The AI Management Essentials Tool (AIME) - Overview and Status

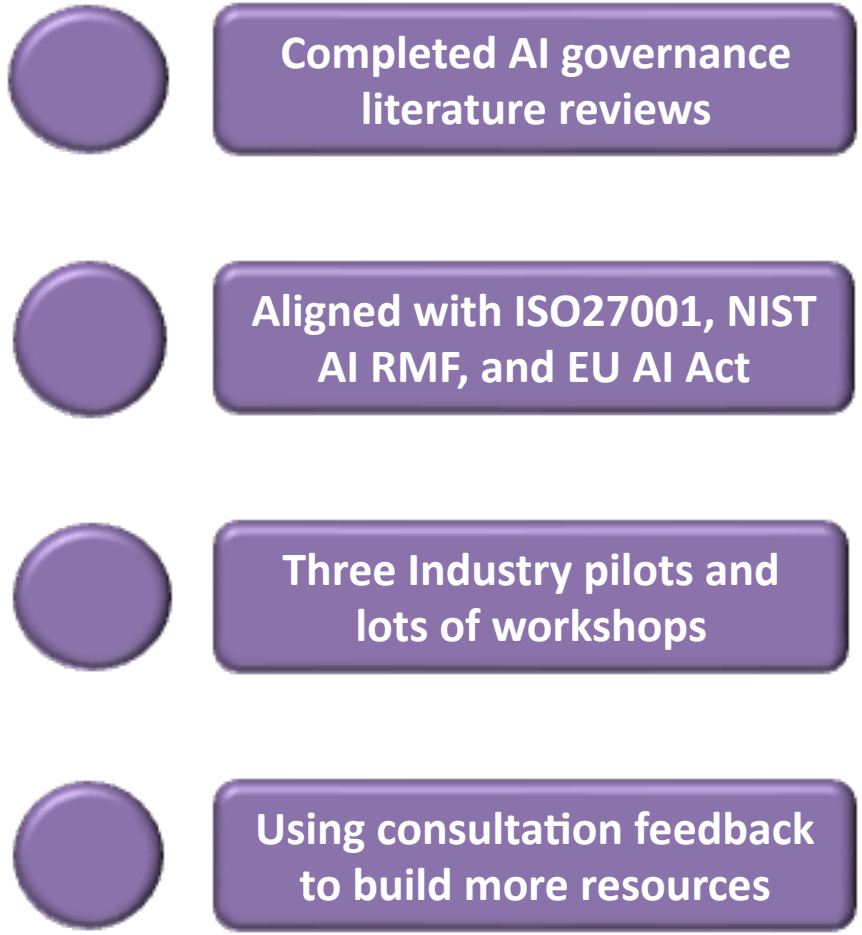
- **Sponsor:** UK Department for Science, Innovation and Technology (DSIT). Link to the original AIME materials.
- **Purpose:** To help organisations assess and improve their AI governance and management processes.
- **Target Audience:** Primarily small to medium-sized enterprises (SMEs) and other firms struggling to navigate AI management standards.
- **Current and Expected Status:** Draft self-assessment, likely to be recommended rather than mandatory.
- **Published 6th November 2024** as an open consultation.
- **Consultation closed 21st January 2025** and responses are under review.

Infospectives™

AIME Background

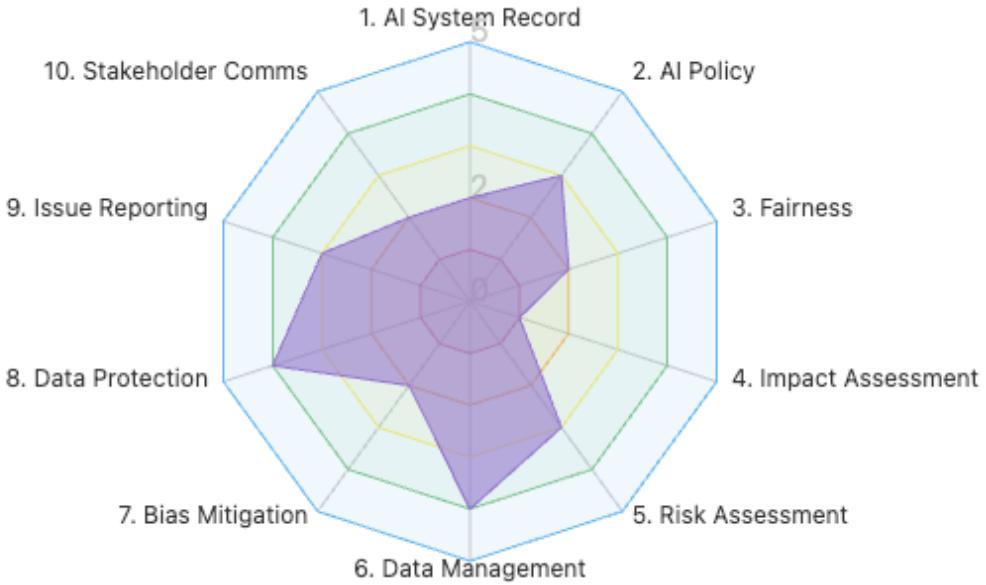
The AIME questionnaire was developed after:

- A **literature review** of current AI frameworks
- Focus on three prominent international frameworks:
  - **ISO/IEC 42001** AI Management System standard
  - **NIST AI Risk Management framework**
  - **EU AI Act**
- Identification of three main areas for self-assessment:
  - **Internal Processes**
  - **Managing Risks**
  - **Communication**



AI Management Maturity Matrix for AI Management Essentials Alignment

A proposed maturity matrix* covering the ten question subsets in the AIME questionnaire. Indicating maturity across five levels.



*This is not part of AIME materials, this is original Infospectives Ltd content based on AIME and historical maturity frameworks.

Level	Name	Description
1	**Initial**	Basic or ad-hoc practices with minimal documentation, no formal processes, and reactive approaches. Limited awareness of AI governance requirements.
2	**Developing**	Some documented practices exist but may be inconsistent. Key governance elements beginning to be implemented but with gaps. Processes are partially defined.
3	**Established**	Formal documented processes covering most key areas. Regular reviews occur but may lack comprehensive coverage. Consistent implementation across most systems.
4	**Advanced**	Well-defined, comprehensive processes with regular reviews and updates. Proactive management with preventative measures. Integration with broader organisational governance.
5	**Optimised**	Comprehensive governance with continuous improvement mechanisms. Leading practices are embedded across the organisation. Metrics-driven approach with predictive capabilities.

But more on that in a minute

AIME Structure

The AIME framework consists of 10 sections of questions, split into the 3 high-level focus areas defined by the AIME working groups:

Internal Processes

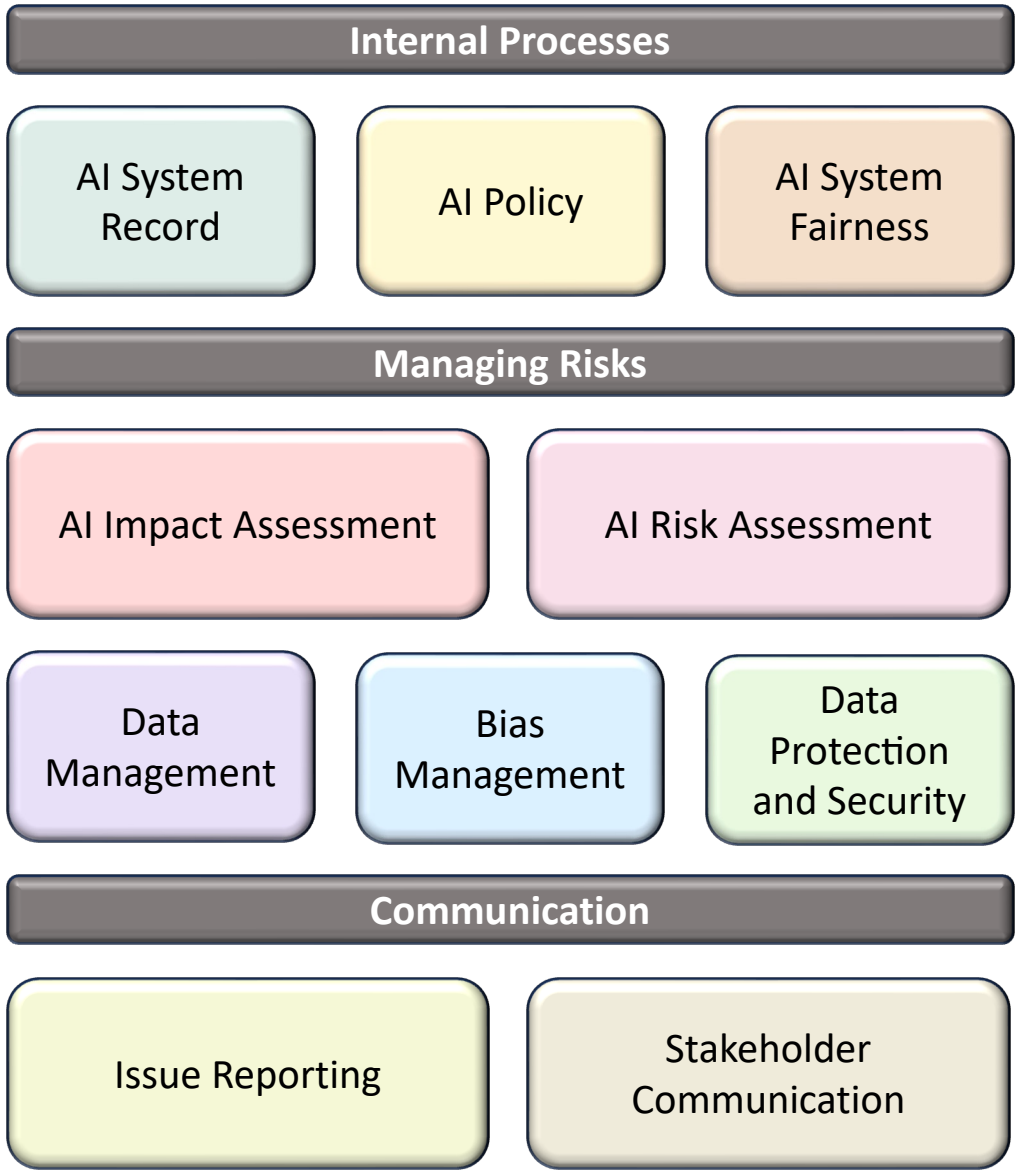
1. AI System Record
2. AI Policy
3. AI System Fairness

Managing Risks

4. AI Impact Assessment
5. Risk Assessment
6. Data Management
7. Bias Identification and Mitigation
8. Data Protection and Security

Communication

9. Issue Reporting
10. Stakeholder Communication



Breaking AIME Down

How we broke down AI Management Essentials content:

- Close reading of the AIME documentation
- Adding actionable objectives and more control context
- Identifying potential supporting evidence
- Mapping to existing governance provision

Updates to existing governance materials:

- Minor amendments to pre-existing AI Use Case Triage and other governance intake materials
- Creation of a maturity model for AIME alignment

ID	AIME Question Objective*	AIME Statement / Question
1	**AI System Record**	**We maintain a complete and up-to-date record of all the AI systems our organisation develops and uses**
1.1	AI System record exists	Do you maintain a record of the AI systems your organisation develops and uses?
1.2	AI System record complete	What proportion of the AI systems that you develop and use are documented in your AI system record?

AIME Section	Potential Supporting Evidence / Assessment*
1. AI System Record	**Centralised AI System Inventory / Database** - Unique system identifiers - System descriptions/specs - Development/deployment dates - Risk classifications - Version history - Documentation links….

***AIME Question Objectives** and **Potential Supporting Evidence / Assessment** content is not part of current official AIME materials. It was was derived by Infospectives Ltd from the **AIME Statements / Questions.**

ID	AIME Question Objective*	AIME Statement / Question
1	**AI System Record**	**We maintain a complete and up-to-date record of all the AI systems our organisation develops and uses**
1.1	AI System record exists	Do you maintain a record of the AI systems your organisation develops and uses?
1.2	AI System record complete	What proportion of the AI systems that you develop and use are documented in your AI system record?
1.3	AI System record maintained	Do you have an established process for adding new systems to your AI system record?
1.4	Third party elements documented	If you procure or access AI systems from third party providers, do you request and receive documentation assets and resources for your AI system record from them?
1.5	AI System record reviewed and updated	How frequently do you review and update your AI system record?
2	**AI Policy**	**We have a clear, accessible and suitable AI policy for our organisation**
2.1	AI policy exists	Do you have an AI policy for your organisation?
2.2	AI policy distributed	Is your AI policy available and accessible to all employees?
2.3	Supports AI fitness for purpose assessment	Does your AI policy help users evaluate whether the use of an AI is appropriate for a given function or task?
2.4	Includes AI roles and responsibilities	Does your AI policy identify clear roles and responsibilities for AI management processes in your organisation?
2.5	AI policy reviewed and updated	How frequently do you review and update your AI policy?
3	**AI System Fairness**	**We seek to ensure that the AI systems we develop and use which directly impact individuals are fair**
3.1	Identified potential direct impact on individuals	Do you develop or use AI systems that directly impact individuals?
3.2	Established fairness definitions	Do you have clear definitions of fairness with respect to these AI systems?
3.3	Identified potentially unfair outcomes	Do you have mechanisms for detecting or identifying unfair outcomes or processes with respect to these AI systems and your definitions of fairness?
3.4	Monitors fairness and mitigates issues	Do you have processes for monitoring fairness of AI systems over time and mitigating against unfairness?
3.5	Fairness assurance processes reviewed and updated	How frequently do you review your process(es) for detecting and mitigating unfairness?

AIME Section	Potential Supporting Evidence / Assessment*
1. AI System Record	**Centralised AI System Inventory / Database** - Unique system identifiers - System descriptions/specs - Development/deployment dates - Risk classifications - Version history - Documentation links - Written maintenance procedures - Automated review notifications - Change logs - Review meeting minutes - Third-party system specifications and integration docs - Change management documentation - Third-party risk assessment results - System architecture diagrams - Data lineage documentation
2. AI Policy	**AI Governance Policy and Processes -** Scope and objectives - Roles and responsibilities - Risk appetite and prohibitions for AI usage - Risk assessment requirements - Development standards - Testing protocols - Deployment criteria - Monitoring requirements - Distribution logs - Policy related training distribution and training records - Review minutes - Version control - Awareness metrics - Decision frameworks - Escalation procedures - Cross-reference to other organisational policies
3. Fairness	**Fairness Documentation and Assessment Framework** – Log of potential direct AI system impact on individuals - Written fairness definitions - System-specific metrics - Testing protocols/results - Bias measurements - Impact assessments - Demographic analyses - Feedback and consultation records - Monitoring reports - Mitigation records - Review audit trails - Baseline fairness metrics - Automated fairness monitoring outputs - Post-deployment fairness evaluations - Stakeholder consultation records - Independent fairness audit reports

ID	AIME Question Objective*	AIME Statement / Question
4	**AI Impact Assessment**	**We have identified and documented the possible impacts of the AI systems our organisation develops and uses**
4.1	Impact Assessment Exists with Appropriate Scope	Where appropriate do you have an impact assessment process for identifying how your AI systems might impact...
4.1.1	Includes potential legal and life opportunity impacts	The legal position or life opportunities of individuals?
4.1.2	Includes physical or psychological wellbeing impacts	The physical or psychological wellbeing of individuals?
4.1.3	Includes human rights impacts	Universal human rights?
4.1.4	Includes societal and environmental impacts	Societies and the environment?
4.2	Potential AI system impacts documented	Do you document potential impacts of your AI systems?
4.3	Potential impacts communicated to AI users and customers	Do you communicate the potential impacts to the users or customers of your AI systems?
5	**Risk Assessment**	**We effectively manage any risks caused by our AI systems**
5.1	Risk assessments conducted	Do you conduct risk assessments of the AI systems you develop and use?
5.2	Risk Assessment Design Fit for Purpose	Risk Assessment Design
5.2.1	Outputs consistent, valid, and comparable	Are your risk assessments designed to produce consistent valid and comparable results?
5.2.2	Integrated with organisational risk benchmarks and appetite	Do you compare the results of your risk assessments to your organisation's overall risk thresholds?
5.2.3	Outputs used to prioritise risk treatment	Do you use the results of your risk assessment to prioritise risk treatment?
5.3	Monitoring Systems In Place and Working	System Monitoring Design and Capability
5.3.1	Monitoring general errors and failures	Do you monitor all your AI systems for general errors and failures?
5.3.2	Monitoring for [performance issues	Do you monitor all your AI systems to check that they are performing as expected?
5.4	Responding to alerts and investigating / fixing Issues	Do you have processes for responding to or repairing system failures?
5.5	Defined thresholds or conditions to cease AI use	Have you defined risk thresholds or critical conditions under which it would become necessary to cease the development or use of your AI systems?
5.6	Risk assessments reviewed and updated	Do you have a plan to introduce necessary updates to your risk assessment process as your AI systems evolve or critical issues are identified?

AIME Section	Potential Supporting Evidence / Assessment*
4. Impact Assessment	**Impact Assessment Framework** - Legal impact analysis - Human rights assessment - Health/safety evaluation - Environmental impact assessment - Societal impact analysis - Stakeholder consultation - Mitigation plans - Communication materials - Review logs - Comparative impact analysis - Severity and likelihood benchmarks - Stakeholder impact matrices - Remediation plans - Threshold criteria
5. Risk Assessment	**Risk Management Framework** - Assessment framework - System-specific assessments - Risk benchmarks - Control evaluations - Treatment plans - Monitoring dashboards - Incident procedures - Failure logs - Threshold definitions - Review minutes - Risk appetite statements - Risk acceptance records - Automated monitoring dashboards/screenshots - Key risk indicators (KRIs) - Incident response test results

ID	AIME Question Objective*	AIME Statement / Question
6	**Data Management**	**We responsibly manage the data used to train, fine-tune and otherwise develop our AI systems**
6.1	Identifying work to fine tune and develop AI systems	Do you train fine-tune or otherwise develop your own AI systems using data?
6.2	Able to evidence data provenance	Do you document details about the provenance and collection processes of data used to develop your AI systems?
6.3	Able to evidence data quality requirements and assessment	Do you ensure that the data used to develop your AI systems meet any data quality requirements defined by your organisation?
6.4	Able to evidence data completeness and representativeness	Do you ensure that datasets used to develop your AI systems are adequately complete and representative?
6.5	Data preparation activities documented	Do you document details about the data preparation activities undertaken to develop your AI systems?
6.6	Contracts with third parties processing personal data	Do you sign and retain written contracts with third parties that process personal data on your behalf?
7	**Bias Identification and Mitigation**	**We mitigate against foreseeable, harmful and unfair algorithmic and data biases in our AI systems**
7.1	Action taken to mitigate foreseeable harms and bias	Do you take action to mitigate against foreseeable harmful or unfair bias related to the training data of your AI systems?
7.2	Training data records for procured AI as a Service or Pre-trained models	If you procure AI as a Service (AIaaS) or pretrained AI systems from third party providers to use or develop upon do you have records of the full extent of the data that has been used to train these systems?
7.3	Appropriate bias due diligence for AIaaS and other procured AI	If you procure AIaaS or pretrained AI systems from third party providers, do you conduct appropriate due diligence on the data used to train or develop these systems to mitigate against foreseeable harmful or unfair bias?
7.4	Capability to comply with Bias assessment and mitigation requirements	Do you have processes to ensure compliance with relevant bias mitigation measures stipulated by international or domestic regulation?
8	**Data Protection and Security**	**We have a 'data protection by design and default' approach throughout the development and use of our AI systems**
8.1	Appropriate security measures to protect personal data	Do you implement appropriate security measures to protect the data used and/or generated by your AI systems?
8.2	All personal data breaches recorded	Do you record all your personal data breaches?
8.3	Compliant data subject breach notification	Do you report personal data breaches to affected data subjects when necessary?
8.4	Appropriate scoping for DPIAs and DPIA completion	Do you routinely complete Data Protection Impact Assessments (DPIAs) for uses of personal data that are likely to result in high risk to individuals' interests?
8.5	AI systems and data protected from third party interference	Have you ensured that all your AI systems and the data they use or generate is protected from interference by third parties?

AIME Section	Potential Supporting Evidence / Assessment*
6. Data Management	**Data Governance Framework** - Dataset provenance docs - Model Cards / AIBOMs - Collection methods - Quality metrics/standards - Completeness assessments - Representation analysis - Processing logs - Third-party agreements - Data Protection assessments - Data pipeline diagrams - Data quality scorecards - Data retention schedules - Data minimisation assessments - Data sharing agreements
7. Bias Identification and Mitigation	**Bias Assessment Framework** - Detection test results - Protected attribute analysis - Demographic studies - Mitigation strategies - Due diligence records - Compliance documentation - Bias mitigation algorithm documentation - Pre/post mitigation comparison metrics - Cross-demographic performance metrics - Vendor bias attestations - Bias monitoring frequency documentation
8. Data Protection and Security	**Data Protection and Security Controls Framework** - AI system security measures documentation - System-specific security controls inventory - Personal data breach register - Breach notification procedures & templates -- ROPA template - Completed ROPA - Data Flows - DPIA template - Completed DPIAs for high-risk AI processing - Third-party inference protection measures - System access controls documentation - Data integrity verification procedures - Data mapping documentation - Privacy notices - Data minimisation strategies - Access control matrices - Technical security reports

ID	AIME Question Objective*	AIME Statement / Question
9	**Issue Reporting**	**We have reporting mechanisms for employees, users and external third parties to report any failures or negative impacts of our AI systems**
9.1	Employee and third-party issue reporting mechanisms in place	Do you have reporting mechanisms for all employees, users and external third parties to report concerns or system failures?
9.2	Options for anonymous and / or confidential reporting available	Do you provide reporters with options for either anonymity or confidentiality or both?
9.3	Effective escalation routes and responsible stakeholders confirmed	Have you identified who in your organisation will be responsible for addressing concerns when they are escalated?
9.4	Transparent reporting procedures for employees and third parties	Are your reporting procedures meaningfully transparent for all employees, users and external third parties?
9.5	Timely response to issues or concerns	Do you respond to concerns in a timely manner?
9.6	All reported concerns and investigations documented	Do you document all reported concerns and results of any subsequent investigations?
10	**Stakeholder Communication**	**We tell every interested party how to use our AI systems safely and what the systems' requirements are**
10.1	Technical documentation requirements confirmed	Have you determined what AI system technical documentation is required by interested parties across your relevant stakeholder categories?
10.2	Documents can be delivered in appropriate formats	Do you provide technical documentation to interested parties in an appropriate format?
10.3	Non-technical documentation requirements confirmed	Have you determined what AI system non-technical documentation is required by interested parties across your relevant stakeholder categories?
10.4	Non-technical documentation delivered to relevant parties	Do you provide non-technical information to your users and other relevant parties?

AIME Section	Potential Supporting Evidence / Assessment*
9. Issue Reporting	**Incident, Event, and Issue Management** - System documentation - Anonymous channels - Issue tracking - Response procedures - Escalation protocols - Investigation templates - Response metrics - Resolution logs - Communication templates - Handler training - Response time metrics - Issue categorisation frameworks - Severity assessment criteria - Feedback loop documentation - Post-resolution follow-up procedures
10. Stakeholder Communication	**Documentation for Stakeholders** - Stakeholder analysis - Requirements matrix - Technical docs - System architecture - API specifications - User manuals - Non-technical docs - Review logs - Distribution records - Stakeholder mapping documentation - Documentation delivery confirmation records - Documentation effectiveness assessments - Documentation update frequency records - Translation or accessibility provisions

Infospectives™

*__AIME Question Objectives__ and __Potential Supporting Evidence / Assessment__ content is not part of current official AIME materials. It was derived by Infospectives Ltd from __AIME Statements / Questions__ copied from published AIME documents (Link) which include useful definitions, examples, and FAQs.

You can’t govern what you can’t see

Why Start With AIME? - You need a starting point and an aiming point

AIME is a solid AI governance foundation and signpost for future control and capability. Discovery to understand the scope and nature of AI built or used is always going to be a first step. Our AI Use Case Triage (next page) is built from the same blocks. A low overhead way to make a start (AIME Section 1).

"It is not most about AI systems, it is most about data and AI usage context"

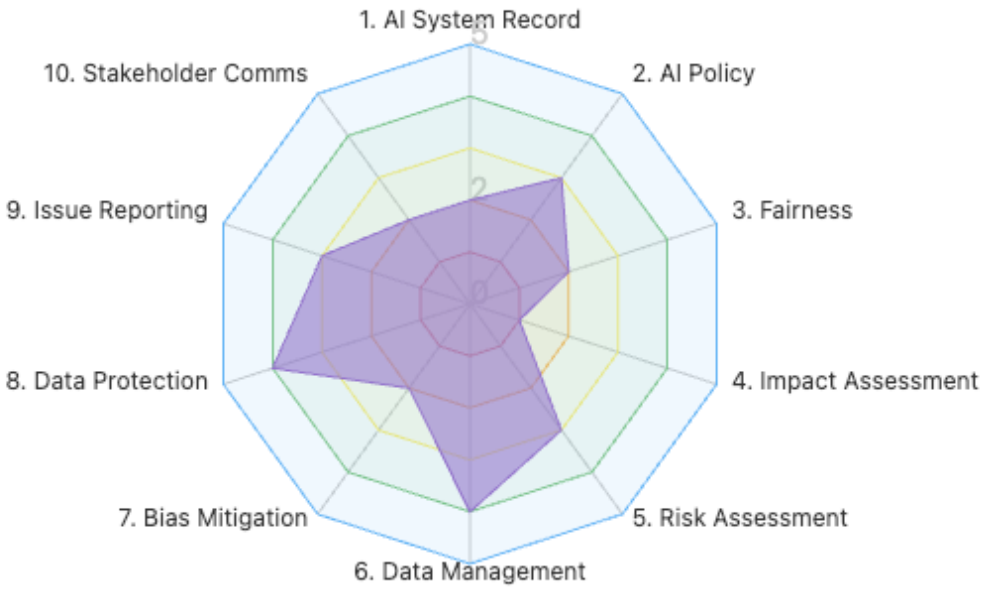
- What is in use or planned, with which data, people, and technology?
- What is the expected value-add, efficiency gain, or cost reduction?
- Involving which 3rd parties, accountable people, and other stakeholders?
- With what kind of future usage scope, scale, and frequency?
- With what kind of trade offs for staff, operations, and others impacted?
- With what kind of integration, monitoring, and support challenges?

AI Use Case Triage Overview

1. A 30 minute AI use case survey to understand current and proposed scope. Tailored for technical and non-technical stakeholders.
2. Integrating legal and regulatory criteria. AI Management Essentials aligned threshold checks and information to kick start work towards alignment with the EU AI Act, GDPR DPIA requirements, ISO42001/42005, or NIST AI Risk Management Framework.
3. Thresholds, FAQs, and training for common criteria (applicable to common risks, scoping benchmarks, or policy requirements) to support some response standardisation and improve broader AI and AI governance literacy:
    - ROI, risk and impact indicators
    - Geographical / internal / external usage scope
    - Usage scale and frequency
    - Input data quality / coverage / sensitivity
    - AI complexity / integration complexity / knowledge scarcity
    - Autonomy level
    - Potential ethical complexity
4. Output validation and feedback effort estimates to inform plans and continuous development.
5. AI Use Case Inventory and summarised findings and recommendations.
6. Structured individual and aggregate use case profiles that are easy to iteratively update. Informing priorities, training requirements, specialist follow up, project plans, strategic plans, and creating or updating AI policies and codes of ethics.

AI Management Maturity Matrix for AI Management Essentials Alignment

A proposed maturity matrix* covering the ten question subsets in the AIME questionnaire. Indicating maturity across five levels.



*This is not part of AIME materials, this is original Infospectives Ltd content based on AIME and historical maturity frameworks.

Level	Name	Description
1	**Initial**	Basic or ad-hoc practices with minimal documentation, no formal processes, and reactive approaches. Limited awareness of AI governance requirements.
2	**Developing**	Some documented practices exist but may be inconsistent. Key governance elements beginning to be implemented but with gaps. Processes are partially defined.
3	**Established**	Formal documented processes covering most key areas. Regular reviews occur but may lack comprehensive coverage. Consistent implementation across most systems.
4	**Advanced**	Well-defined, comprehensive processes with regular reviews and updates. Proactive management with preventative measures. Integration with broader organisational governance.
5	**Optimised**	Comprehensive governance with continuous improvement mechanisms. Leading practices are embedded across the organisation. Metrics-driven approach with predictive capabilities.

Sample Maturity Breakdown by AIME Section

1. AI System Record Management

Level	Maturity Indicators
1	Some AI systems and AI uses are informally tracked but with no centralised record. Documentation is minimal or inconsistent. No process for updating records.
2	Basic inventory of major AI systems and use cases exists, but may be incomplete. Limited documentation standards. Ad-hoc updates to the system record. Minimal detail about third parties.
3	Formal record exists for most AI systems and AI use cases, with defined documentation standards. Regular review process in place. Third-party system details are included.
4	Comprehensive record of all AI systems and use cases with detailed documentation. Established process for adding new systems and uses. Consistent documentation from third parties. Bi-annual reviews.
5	Complete and continuously updated record with automated tracking. Advanced metadata and relationship mapping. Third-party documentation fully integrated. Regular reviews drive improvement.

My Next Steps

- Watching for updates to the AIME tool and associated standards
- Evolving the AIME maturity model and testing on willing victims
- Exploring more potential AIME benchmarks and examples of evidence
- Testing and refining the AI Use Case Triage in more usage contexts
- Reviewing FAQs and training materials to make sure they stay user friendly
- Creating space for more people interested in AI to be comfortably clueless

Getting In touch: Sarah.Clarke@Infospectives.co.uk Linkedin.com/in/infospectives

About the Author

Sarah Clarke, Owner, Infospectives Ltd

Sarah is an experienced GRC (Governance, Risk, and Compliance) specialist with substantial practical insight into governance for data protection, security, and novel technology. She is the owner of Infospectives Ltd, specialising in strategic consultancy to improve and mature related assurance.

- Contributor to the **IEEE P3119** public sector AI procurement standard
- Member of the **Women in AI Governance** initiative
- Technology Governance Specialist for the **World Ethical Data Foundation**
- Emeritus Fellow and former Director of **For Humanity**, a not-for-profit defining AI audit criteria
- Guest lecturer on supplier security governance for Manchester University
- One of **Computer Weekly's most influential women in UK tech** 2022, 2023, 2024
- Past contributor to the IASME **Cyber Essentials** Standard