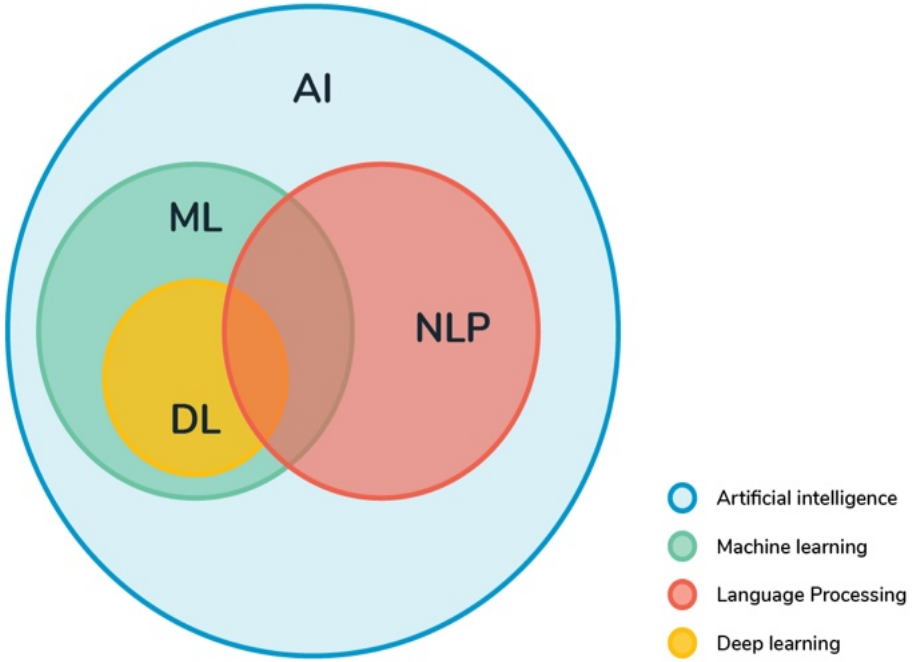
AI VISIBILITY, CONTROL AND TRUST

CYBER SECURITY PERSPECTIVE

CYBER SECURITY PERSPECTIVE FOR MANAGING AI RISK

AI is no longer only solving operational problems ,
it is becoming a core enabler of enterprise control, trust, and security.

As adoption accelerates, risk exposure grows in parallel, unless governance is designed into deployment from the outset.



Contract Taxation	Healthcare	Retail
Legal Verification	Workflow Automation	Property lettings

HTP

This

THE THREE CRITICAL AI RISK GAPS

Board Level Strategic Assessment

Strategic Risk	Board Level Exposure	Business Impact
01 **Lack of Visibility** Limited understanding of where AI operates across enterprise systems	*No governance without visibility. Board cannot assess what it cannot see.*	**Hidden dependencies & unmanaged risk exposure**
02 **Unpredictable Behaviour** Nondeterministic outputs from models and agents across critical workflows	*AI systems may act inconsistently, creating brand, legal or financial liability.*	**Hallucinations, bias & operational inconsistency**
03 **Compliance Blind Spots** Controls not aligned to regulatory or internal policy requirements	*Regulatory change creates sudden non-compliance risk at enterprise scale.*	**Legal exposure & audit weakness**

01 ESTABLISH AI ASSET VISIBILITY

Build a Live AI Bill of Materials(ALBOM)

Models

Foundation + fine-tuned

Agents

Autonomous task runners

RAG Architectures

Retrieval-augmented systems

MCP Layers

Model Context Protocol

Third-Party AI

Embedded external services

↓ FEEDS INTO ↓

Enterprise Applications → **AI Components Inventory** → **Live AI-BOM** → **Continuous Risk Visibility**

KEY INSIGHT: *A live AI Bill of materials creates an always current view of AI assets, dependencies, ownership, and exposure the foundation of enterprise AI control.*

02 CONTINUOUS ADVERSARIAL TESTING

Stress Test as Cyber-Critical Infrastructure

- Hallucination Exposure
- Bias Drift
- Data Leakage
- Jailbreak Attempts
- Prompt Injection
- Unsafe Responses

TEST → **DETECT** → **CORRECT** → **REVALIDATE**

03 POLICY DRIVEN GOVERNANCE

Embed Controls into AI Deployment Workflows

Policy Rules

Licensing, safety, ethics standards

↓

Automated Controls

Machine speed enforcement

↓

Approval Workflow

Human review for exceptions

↓

Audit Readiness

Full traceability & reporting

GOVERNANCE PRIORITIES

- Licensing Validation
- Prompt Safety Controls
- Approval Workflows
- Exception Handling
- Scheduled Policy Review

STRATEGIC OUTCOMES FOR THE BOARD

Four Competitive Advantages

01 Controlled AI Scale Up

Expand AI capability confidently with full asset visibility and governance rails in place from day one.

02 Reduced Regulatory Exposure

Policy controls aligned to compliance requirements reduce audit risk and eliminate legal liability at scale.

03 Stronger Trust in AI Decisions

Continuous adversarial testing creates confidence in AI-driven outputs across all enterprise operations.

04 Faster Adoption, Lower Risk

Governance by design accelerates deployment timelines while measurably reducing operational exposure.

HTP

Organisation that act early create durable competitive and compliance advantage

BOARD MESSAGE

AI should now be governed as a strategic operating capability not simply as a technology deployment

The winners will be organisations that build visibility, resilience, and policy control before scale creates complexity.