
TÜV SÜD BABT Unlimited

AI Essentials
A Practical Introduction to Responsible AI Governance

TÜV SÜD BABT Unlimited is a Certification body of TÜV SÜD Group

Introduction

Artificial Intelligence is now part of everyday business operations. It may be visible through tools such as Microsoft Copilot, ChatGPT or Gemini, or embedded within products and services that organisations already use.

Many organisations are already using AI without having formally recognised it. Employees may be experimenting with AI tools, software suppliers may have added AI functionality to existing products, or teams may be using AI services without a clear understanding of associated risks and responsibilities.

AI Essentials provides a practical starting point. It helps organisations understand where AI is being used, establish appropriate oversight, and demonstrate that AI is being used responsibly and transparently. AI Essentials Plus builds upon this foundation by providing independent verification that the controls an organisation has established are operating effectively in practice.

The examples provided in this guide are intended to illustrate the types of evidence and governance artefacts commonly used by organisations. They are not mandatory requirements, nor do they prescribe a specific implementation approach. Organisations may choose alternative methods that are appropriate to their size, complexity, role within the AI value chain and level of risk.

1 Understanding Your Organisation's AI Landscape

Before governance can be established, it is important to understand how AI is already being used.

For some organisations this may involve only a small number of AI-powered productivity tools. For others, AI may be embedded across business processes, products, customer services, analytics platforms or operational systems.

Organisations generally fall into one or more of the following roles:

AI Users

Organisations that use AI systems developed by others to support their own operations.

Examples include:

- Using AI assistants for document creation
- Using AI-powered customer service tools such as Chatbots
- Using AI features embedded within software products

AI Providers

Organisations that integrate or supply AI-enabled services to customers.

Examples include:

- Software providers incorporating AI functionality
- Managed service providers offering AI solutions
- Organisations embedding third-party AI within customer-facing services

AI Producers

Organisations that design, train or develop AI models and systems.

Examples include:

- AI product developers
- Machine learning solution providers
- Organisations creating proprietary AI applications

The level of governance required will often depend on the role performed and the potential impact of AI use.

Note: an organisation may have more than one role.

Typical Evidence	Common Governance Assets
• Staff AI surveys • Questionnaires issued to departments • Software inventories • IT asset registers • Procurement records • Supplier lists • SaaS subscription records • Software licence inventories	• AI discovery survey • AI inventory questionnaire • AI governance project charter • AI governance scope statement • Organisational AI role declaration (User, Provider, Producer)

2 Establishing Governance and Accountability

AI governance does not necessarily require a large team or a complex management system. What is important is that responsibility for AI is visible and understood.

Many organisations choose to identify an individual or governing group responsible for overseeing AI use. The size and structure of this governance resource will vary according to organisational size, complexity and risk profile.

Typical responsibilities may include:

- Maintaining awareness of AI use
- Reviewing risks and impacts
- Monitoring compliance with organisational policies
- Coordinating training and awareness activities
- Escalating significant concerns to leadership

AI governance should help ensure that AI use remains visible, accountable and aligned with organisational objectives.

Typical Evidence	Common Governance Assets
• Board meeting minutes • Management meeting records • Governance committee terms of reference • Appointment records • Organisation charts • Role descriptions	• AI Governance Framework • AI Governance Committee • AI Accountable Officer appointment • AI Governance Policy • AI Governance Charter • AI Roles and Responsibilities Matrix

3 Discovering Existing AI Use

Many organisations are surprised by how much AI is already being used.

A useful starting point is to identify:

- AI applications used by employees
- AI features embedded within existing software
- AI-enabled supplier services
- Customer-facing AI systems
- Internally developed AI tools
- Automated decision-support systems

This discovery activity often helps uncover:

- "Shadow AI" usage
- Unapproved tools
- Personal AI accounts used for business activities
- "Hidden AI" - AI features that were enabled by software suppliers without formal review

The objective is not to stop innovation, but to create visibility and understanding.

Typical Evidence	Common Governance Assets
• Staff responses • IT software scans • Supplier declarations • Existing risk registers • Business process documentation • Application inventories	• AI Discovery Report • AI Usage Assessment • AI Estate Review • Departmental AI Usage Register

4 Creating an AI Registry

An AI Registry is one of the core foundations of AI Essentials.

The registry acts as a central record of AI systems and services used within the organisation.

A registry may contain information such as:

- System name
- Purpose & known limitations
- Business owner
- Supplier or developer
- Users of the system
- Data processed
- Risk classification
- Current status

An AI Registry helps organisations answer important questions:

- What AI do we use?
- Who is responsible for it?
- Where is it being used?
- Which systems present higher levels of risk?
- Which systems require additional oversight?

The registry becomes an important source of information for governance activities, risk reviews and future assurance assessments.

Typical Evidence	Common Governance Assets
• Completed AI Registry entries • AI system descriptions • Supplier information • Ownership assignments • Registry review records	• AI Registry • AI Asset Register • AI Service Register • Third-Party AI Register • AI Lifecycle Register

5 Staff Awareness and AI Training

Technology controls alone are not enough. People remain responsible for how AI is used within an organisation.

- AI training helps employees understand:
- What AI is
- How it is being used within the organisation
- Benefits and limitations of AI systems
- Appropriate use of organisational AI tools
- Security and data protection considerations
- The importance of human judgement

Training does not need to make everyone an AI specialist. Instead, it should help individuals understand their responsibilities and make informed decisions when using AI-enabled systems.

As AI use expands, organisations may choose to provide additional role-specific training for managers, technical teams or governance personnel.

Typical Evidence	Common Governance Assets
• Training attendance records • Learning management system reports • Assessment results • Awareness campaign records • Staff communications	• AI Awareness Training • AI Literacy Programme • E-Learning Modules • Role-Based Training Paths • AI Induction Material • Executive AI Briefings

6 Developing an Acceptable AI Use Policy

An Acceptable AI Use Policy establishes organisational expectations for AI use.

The policy provides guidance on:

- Approved and authorised AI tools
- Appropriate use of organisational information
- Human responsibility for AI-generated outputs
- Protection of confidential data
- Review and validation of AI outputs
- Escalation of concerns or incidents

The purpose of the policy is not to prevent AI use. Instead, it helps ensure that AI is used consistently, responsibly and in a manner that supports organisational objectives.

A well-communicated policy often becomes one of the most visible components of an organisation's AI governance framework

Typical Evidence	Common Governance Assets
• Approved policy document • Employee acknowledgements • Policy review records • Internal communications • Published intranet guidance	• Acceptable AI Use Policy (AAUP) • AI Security Guidance • AI Data Handling Guidance • AI Human Oversight Guidance • AI User Handbook

7 Understanding AI Risks

AI can create a range of opportunities and risks. Typical risk topics

- Security
- Data protection
- Accuracy
- Reliability
- Fairness
- Regulatory compliance
- Supplier dependency
- Reputation

Potential risks may include:

- Information Risks
- Inappropriate disclosure of confidential information
- Data protection concerns
- Intellectual property exposure
- Operational Risks
- Incorrect outputs
- Hallucinations or fabricated information
- Over-reliance on AI-generated recommendations
- Security Risks
- Unauthorised access
- Manipulation of AI systems
- Adversarial attacks
- Governance Risks
- Lack of accountability
- Unclear ownership
- Insufficient oversight

Not every AI system presents the same level of risk. Understanding risk helps organisations apply proportionate oversight and governance.

Typical Evidence	Common Governance Assets
• Risk assessments • Enterprise risk registers • Incident records • Security reviews • Internal audit findings	• AI Risk Register • AI Risk Assessment Template • AI Governance Dashboard • AI Incident Reporting Process • AI Risk Review Records

8 Understanding AI Impacts

Risk focuses on what could go wrong. Impact considers the consequences if something does happen.

AI impacts may affect:

- Customers
- Employees
- Suppliers
- Regulators
- Society
- The organisation itself

Examples could include:

- Customer decisions influenced by AI
- Recruitment recommendations
- Automated communications
- Service prioritisation
- Data processing activities

Higher-impact AI systems may require a more detailed review and stronger governance arrangements than lower-impact systems.

AI Essentials encourages organisations to understand these impacts and ensure that significant uses of AI receive appropriate consideration.

Typical Evidence	Common Governance Assets
• Impact assessments • Stakeholder consultations • Board papers • Legal reviews • Privacy assessments • Business case documentation	• AI Impact Assessment (AIIA) • Ethical Impact Assessment • Data Protection Impact Assessment • AI Transparency Statement • Societal Impact Review

9 Monitoring AI Use

Governance is not a one-time activity. Once AI systems have been identified, organisations should maintain awareness of how they continue to operate and evolve.

- Monitoring activities may include:
- Reviewing changes to AI systems
- Updating the AI Registry
- Tracking incidents and concerns
- Reviewing feedback from users
- Monitoring supplier changes
- Evaluating whether controls remain effective

The objective is to ensure that governance remains aligned with actual AI use rather than becoming a static exercise.

Typical Evidence	Common Governance Assets
• Monitoring reports • Governance meeting minutes • Incident logs • System review records • Internal audit reports • Supplier review records	• AI Monitoring Programme • AI Performance Dashboard • AI Governance Review Schedule • AI Incident Register • AI Change Review Process

10 Completing the AI Essentials Self-Assessment

Once governance foundations have been established, organisations can complete the AI Essentials Self-Assessment Questionnaire (SAQ).

The self-assessment enables the organisation to demonstrate that key governance elements are in place, including:

- Accountability
- AI inventory and visibility
- Policy arrangements
- Staff awareness
- Risk and impact consideration
- Governance oversight

The assessment provides a structured way to demonstrate that AI use is visible, governed and subject to appropriate organisational control

Typical Evidence	Common Governance Assets
• Completed SAQ • Supporting governance documents • Policy records • Registry records • Training records • Risk and impact assessments	• Self-Assessment Questionnaire (SAQ) • Evidence Pack • Governance Summary • Board Declaration • AI Transparency Statement

11 Progressing to AI Essentials Plus

AI Essentials provides confidence that governance arrangements have been established. AI Essentials Plus goes further by independently assessing whether those arrangements are operating effectively in practice.

The focus shifts from:

"Have controls been established?"

to

"Are the controls working?"

An AI Essentials Plus assessment may include:

- Review of governance arrangements
- Verification of assessment evidence
- Examination of operational controls
- Review of monitoring activities
- Validation of accountability arrangements
- Role-appropriate technical testing

The exact activities depend on the organisation's role as an AI User, Provider or Producer and the nature of the AI systems being assessed.

Typical Evidence	Common Governance Assets
• Internal validation records • Control testing records • Monitoring evidence • Governance reviews • Effectiveness measurements • Audit evidence	• AI Essentials Plus Readiness Review • Internal Validation Plan • Test Reports • Findings Register • Corrective Action Tracker • Audit Evidence Pack

Areas Often Reviewed

- Governance effectiveness
- Human oversight arrangements
- Monitoring effectiveness
- Registry maintenance
- Risk management activities
- Control implementation
- Technical safeguards appropriate to organisational role

Conclusion

AI governance should not be viewed as a barrier to innovation. Its purpose is to help organisations understand how AI is being used, manage associated risks, and build confidence among customers, employees and stakeholders.