

Creating Confidence in AI

Mona de Boer, Gülnur Orpak

Are we where
we need to be?

Big Year-Over-Year Changes

2024

2025

17%

Organizations with a
comprehensive AI policy

31%

45%

Organizations that permit
the use of generative AI

63%

12%

Provide AI training to
all employees

28%

ISACA AI Pulse Poll 2025

Big Year-Over-Year Changes

2024

2025

17%

Organizations with a comprehensive AI policy

31%

45%

Organizations that permit the use of generative AI

63%

12%

Provide AI training to all employees

28%

15%

all employees
Provide AI training to

58%

THE AI RISKS:

1



85% Misinformation/disinformation

2



68% Privacy violations

3



62% Social engineering

4



58% Loss of IP

5



37% Increasing skills gap

2



31% Increasing skills gap

3



28% Loss of IP



64%

are very or extremely worried that generative AI will be **EXPLOITED** by bad actors.



ONLY 28%

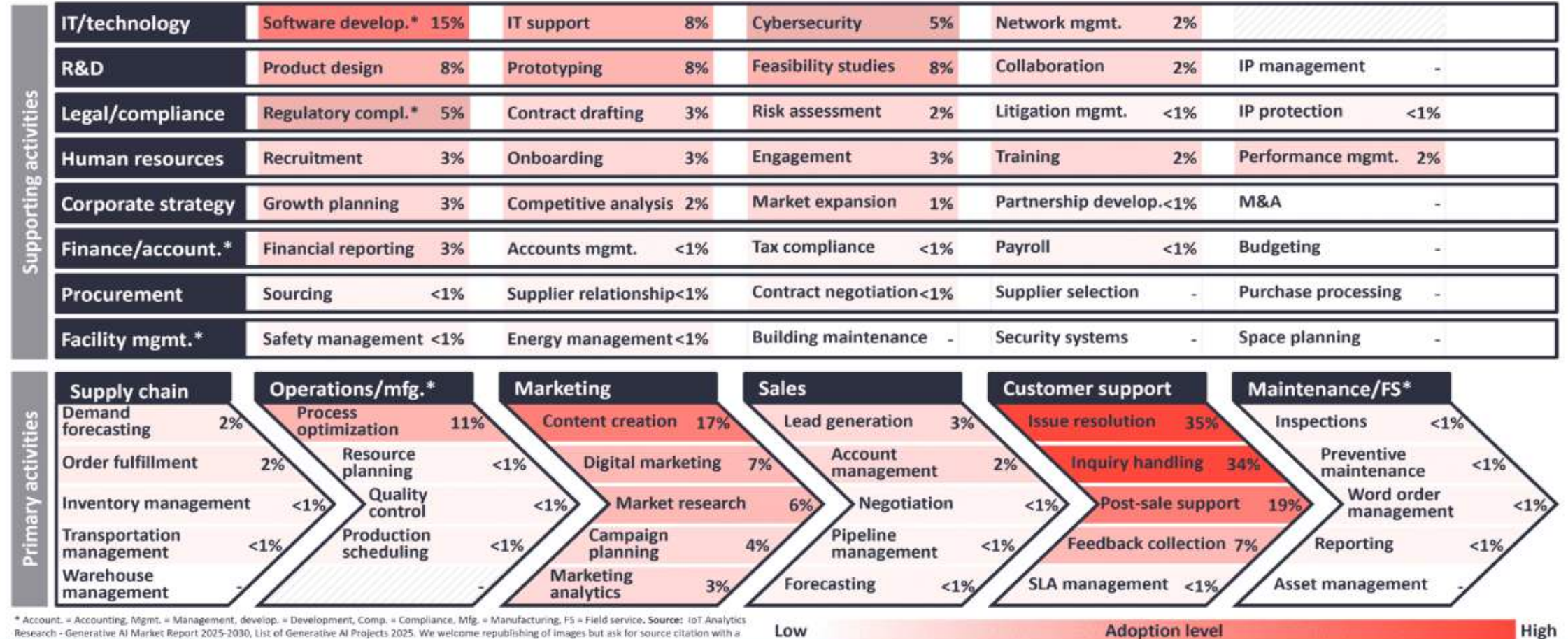
believe organizations are adequately addressing **ETHICAL CONCERNS** in AI deployment, such as data privacy, bias and accountability.

(Confident) AI Adoption: where are we at?
ISACA AI Pulse Poll 2025

Enterprise generative AI application landscape

Mapping 530 real world projects across 68 common business activities

XX% = Share of GenAI projects that support the respective activity



Our next destination requires even more confidence...

AI represents a shift in how business value is created

How leading organizations are responding to complexity and opportunity in an AI-powered world:

AI Governance/Security Platforms

AI-Native Development Platforms

AI Supercomputing Platforms

Why these matter now:

Not just technical shifts: strategic imperatives

Align digital strategy with enterprise goals

Scale AI securely and responsibly

No single capability is enough

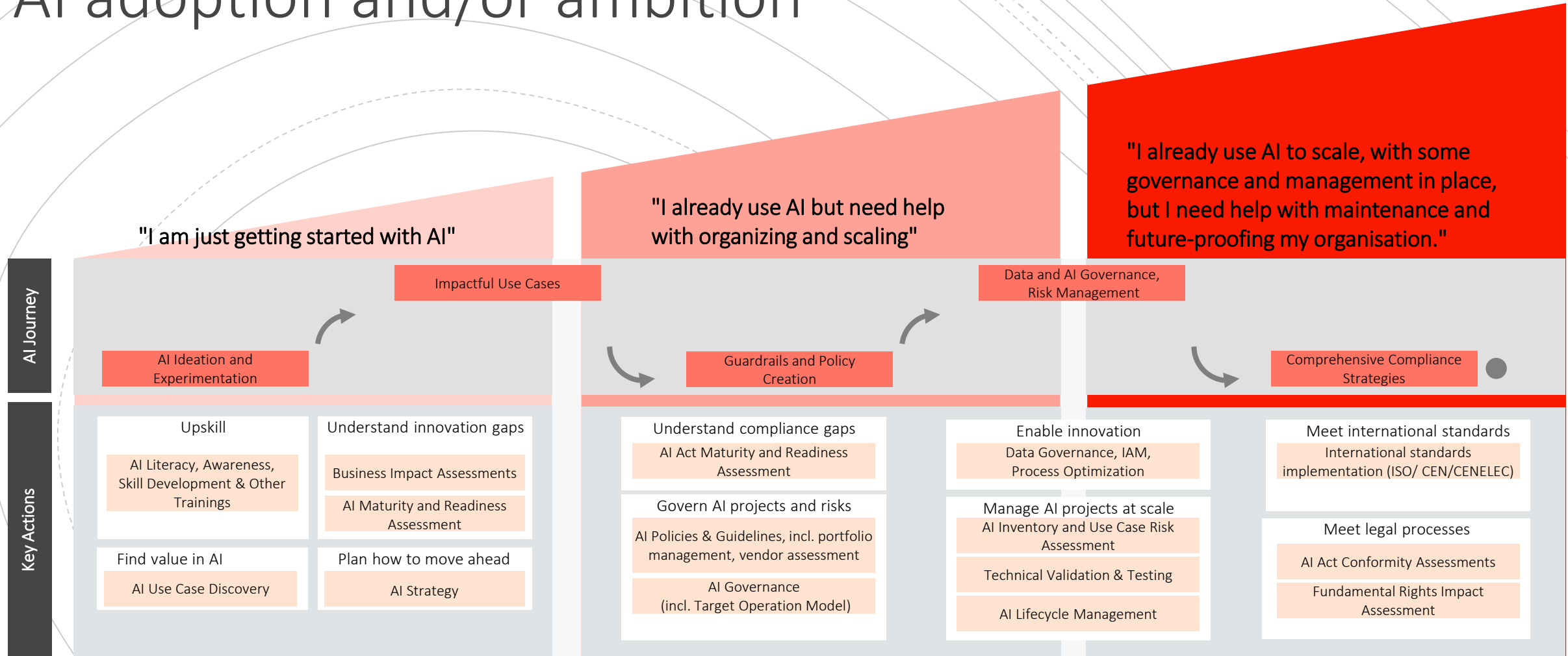
Innovate

Compete

Protect Value

**Gartner Top Strategic
Technology Trends**

The need for confidence is a sign of progressing AI adoption and/or ambition





Who has
performed
an 'AI Audit'?

A. Entity Level Controls

1. Organisation-level Controls

- Organisational values and principles e.g. Ethics
- AI Strategy
- AI Governance
- AI Policy and Standards
- AI Culture, Awareness and Literacy
- AI Inventory

2. Process-level Controls

- Business case process
- Software Development Lifecycle (SDLC) and CI/CD pipelines
- Key IT processes e.g. LCM
- IT Architecture
- Risk Management and Compliance
- Data Management
- Information Security Management
- Incident Management
- Outsourcing and Third-Party Risk Management

B. Infrastructure Level Controls

Platform - CI/CD pipelines - Data pipelines

Data

Quality, Governance, Security, Integrity

Model

Technical Documentation, Model Integrity, Model Validation, Human oversight, Regular audits, Model Performance

Application

Logging & Monitoring - Access management - Scalability and load management - Patch management - Continuity

How can risk
and audit
functions
contribute?

Focus of current and forthcoming 'AI audits'

AI Governance, Risk Mgt & Control

- (Quality) Management System
- Risk Management
- Data and Data Governance
- Accuracy, robustness and security
- Documentation and record keeping
- Transparency and provision of information to users
- Human oversight

AI Compliance

- EU AI Act
 - Prohibited AI
 - AI Literacy
- GDPR
- Data Act
- DORA

Conformity
Assessment
(Aug 2026)

AI System Functionality

- Lawfulness
- Ethics
- (Technical) robustness

AI System Impact

- Lawfulness
- Ethics
- (Technical) robustness

