AI Governance Standard (AGS Verified)
Technical Requirements (Version 2.1)

Contents

1. Introduction

The AI Governance Standard (AGS) sets out the minimum organisational controls required to support the responsible use of artificial intelligence (AI) within business operations.

The standard is designed to be proportionate, practical, and applicable across a wide range of organisations, with a particular focus on operational use of AI tools rather than technical system development.

AGS provides a structured framework through which organisations can demonstrate that AI is used in a controlled, accountable, and transparent manner.

The AGS framework includes a defined set of critical controls, representing the minimum requirements for responsible AI use.

These controls address the most significant risks associated with AI, including governance, accountability, verification of outputs, and protection of sensitive information.

All critical controls must be met in order to achieve certification. Organisations that do not meet these minimum requirements will not be awarded AGS Verified status, regardless of overall performance.

2. Scope of the Standard

AGS applies to the use of AI tools within organisational workflows, including generative AI systems and AI-enabled features within commercial software platforms.

The standard is intended to assess how AI is governed and applied in practice, rather than how AI systems are designed or built.

The following are within scope:

- Use of AI tools in business operations
- AI-assisted decision-making
- Generative AI outputs (text, image, code, etc.)
- AI features embedded within software platforms

The following are out of scope:

- Development or training of AI models
- Research or experimental AI systems
- Technical evaluation of AI system performance

3. Control Framework Overview

The AGS framework is structured across seven control domains, each addressing a key aspect of organisational AI governance.

Together, these domains form a complete and proportionate control environment.

The control domains are:

- Governance and Policy
- AI Usage Controls
- Human Oversight
- Data and Information Handling
- Training and Awareness
- Monitoring and Oversight
- Transparency

Each domain defines both an **objective** and a set of **minimum control requirements**.

4. Control Domains and Requirements

4.1 Governance and Policy

Effective governance is the foundation of responsible AI use. Organisations must establish clear policies, roles, and oversight mechanisms to ensure AI use is controlled and understood.

Key requirements include:

- Maintaining a documented AI policy
- Ensuring the policy is accessible and communicated to staff
- Defining acceptable and prohibited uses of AI
- Assigning responsibility for AI oversight
- Defining and maintaining approved AI tools
- Reviewing and updating policies periodically
- Communicating changes in AI-related risks or controls

4.2 AI Usage Controls

AI tools must be used in a structured and controlled manner to ensure outputs are reliable and appropriate.

Organisations are expected to:

- Define procedures for how AI tools are used
- Require AI-generated outputs to be checked before use
- Restrict AI use in higher-risk activities where appropriate
- Ensure AI-generated content is identifiable in internal use
- Require staff to follow defined usage processes

4.3 Human Oversight

Human judgement and accountability must remain central to all outputs produced using AI.

Organisations must ensure that:

- Accountability for outputs remains with a human
- AI-generated outputs are subject to verification
- Errors in AI outputs are identified and corrected
- Higher-risk uses of AI are identified
- Additional controls are applied to higher-risk uses
- Staff apply professional judgement when using AI outputs
- Processes exist to identify inaccurate, biased, or misleading outputs

4.4 Data and Information Handling

The use of AI tools introduces risks relating to data handling. Organisations must ensure that sensitive information is protected.

Key controls include:

- Defining how organisational and client data may be used in AI tools
- Identifying data types that must not be used in AI tools
- Implementing controls to prevent unauthorised data use
- Providing staff with guidance on safe data handling in AI systems

4.5 Training and Awareness

Staff must understand how to use AI tools responsibly and recognise their limitations.

Organisations must:

- Provide guidance or training on responsible AI use
- Ensure staff understand the limitations of AI-generated outputs

- Include AI governance within onboarding processes
- Provide clear routes for reporting misuse or concerns

4.6 Monitoring and Oversight

AI use must be actively monitored to ensure controls remain effective over time.

Organisations are expected to:

- Periodically review how AI tools are used
- Maintain a process for reporting AI-related incidents or misuse
- Record issues relating to AI use
- Take action to address identified issues
- Maintain visibility over where AI tools are used within workflows

4.7 Transparency

Organisations must consider how AI use is communicated internally and externally.

This includes:

- Defining when clients are informed of AI use
- Ensuring AI-generated content is identifiable when shared externally
- Providing guidance to staff on communicating AI use to clients and external parties

5. Critical Controls

The AGS framework includes a defined set of critical controls, representing the minimum baseline required for responsible AI governance.

All critical controls must be met in order to achieve certification.

Failure to meet one or more critical controls will result in the organisation being placed into Review or Not Certified, depending on the nature of the gap.

5.1 Purpose of Critical Controls

Critical controls are designed to address the most significant and immediate risks associated with AI use.

These include:

- absence of governance or policy
- lack of accountability

- unverified use of AI outputs
- exposure of sensitive information
- uncontrolled or unmonitored AI use

These controls establish a minimum viable governance framework, below which certification cannot be granted.

5.2 Critical Control Areas

The critical controls align to the core principles of the AGS framework and cover the following areas:

- Existence of a documented AI policy
- Accessibility of governance and guidance to staff
- Defined acceptable and prohibited uses of AI
- Assignment of responsibility for oversight
- Retention of human accountability for outputs
- Verification of AI-generated outputs before use
- Protection of sensitive organisational and client information

5.3 Relationship to Assessment

Each critical control is assessed through a corresponding question within the AGS assessment.

Organisations must confirm that each of these controls is in place.

Where a critical control is not met:

- the organisation may be required to implement the control, or
- provide clarification during the review process

6. Assessment Model

Assessment under AGS is based on a structured set of control-based questions.

Organisations are required to confirm whether each control is in place through Yes / No responses.

The assessment includes:

- A set of critical controls, which must be met in all cases
- A broader set of scored controls, which determine overall performance

Certification requires that:

- all critical controls are met, and
- a high proportion of remaining controls are achieved

7. Certification Outcomes

Organisations will receive one of the following outcomes:

- AGS Verified — where all critical controls are met and the required threshold is achieved
- Review Required — where clarification or remediation is needed
- Not Certified — where significant gaps are identified

8. Review and Validation

Where required, organisations may be asked to provide additional information to support their responses.

The review process is proportionate and focused on confirming the presence and application of governance controls, rather than conducting a full audit.

9. Definitions

A separate Definitions section forms part of this standard and provides clarity on key terms used throughout the document.

10. Relationship to Assessment Questions

The AGS assessment questionnaire is derived directly from the control requirements set out in this document.

Each question maps to one or more control requirements within the framework.

Organisations should refer to the assessment questionnaire for the practical application of this standard.