emite
A PROPHECY SOLUTION

Understanding Data and AI Governance:

A Practical Guide to Frameworks, Standards and Expectations

A positive, practical guide to making sense of global data and AI governance frameworks

Organisations today are investing heavily in data, analytics and AI to improve decision-making, automate processes and unlock new opportunities.

These technologies are powerful. They can connect information across systems, surface insights faster and make advanced analysis accessible to more people across the business.

At the same time, they introduce an important question:

How do we ensure that the information and outputs we rely on are trustworthy, explainable and used appropriately?

This is where governance frameworks and standards come in.

Across industries and regions, a growing number of global frameworks, such as DAMA-DMBOK, ISO standards, COBIT, NIST and the EU AI Act, are helping organisations define what responsible data and AI use looks like in practice.

For many teams, however, the landscape can feel complex:

- Which frameworks are relevant?
- How do they differ?
- Do we need to adopt all of them?
- How do they apply to everyday reporting, analytics and AI use?

This document is designed as a practical guide to help answer those questions.

It explains the purpose of key global frameworks, highlights the common expectations they share and outlines how organisations can build a governance approach that supports both innovation and accountability.

Rather than viewing governance as a barrier, this guide treats it as an enabler, helping organisations use data and AI with greater confidence, clarity and consistency.

Trust is built before the dashboard

Most reporting problems do not begin in the dashboard.

They begin further upstream.

They begin when two applications define the same measure differently.

They begin when data is extracted without documenting which records were excluded.

They begin when a spreadsheet becomes an unofficial source of truth.

They begin when a KPI changes but the calculation is not updated consistently across reports.

They begin when data ownership is unclear and no one is responsible for validating quality.

They begin when an AI application is given access to information without an agreed purpose, risk assessment or review process.

By the time the information reaches a dashboard, many decisions have already been made:

- which systems should be treated as authoritative
- which data should be included
- how records should be matched
- how information should be transformed
- how business terms should be defined
- which users should have access
- how frequently the information should be updated
- what validation should occur
- how exceptions should be handled

If those decisions are undocumented or inconsistently applied, a polished dashboard can create confidence without creating certainty.

The information may look authoritative while still being difficult to validate, reproduce or explain.

This is why data confidence cannot be created through presentation alone.

It must be designed into the process.

More technology creates more process decisions

The average organisation now manages approximately **957 applications**, but only **27% are connected.**

Every application can introduce another source of data, another integration, another access model and another way of defining performance.

This creates a significant process challenge.

Which system owns the customer record?

Which system provides the definitive interaction time?

Which version of revenue should be used?

How should records be matched across platforms?

What happens when one system updates in real time and another closes monthly?

Who is responsible when the figures do not reconcile?

Technology can move information between systems, but it cannot independently resolve every question about meaning, ownership and appropriate use.

Those decisions require governance.

Without a clear process, individual analysts and business teams are forced to make their own interpretations. Over time, local decisions become embedded in spreadsheets, data pipelines, reports and dashboards.

The organisation may then have several technically correct versions of the same business measure, each based on different assumptions.

> ***The problem is not necessarily poor analysis.***
>
> ***It is the absence of an agreed process for determining which interpretation should apply.***

Governance is more than control

Governance is sometimes perceived as a compliance exercise that adds approvals and slows down innovation.

Poorly designed governance can have that effect.

Effective governance does the opposite.

It reduces the time teams spend debating definitions, locating owners, validating reports and recreating previous decisions.

It creates a common operating model for how information is managed and used.

Good data governance establishes:

- clear ownership
- agreed definitions
- appropriate access
- repeatable quality controls
- visible data lineage
- documented decision-making
- accountable use
- ongoing monitoring

These controls do not exist simply to satisfy an auditor.

They help employees determine which information they can use, how they should interpret it and whether it is appropriate for the decision in front of them.

Governance creates speed by reducing uncertainty.

It allows people to move faster because the organisation has already established the rules, responsibilities and evidence needed to support confident action.

What makes a data process auditable?

An auditable process is one that can be followed, reviewed and reproduced.

It should be possible for someone other than the original analyst or system owner to understand how an output was created.

That does not mean documenting every technical detail for every user.

It means maintaining enough evidence to answer the questions that matter.

What was the purpose?

Every analytical or AI-supported process should begin with a clearly defined business purpose.

What decision is the information intended to support?

Who will use it?

What could happen if the answer is incomplete or incorrect?

A weekly operational report may require different controls from an automated decision affecting customers, employees or regulated activity.

Governance should be proportionate to the potential impact.

Where did the information come from?

The organisation should be able to identify the source systems contributing to an output.

Where several sources contain similar information, the authoritative source should be agreed and documented.

This creates provenance: evidence of where the information originated.

How was it transformed?

Raw information is rarely presented without modification.

Records may be filtered, grouped, joined, standardised or calculated.

Those transformations should be sufficiently visible to explain how the source data became the final metric, report or AI-supported answer.

Which definitions were applied?

Critical business terms should have agreed definitions.

A metric such as customer satisfaction, first-contact resolution or conversion should not depend on which dashboard a person opens.

Consistent definitions are essential for comparable reporting and coordinated decision-making.

Who owns the information?

Ownership should not be ambiguous.

A data owner is accountable for the meaning and appropriate use of the information. Data stewards or operational custodians may be responsible for quality, maintenance and day-to-day controls.

Without clear accountability, quality issues can persist because everyone uses the data but no one owns the outcome.

Who can access and use it?

Access should reflect role, purpose and sensitivity.

Not every user needs visibility of every customer record, employee measure or commercially sensitive metric.

Governance should define who can view, interrogate, modify or distribute information, and under which conditions.

How was the result validated?

Validation should be repeatable and proportionate to risk.

This might include automated quality checks, reconciliation against source systems, peer review, threshold monitoring or approval by an accountable business owner.

For AI-supported analysis, validation may also include checking whether the response is grounded in the right information and whether important context has been omitted.

Can the result be reproduced?

An auditable output should not depend entirely on the memory of one analyst.

Another authorised person should be able to follow the process, apply the same definitions and reach a consistent result.

Reproducibility reduces key-person risk and strengthens confidence in the information.

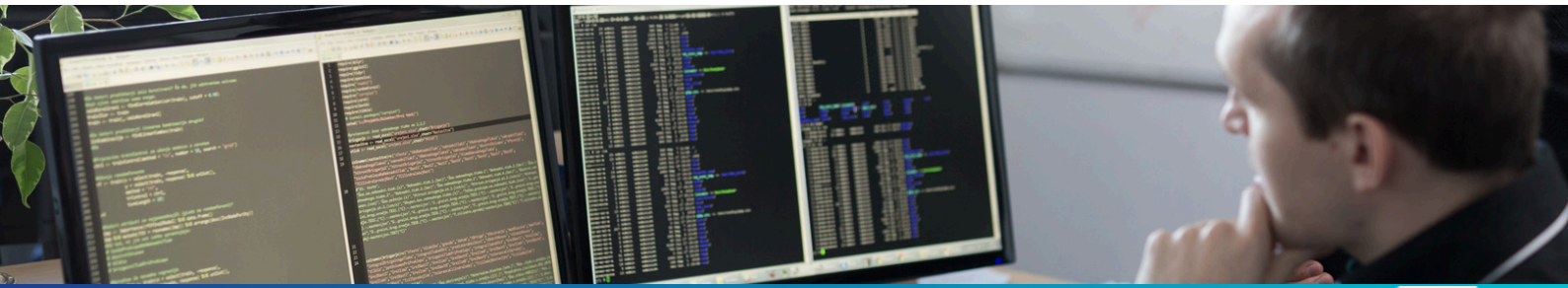
What happens when something changes?

Data processes are not static.

Applications are upgraded. Fields change. KPIs evolve. New regulations emerge. Business structures and customer journeys are redesigned.

Change management should assess how those developments affect integrations, definitions, reports, models and controls.

A process that was reliable when created may not remain reliable without ongoing review.



AI raises the governance standard

Traditional reporting already requires data quality, ownership and access controls.

AI increases the importance of those disciplines because it can analyse information faster, combine more variables and make answers accessible to a wider group of users.

It can also produce outputs that appear complete and confident even when the underlying context is fragmented.

Before an organisation relies on an AI-supported answer, it should be able to determine:

- which information the system accessed
- whether the information was current
- whether the user was authorised to access it
- how relevant business terms were interpreted
- whether the output can be explained
- whether the answer requires human review
- whether the use could affect customers, employees or other stakeholders
- how errors or unexpected outcomes will be identified
- who remains accountable for the final decision

AI governance should therefore not operate separately from data governance.

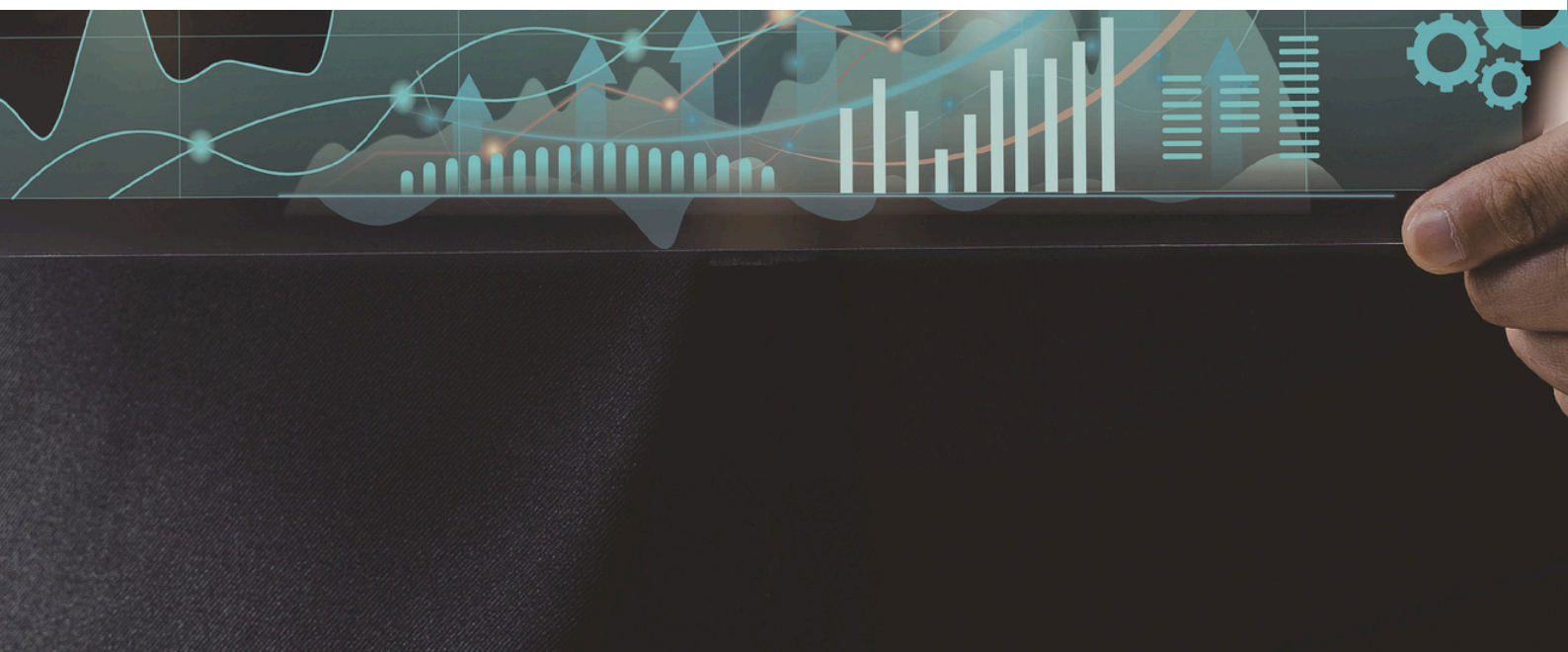
An AI system cannot be trusted if the information feeding it is unmanaged, inconsistently defined or impossible to trace.

The faster the analysis becomes, the more important it is to know that the underlying process remains controlled.

Different frameworks, common expectations

Organisations do not need to adopt every governance framework available. But understanding the major global approaches can help businesses build processes that are more consistent, defensible and adaptable across markets. Although the frameworks differ in scope, most reinforce a common set of expectations:

Accountability | Purpose | Risk management | Data quality | Security | Transparency | Human oversight | Monitoring | Evidence.



DAMA-DMBOK: Establishing the data management foundation

The DAMA Data Management Body of Knowledge is a widely recognised framework for structuring data management practices.

It places data governance at the centre of related disciplines such as:

- data architecture
- data integration
- metadata
- data quality
- security
- master and reference data
- warehousing and analytics

Its relevance is practical.

Governance does not work as an isolated policy function. It must influence how data is designed, integrated, defined, secured and maintained throughout its lifecycle.

For organisations struggling with inconsistent metrics, unclear ownership or duplicated data processes, DAMA-DMBOK provides a useful structure for defining the responsibilities and capabilities needed around the technology.

ISO/IEC 38505: Treating data as an enterprise governance issue

ISO/IEC 38505 applies broader governance principles to the current and future use of data.

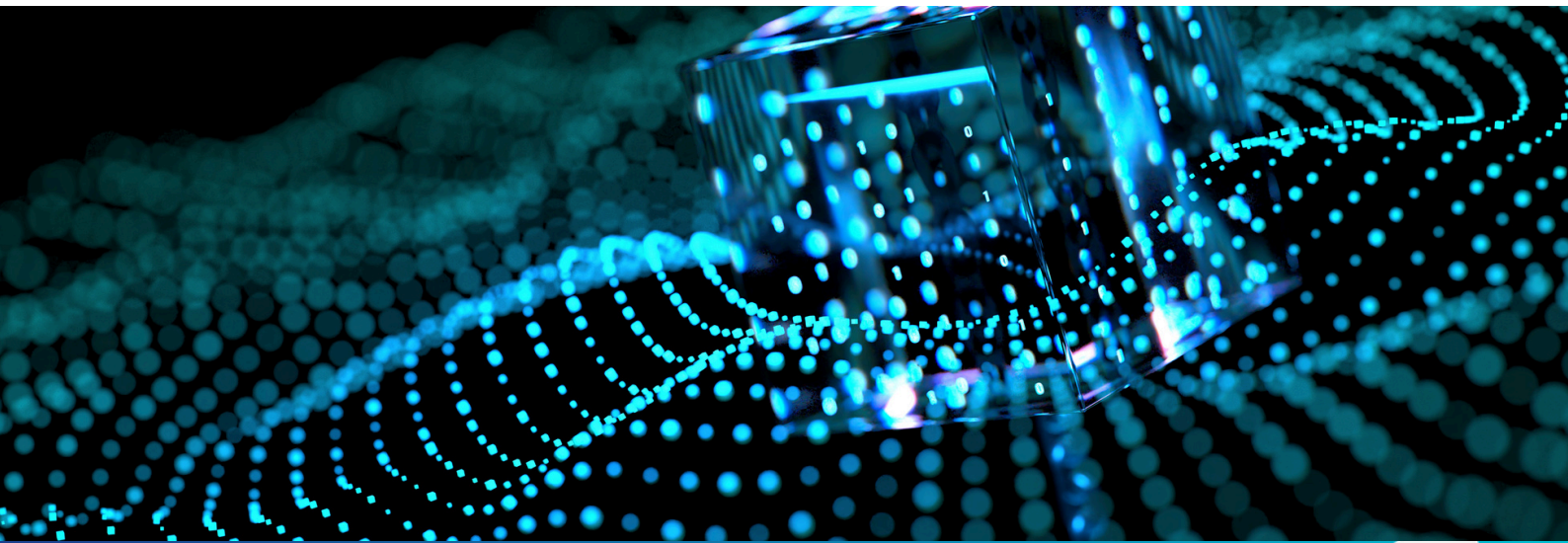
Importantly, it positions data governance as part of organisational governance, not simply a technical responsibility assigned to IT.

This reflects the reality that data decisions affect:

- business strategy
- risk
- customer outcomes
- regulatory obligations
- operational performance
- investment priorities
-

Senior leaders therefore need visibility of how data is being acquired, controlled, used and protected.

The framework supports a shift from asking, **"Who manages the database?"** to asking, **"How does the organisation govern the value and risk associated with its data?"**



COBIT: Connecting information governance to enterprise objectives

COBIT provides a framework for the governance and management of enterprise information and technology.

Its value lies in connecting technology decisions with business objectives, risk, accountability and performance.

For data and analytics, this means ensuring that:

- technology investments support defined outcomes
- responsibilities are clear
- controls are proportionate
- risks are managed
- performance is monitored
- governance is integrated with wider enterprise priorities

COBIT helps reinforce that data governance should not be a standalone program disconnected from the way the organisation governs technology, risk and value.

ISO/IEC 27001: Protecting the information foundation

Trust also depends on security.

ISO/IEC 27001 provides requirements for establishing, maintaining and continually improving an information security management system.

It focuses on managing risks to the confidentiality, integrity and availability of information.

For analytics and AI, those principles are fundamental.

Information should be protected from unauthorised access, inappropriate modification and loss. Access controls, risk assessment, incident management and continuous improvement must extend to the data supporting reports, models and AI-generated outputs.

Data cannot be considered trustworthy if it is not appropriately protected.

ISO/IEC 42001: Creating a management system for AI

ISO/IEC 42001 is an international standard for establishing, implementing, maintaining and continually improving an AI management system.

Rather than treating responsible AI as a collection of isolated checks, it encourages organisations to build a repeatable management system around how AI is developed, acquired, deployed and monitored.

That includes:

- defined responsibilities
- policies and objectives
- risk assessment
- impact consideration
- operational controls
- documented information
- performance evaluation
- corrective action
- continual improvement

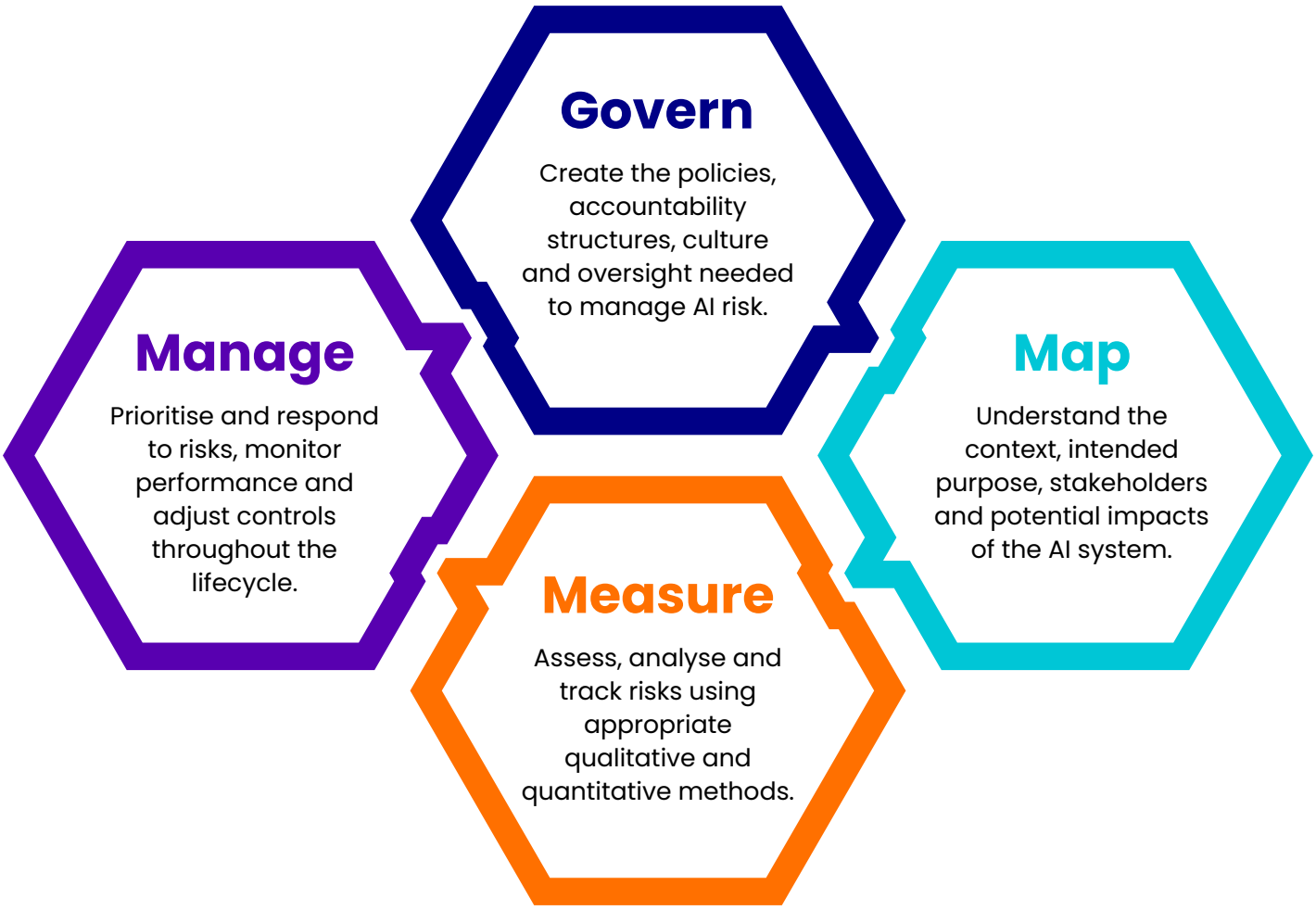
This management-system approach is important because AI governance cannot rely on good intentions or one-time reviews.

It must become part of the organisation's normal operating processes.

NIST AI Risk Management Framework:
Govern, map, measure and manage

The US National Institute of Standards and Technology AI Risk Management Framework provides a voluntary approach for managing AI risk.

It is organised around four functions:



The framework is particularly useful because it connects high-level governance with practical risk activity.

It reinforces that AI risk management begins before deployment and continues after the system becomes operational.

OECD AI Principles: A shared international direction

The OECD AI Principles promote AI that is innovative and trustworthy while respecting human rights and democratic values.

They emphasise areas including:

- inclusive growth and wellbeing
- human-centred values
- transparency and explainability
- robustness, security and safety
- accountability

The principles have influenced policy approaches across multiple jurisdictions and provide a useful international reference point.

For organisations operating globally, they help identify the expectations that increasingly sit beneath national regulation and industry guidance.

The EU AI Act: From principles to legal obligations

The EU AI Act introduces a risk-based legal framework for AI.

Its obligations vary according to the nature of the system and the level of risk. For applicable high-risk systems, requirements include areas such as:

- risk management
- data and data governance
- technical documentation
- record-keeping
- transparency
- human oversight
- accuracy, robustness and cybersecurity

The significance for data teams is clear. AI governance is not limited to the final model or user interface. It extends into the quality, suitability, provenance and management of the information supporting the system.

Organisations operating in or serving European markets need processes that can demonstrate how relevant AI systems are governed, not merely state that responsible practices are in place.

Regional frameworks reinforce the same direction

Other markets are developing practical approaches around similar principles. Australia's Voluntary AI Safety Standard provides guardrails for organisations developing and deploying AI safely and responsibly.

The UK's approach emphasises safety, security and robustness; transparency and explainability; fairness; accountability and governance; and contestability and redress.

Singapore has developed model governance frameworks covering traditional, generative and agentic AI, supported by practical assurance tools and testing initiatives.

These approaches are not identical.

But they reinforce a consistent international direction: organisations must be able to identify AI use, assign accountability, manage risk, maintain appropriate data controls, monitor outcomes and provide sufficient transparency.

A practical governance model for trusted data and AI

The number of frameworks can feel overwhelming.

The practical objective is not to create a separate governance process for every standard or jurisdiction.

It is to establish a common control foundation that can be mapped to multiple requirements.

A strong operating model should include the following.

1. Define the purpose

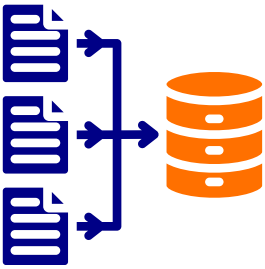
Document the business objective, intended users and decisions the data or AI capability will support.

The more significant the potential impact, the stronger the review and controls should be.

2. Assign accountable ownership

Identify who owns the data, the metric, the analytical process and the final decision.

Accountability should remain clear even where technology performs part of the analysis.



3. Maintain an inventory

Record important data sources, integrations, models, AI systems and business uses.

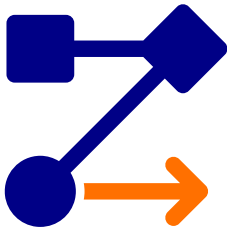
An organisation cannot govern capabilities it does not know exist.

4. Standardise definitions

Create governed definitions for critical data entities and KPIs.

Ensure those definitions are applied consistently across teams, systems and reporting layers.

5. Document lineage and transformation



Maintain sufficient visibility of where information came from and how it was processed.

This should cover significant joins, exclusions, calculations and transformations.

6. Apply quality controls

Define what acceptable quality means for each use case.

Monitor completeness, accuracy, timeliness, consistency and relevance.

7. Control access by role and purpose

Give people access to the information required for their responsibilities without exposing unnecessary or sensitive data.

Review access as roles, systems and uses change.

8. Build in human oversight

Define where people must review, approve, challenge or override an automated output.

Human oversight should be meaningful, not merely a procedural checkbox.

9. Monitor performance and risk

Track whether data pipelines, metrics and AI-supported processes continue to operate as intended.

Look for quality deterioration, unusual outputs, access issues and changes in business context.

10. Preserve evidence

Retain the documentation, logs, approvals, testing and decision records needed to demonstrate how the process operates.

Evidence creates auditability. Auditability creates accountability. Accountability strengthens trust.

Governance should scale with risk

Not every report requires the same level of control.

A low-impact internal dashboard should not necessarily follow the same approval process as an AI-supported decision affecting employment, credit, healthcare or access to essential services.

A proportionate approach considers:

- the sensitivity of the information
- the number of people affected
- whether decisions are automated
- whether outcomes can be reversed
- the potential financial or operational impact
- applicable regulatory obligations
- the consequences of an incorrect result

This allows governance to protect the organisation without becoming unnecessarily burdensome.

The objective is not maximum control over every use.

It is the right level of control for the context and risk.

Move beyond the dashboard

A dashboard shows the result.

Governance provides the confidence behind it.

As data volumes, applications and AI use continue to grow, organisations must be able to do more than produce faster answers.

They must be able to demonstrate:

- where the information came from
- how it was interpreted
- which controls were applied
- who remains accountable
- whether the result can be explained
- whether it should be trusted

The businesses that gain the greatest advantage from data and AI will not be those with the most dashboards or the most tools.

They will be those that combine skilled people, connected technology and clear, auditable processes to make better decisions with confidence.

Speak to an emite specialist

If this checklist has surfaced gaps you want to address with expert support, we are ready to help. Bring your completed checklist and we will start there.

emite.com/contact-us