AI Security & Compliance

CONTROL	STATUS
AI system impact assessment The organisation shall perform AI system impact assessments according to 6.1.4 at planned intervals or when significant changes are proposed to occur. The organisation shall retain documented information of the results of all AI system impact assessments.	✓
Determining the scope of the AI management system The organisation shall determine the boundaries and applicability of the AI management system to establish its scope. When determining this scope, the organisation shall consider: ▪ the external and internal issues referred to in 4.1; ▪ the requirements referred to in 4.2. The scope shall be available as documented information. The scope of the AI management system shall determine the organization's activities with respect to this document's requirements on the AI management system, leadership, planning, support, operation, performance, evaluation, improvement, controls and objectives.	✓
AI objectives and planning The organisation shall establish AI objectives at relevant functions and levels. The AI objectives shall: a) be consistent with the AI policy (see 5.2); b) be measurable (if practicable); c) take into account applicable requirements; d) be monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information. When planning how to achieve its AI objectives, the organisation shall determine: ▪ what will be done; ▪ what resources will be required; ▪ who will be responsible; ▪ when it will be completed; ▪ how the results will be evaluated. NOTE A non-exclusive list of AI objectives relating to risk management is provided in Annex C. Control objectives and controls for identifying objectives for responsible development and use of AI systems and measures to achieve them are provided in A.6.1 and A.9.3 in Table A.1. Implementation guidance for these controls is provided in B.6.1 and B.9.3.	✓
Monitoring, measurement, analysis The organisation shall determine: ▪ what needs to be monitored and measured; ▪ the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results; ▪ when the monitoring and measuring shall be performed; ▪ when the results from monitoring and measurement shall be analysed and evaluated. Documented information shall be available as evidence of the results. The organisation shall evaluate the performance and the effectiveness of the AI management system.	✓

General
The organisation shall conduct internal audits at planned intervals to provide information on whether the AI management system:

a) conforms to:
   - the organisation's own requirements for its AI management system;
   - the requirements of this document;

b) is effectively implemented and maintained.

Continual improvement
The organisation shall continually improve the suitability, adequacy and effectiveness of the AI management system.

Nonconformity and corrective action
When a nonconformity occurs, the organisation shall:

a) react to the nonconformity and as applicable:
   - take action to control and correct it;
   - deal with the consequences;

b) evaluate the need for action to eliminate the cause(s) of the nonconformity, so that it does not recur or occur elsewhere, by:

d) review the effectiveness of any corrective action taken;

e) make changes to the AI management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.
Documented information shall be available as evidence of:
   - the nature of the nonconformities and any subsequent actions taken;
   - the results of any corrective action.

AI policy
The organisation should document a policy for the development or use of AI systems.

External reporting
The organisation should provide capabilities for interested parties to report adverse impacts of the system.

Communication of incidents
The organisation should determine and document a plan for communicating incidents to users of the system.

Information for interested parties
The organisation should determine and document its obligations to reporting information about the AI system to interested parties.

Processes for responsible use of AI
The organisation should define and document the processes for the responsible use of AI systems.

Objectives for responsible use of AI
The organisation should identify and document objectives to guide the responsible use of AI systems.

Intended use of the AI system
The organisation should ensure that the AI system is used according to the intended uses of the AI system and its accompanying documentation.

Allocating Responsibilities

The organisation should ensure that responsibilities within their AI system life cycle are allocated between the organisation, its partners, suppliers, customers and third parties.

Data resources

As part of resource identification, the organisation should document information about the data resources utilised for the AI system. Documentation on data should include, but is not limited to, the following topics:

- the provenance of the data;
- the date that the data were last updated or modified (e.g. date tag in metadata);
- for machine learning, the categories of data (e.g. training, validation, test and production data);
- categories of data (e.g. as defined in ISO/IEC -1);
- process for labelling data;
- intended use of the data;
- quality of data (e.g. as described in the ISO/IEC 5259 series);
- applicable data retention and disposal policies;
- known or potential bias issues in the data;
- data preparation.

Understanding the organisation and its context

The organisation shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended result(s) of its AI management system. The organisation shall determine whether climate change is a relevant issue. The organisation shall consider the intended purpose of the AI systems that are developed, provided or used by the organisation. The organisation shall determine its roles with respect to these AI systems.

Understanding the needs and expectations of interested

The organisation shall determine:

- the interested parties that are relevant to the AI management system;
- the relevant requirements of these interested parties;
- which of these requirements will be addressed through the AI management system.

AI management system

The organisation shall establish, implement, maintain, continually improve and document an AI management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the AI management system by:

- ensuring that the AI policy (see 5.2) and AI objectives (see 6.2) are established and are compatible with the strategic direction of the organisation;
- ensuring the integration of the AI management system requirements into the organisation's business processes;
- ensuring that the resources needed for the AI management system are available;
- communicating the importance of effective AI management and of conforming to the AI management system requirement;
- ensuring that the AI management system achieves its intended result(s);
- directing and supporting persons to contribute to the effectiveness of the AI management system;
- promoting continual improvement;
- supporting other relevant roles to demonstrate their leadership as it applies to their areas of responsibility.

AI policy

Top management shall establish an AI policy that:

a) is appropriate to the purpose of the organisation;
b) provides a framework for setting AI objectives (see 6.2);
c) includes a commitment to meet applicable requirements;
d) includes a commitment to continual improvement of the AI management system.

The AI policy shall:

- be available as documented information;
- refer as relevant to other organisational policies;
- be communicated within the organisation;
- be available to interested parties, as appropriate.

Control objectives and controls for establishing an AI policy are provided in A.2 in Table A.1. Implementation guidance for these controls is provided in B.2.

Roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization. Top management shall assign the responsibility and authority for:

a) ensuring that the AI management system conforms to the requirements of this document;
b) reporting on the performance of the AI management system to top management.

Awareness

Persons doing work under the organisation's control shall be aware of:

- the AI policy (see 5.2);
- their contribution to the effectiveness of the AI management system, including the benefits of improved AI performance;
- the implications of not conforming with the AI management system requirements.

Communication

The organisation shall determine the internal and external communications relevant to the AI management system including:

- what it will communicate;
- when to communicate;
- with whom to communicate;
- how to communicate.

General

The organisation's AI management system shall include:

a) documented information required by this document;
b) documented information determined by the organisation as being necessary for the effectiveness of the AI management system.

Creating and updating

When creating and updating documented information, the organisation shall ensure appropriate:

- identification and description (e.g. a title, date, author or reference number);
- format (e.g. language, software version, graphics) and media (e.g. paper, electronic);
- review and approval for suitability and adequacy.

AI risk treatment
The organisation shall implement the AI risk treatment plan according to 6.1.3 and verify its effectiveness. When risk assessments identify new risks that require treatment, a risk treatment process in accordance with 6.1.3 shall be performed for these risks. When risk treatment options as defined by the risk treatment plan are not effective, these treatment options shall be reviewed and revalidated following the risk treatment process according to 6.1.3 and the risk treatment plan shall be updated. The organisation shall retain documented information of the results of all AI risk treatments.

Internal audit programme
The organisation shall plan, establish, implement and maintain (an) audit programme(s), including the frequency, methods, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organisation shall consider the importance of the processes concerned and the results of previous audits.

The organisation shall:

a) define the audit objectives, criteria and scope for each audit;
b) select auditors and conduct audits to ensure objectivity and the impartiality of the audit process;
c) ensure that the results of audits are reported to relevant managers.

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

General Management Review
Top management shall review the organisation's AI management system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness.

Management review inputs
The management review shall include:

a) the status of actions from previous management reviews;
b) changes in external and internal issues that are relevant to the AI management system;
c) changes in needs and expectations of interested parties that are relevant to the AI management system;
d) information on the AI management system performance, including trends in:
   - nonconformities and corrective actions;
   - monitoring and measurement results;
   - audit results;

e) opportunities for continual improvement.

Management review results
The results of the management review shall include decisions related to continual improvement opportunities and any need for changes to the AI management system. Documented information shall be available as evidence of the results of management reviews.

Alignment with other organisational policies
The organisation should determine where other policies can be affected by or apply to, the organisation's objectives with respect to AI systems.

Review of the AI policy
The AI policy should be reviewed at planned intervals or additionally as needed to ensure its continuing suitability, adequacy and effectiveness.

Reporting of concerns
The organisation should define and put in place a process to report concerns about the organisation's role with respect to an AI system throughout its life cycle.

Resources
The organisation shall determine and provide the resources needed for the establishment, implementation, maintenance and continual improvement of the AI management system.

Competence
The organisation shall:

- determine the necessary competence of person(s) doing work under its control that affects its AI performance;
- ensure that these persons are competent on the basis of appropriate education, training or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken.

Appropriate documented information shall be available as evidence of competence.

Control of documented information
Documented information required by the AI management system and by this document shall be controlled to ensure:

a) it is available and suitable for use, where and when it is needed;
b) it is adequately protected (e.g. from loss of confidentiality, improper use or loss of integrity).

For the control of documented information, the organisation shall address the following activities, as applicable:

- distribution, access, retrieval and use;
- storage and preservation, including preservation of legibility;
- control of changes (e.g. version control);
- retention and disposition.

Documented information of external origin determined by the organisation to be necessary for the planning and operation of the AI management system shall be identified as appropriate and controlled.

NOTE
Access can imply a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information.

General
When planning for the AI management system, the organisation shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed to:

- give assurance that the AI management system can achieve its intended result(s);
- prevent or reduce undesired effects;
- — achieve continual improvement.

The organisation shall establish and maintain AI risk criteria that support:

- distinguishing acceptable from non-acceptable risks;
- performing AI risk assessments;
- conducting AI risk treatment;
- assessing AI risk impacts.

AI risk assessment
The organisation shall define and establish an AI risk assessment process that:

- a) is informed by and aligned with the AI policy (see 5.2) and AI objectives (see 6.2);

AI risk treatment
Taking the risk assessment results into account, the organisation shall define an AI risk treatment process to:

a) select appropriate AI risk treatment options;
b) determine all controls that are necessary to implement the AI risk treatment options chosen and compare the controls with those in Annex A to verify that no necessary controls have been omitted;

AI risk assessment
The organisation shall perform AI risk assessments in accordance with 6.1.2 at planned intervals or when significant changes are proposed or occur. The organisation shall retain documented information of the results of all AI risk assessments.

AI system verification and validation
The organisation should define and document verification and validation measures for the AI system and specify criteria for their use.

AI system deployment
The organisation should document a deployment plan and ensure that appropriate requirements are met prior to deployment.

AI system recording of event logs
The organisation should determine at which phases of the AI system life cycle, record keeping of event logs should be enabled, but at the minimum when the AI system is in use.

Acquisition of data
The organisation should determine and document details about the acquisition and selection of the data used in AI systems.

Quality of data for AI systems
The organisation should define and document requirements for data quality and ensure that data used to develop and operate the AI system meet those requirements.

System documentation and information
The organisation should determine and provide the necessary information to users of the system.