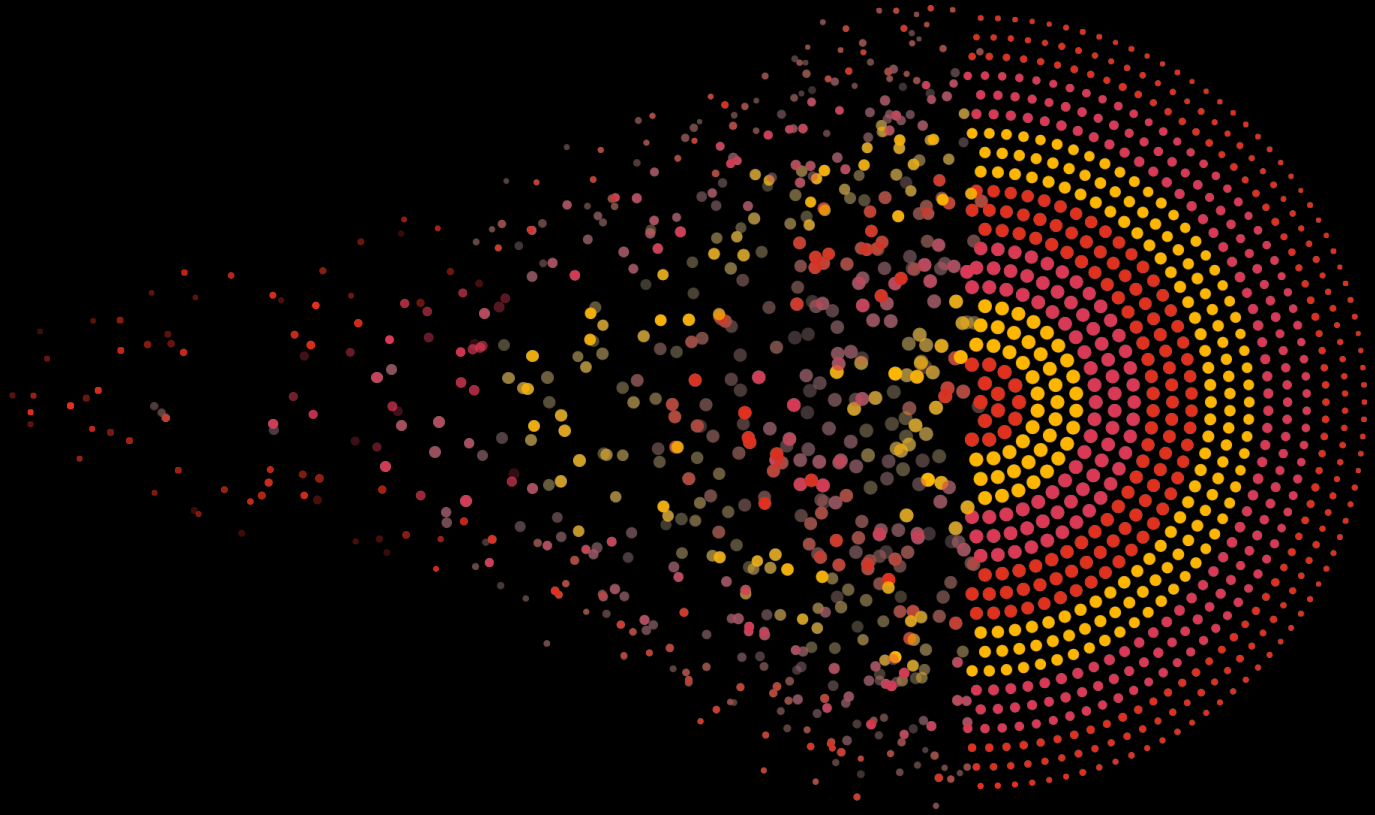
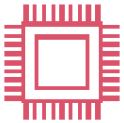
GenAI

May 2025



AI Approach

AI Strategy



Apply

- Use and Business Case
- Generative AI
- Chatbots
- ML Model Build
- Intelligent Collaboration

Protect

- AI Privacy
- AI enabled Cybersecurity
- Secure AI
- Counter AI Cybersecurity

Comply

- AI Exposure Register
- EU AI Act
- Responsible AI
- Industry Regulation

Adopt

- AI Governance
- Change Management
- Human Centricity
- Upskilling

Trust

Approach - Five no regret areas of focus

To help clients navigate their GenAI journey and set themselves up to release its full potential, we have identified five no regrets areas of focus that all organisations should consider. This foundational framework can guide organisations to lay the right foundations, start small and scale success.

Our ongoing client interactions and engagements reflect most traction and momentum in the below 2 areas:

Developing strategic vision

- Assessing impacts across value-chain, business functions and operations
- Looking at broader AI spectrum holistically for disruption
- Preparing for new commercial models

Tech vision and strategy evolution - Apply, Protect, Comply

- Designing and standing up the right cloud and infrastructure ecosystem
- Assessing and aggregating data with right management
- Data privacy, governance and IP policy
- Cyber security
- Preparing for new commercial models

Four Dimensions of Responsible AI

Responsible AI at its core is simply good data science, governed by key guiding principles **from strategy to execution.**

Strategy

Data & AI Ethics
Consider the moral implication of uses of data and AI and codify them into your organization's values.

Policy & Regulation
Anticipate and understand key public policy and regulatory trends to align compliance processes.

Control

Governance
Enable oversight of systems across the three lines of defense.

Compliance
Comply with regulation, organizational policies, and industry standards.

Risk Management
Expand transitional risk detection and mitigation practices to address risks and harms unique to AI.

Responsible Practices

Interpretability & Explainability
Enable transparent model decision-making.

Sustainability
Minimize negative environmental impact.

Robustness
Enable high performing and reliable systems.

Bias & Fairness
Define and measure fairness and test systems against standards.

Security
Enhance the cybersecurity of systems.

Privacy
Develop systems that preserve data privacy.

Safety
Design and test systems to prevent physical harm.

Core Practices

Problem Formulation
Identify the concrete problem you are solving for and whether it warrants an AI / ML solution.

Standards
Follow industry standards and best practices.

Validation
Evaluate model performance and continue to iterate on design and development to improve metrics.

Monitoring
Implement continuous monitoring to identify drift and risks.

Developing responsible AI is not just one person's job

Diverse stakeholders across all parts of the organization must **collaborate** to apply responsible AI practices consistently and effectively.

The 3 lines of defense

Enterprise-level

External

Regulators
External auditors

External audit
Regulatory requirements and legal action
External standards development

3rd Line of Defense

Internal Audit
Ethicists

Internal audit review
Ethics review

2nd Line of Defense

Compliance
Legal & Privacy
Leadership
Independent Review Group
SME Model Approver

Standards and Specs
Independent Review and Challenge
Final Approval
Legal, Data & Privacy Governance requirements

Application-Level

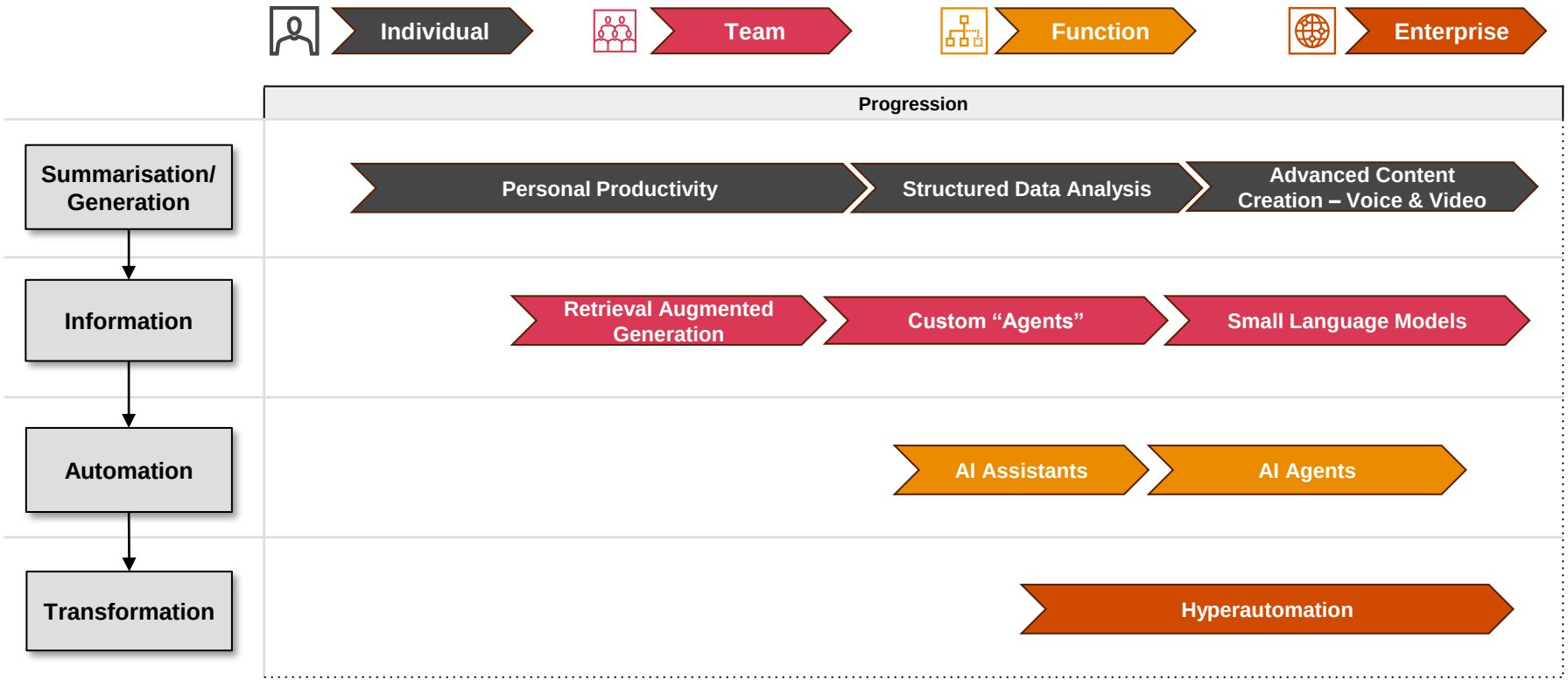
1st Line of Defense

Model devs
Model owners
Ops support

Risk Assessment
Model Sourcing and/or Development
Data Collection and Use
Process Documentation

Infrastructure
Deployment
Ongoing Monitoring

Evolution of GenAI



AI Agents

Information Agents
Purpose
To retrieve information from specified sources of information only. Does not use its own knowledge or web searching to augment the information sources
Complexity
Low – easy to create with off the shelf tools. Often aimed at the end user creating their own personal agent or sharing agents with their team. More complex and robust agents can be created by developers
Information Sources
Generally departmental or specific topic information repositories. Tend to be internal web sites or sharepoint sites. Requires some data governance to manage information access
Example Uses
Sharepoint agent to retrieve information from a team site. Agent to do a web search of specific regulators sites to answer questions
Automation Assistants
Purpose
Human driven assistant retrieve information and execute actions. Requires the human to request an action to be executed
Complexity
Med – Generally used to create enterprise-wide capabilities. Requires developer skills to build system and RPA developer skills to build the automations. Existing automations or IT services ca
Information Sources
Information sources tend to be enterprise in nature, these can be information repositories, data bases or enterprise operational systems. Strong data governance is required.
Example Uses
HR or IT chatbot that will not only answer questions but will also execute common actions or open a ticket automatically when it cannot resolve the issue. Other use cases include customer service chatbots
Automation Agents
Purpose
AI agent that executes actions without requirement for human input. AI decides which actions to execute based on output from previous actions or data input
Complexity
High – Requires the same skills for development of the agent and the RPAs as the automation assistant, however more in-depth testing, robustness and process mapping as the system will run autonomously
Information Sources
Information sources tend to be enterprise in nature, similar to Automation Assistants. Very high level of data governance is required as humans are not in the loop to
Example Uses
Running the onboarding process for new hires, it manages and coordinates the processes across multiple departments and operational systems. Other use cases include KYC and other comple
Multimodal Agents
Purpose
AI Agent to execute actions driven by multiple data types (voice, audio, video, images), and can also create outputs in these formats.
Complexity
Very High – Need to have the ability to understand inputs in multiple formats. Regarded as cutting-edge technologies which few people have experience with
Information Sources
Information sources tend to be complex in nature, e.g. realtime voice conversations with humans or video/images that need to be interpreted. Very complex data
Example Uses
Automated insurance claims handling over the phone. Identifying fraud through the review of video/images. Other examples include as a call centre agent or used to generate store layouts from video of the site