

ISO/IEC 38505-1 Board Briefing

What the international standard for the governance of data asks of directors — explained in plain English, with the questions to put to management.

About this briefing

What it is. A plain-English briefing on ISO/IEC 38505-1, the international guidance on how a governing body should oversee an organisation's data. It is our interpretation, written for directors; it does not reproduce the standard.

Who it is for. Board directors, non-executive directors, trustees and members of audit, risk or technology committees.

How to use it. Read pages 1–3 before a board or committee discussion on data. Use the ten questions (page 4) to test management's assurance, and the 90-day agenda (page 5) to plan the board's own next steps. Nothing needs to be filled in. Reading time: about 15 minutes.

Why data is a board matter

Data now underpins revenue, operations, regulatory standing and reputation. It is simultaneously an asset that can create value and a liability that can cause harm. Decisions about data — what to collect, how to use it, who to share it with, how long to keep it — carry consequences that management alone should not be left to weigh. Directors do not manage data, but they remain accountable for how well it is governed.

- **Value:** are we getting a return from the data we hold and the money we spend on it?
- **Risk:** could our use, loss or misuse of data harm customers, the organisation or third parties?
- **Constraints:** are we operating inside the legal, regulatory, contractual and ethical limits that apply to our data?

These three lenses — value, risk and constraints — run through ISO/IEC 38505-1 and through this briefing.

The standard in brief

	In plain English
What it is	International guidance for governing bodies on overseeing the use of data. It applies the governance model of ISO/IEC 38500 (the standard for governance of IT) specifically to data.
What it is not	It is not a data-management manual, a technical specification or a certifiable management-system standard. It tells the board what to oversee, not how management should run data operations.
Who it applies to	Any organisation, of any size or sector, public or private, that relies on data — which today is every organisation.
Its core idea	The board should evaluate the current and future use of data, direct management through strategy and policy, and monitor performance and conformance — applying six governance principles to data across its whole life, from collection to disposal.
Related parts	ISO/IEC 38505-1 is Part 1 of a series. A companion part addresses how governance connects to day-to-day data management. Your data or risk function can advise which parts your organisation uses.

The board's cycle: Evaluate, Direct, Monitor

The governance model behind the standard gives the board three continuous tasks. Applied to data, this is how we interpret them:

Task	What the board does	What to expect from management	Evidence you might see
Evaluate	Considers how data is used today and how it should be used in future, including opportunities, threats and obligations.	A candid assessment of data assets, their value, the main data risks and the legal/ethical constraints.	Data strategy review; data risk assessment; inventory of critical data.
Direct	Sets direction: approves data strategy, assigns accountability, sets risk appetite for data and approves key policies.	Plans and policies that translate board direction into action, with named owners.	Approved data strategy and policies; data ownership model; risk appetite statement covering data.
Monitor	Checks that direction is followed and outcomes achieved, and that the organisation stays within constraints.	Regular, measurable reporting — not just narrative — and early escalation of material issues.	Data governance dashboard; incident and breach reporting; audit findings; benefit tracking.

Six principles, applied to data

ISO/IEC 38505-1 carries across the six principles of ISO/IEC 38500. The principle names are the standard's; the interpretation and questions below are ours.

Principle	What it means for data (our reading)	A question for the board
Responsibility	Everyone who collects, uses or decides on data understands and accepts their accountability, and that accountability is clearly assigned.	Who is accountable for each of our most important data sets — by name?
Strategy	The data the organisation holds and plans to use supports its strategy, and the strategy reflects what data makes possible.	Does our business strategy say what data it depends on, and does our data strategy follow from it?
Acquisition	Data, and capabilities to manage it, are obtained for valid reasons, with a balanced view of benefits, costs, risks and obligations — including data bought or received from third parties.	When we collect or buy data, how do we decide it is justified and lawful?
Performance	Data is of the quality and availability the business needs, and data investments deliver their expected value.	How do we know our critical data is good enough — and what did our last data investment actually return?
Conformance	Data use complies with laws, regulation, contracts, internal policies and the organisation's ethical commitments.	What assurance tells us we are within our legal and ethical limits for data, and when was it last tested?
Human behaviour	Data practices respect the people affected — customers, staff and the public — and the culture supports responsible use.	Would our customers and staff be comfortable with how we use their data if they saw it?

Following data through its life

A distinctive feature of ISO/IEC 38505-1 is that it asks the board to consider accountability for data at each stage of its life. The standard uses six activities — **collect, store, report, decide, distribute and dispose** — and considers value, risk and constraints at each. The table below is our board-level reading of that idea.

Activity	Board focus: value	Board focus: risk	Board focus: constraints
Collect	Are we collecting the data our strategy needs?	Are we collecting more than we need, or from unreliable sources?	Do we have a lawful basis and consent where needed?
Store	Is data held where it can be found and reused?	Is it secure, backed up and recoverable?	Are location, sovereignty and contractual rules met?
Report	Do reports turn data into insight decision-makers trust?	Could inaccurate reporting mislead the board, regulators or markets?	Are regulatory and statutory reporting obligations met?
Decide	Are decisions — including automated or AI-driven ones — better because of data?	Could data-driven decisions be biased, opaque or wrong?	Are automated decisions explainable and challengeable where required?
Distribute	Do we share or monetise data where it creates value?	Could sharing expose us to leakage or misuse by others?	Are sharing agreements, transfers and licences compliant?
Dispose	Are we releasing the cost of data we no longer need?	Is retained data increasing our breach exposure?	Do we delete on time and hold data when legally required?

[EXAMPLE] Fictional illustration

*[EXAMPLE] Northvale Housing Association (a fictional organisation) reviewed its tenant data against the six activities. The board found that **dispose** was the weakest: records of former tenants were kept indefinitely “just in case”. It directed management to set and apply retention periods and asked for quarterly evidence of deletions. Exposure fell, storage costs dropped, and the risk register recorded a reduced data-retention risk.*

What good looks like — and warning signs

Signs of effective data governance	Warning signs for the board
Named, senior accountability for data, with a clear mandate.	“IT owns the data” — or nobody can say who does.
Data appears in strategy, risk appetite and investment cases.	Data is discussed only after an incident or audit finding.
Board reporting uses measures with trends and targets.	Reporting is narrative-only, or always green.
Critical data is identified, and its quality is measured.	No agreed list of the data the business cannot do without.
Data risks are on the risk register with owners and actions.	Data risk is folded into a generic “cyber” line.
Retention and disposal happen, with evidence.	Everything is kept forever “just in case”.
Benefits from data investments are tracked after go-live.	Data programmes are judged on delivery, never on value.

Ten questions to ask management

Use these to test whether management's assurance is substantive. A strong answer is specific, evidenced and owned; a weak one is general, reassuring and unowned.

#	Question	A strong answer includes...
1	What are our most critical data assets, and who is accountable for each?	A short, maintained list with named senior owners.
2	How does our data strategy support our business strategy?	Explicit links from strategic goals to data needs and investments.
3	What is our appetite for data-related risk, and are we within it?	A stated appetite, measures against it, and current position.
4	How do we decide what data to collect, buy or share?	A defined approval route considering value, risk and obligations.
5	How good is our critical data, and how do we know?	Measured quality against agreed thresholds, with trends.
6	What value have recent data investments delivered?	Tracked, evidenced benefits compared with the original business case.
7	Which laws, regulations and contracts constrain our data, and how is compliance assured?	A register of obligations and independent assurance results.
8	Where do we use data to make automated or AI-assisted decisions, and how are they overseen?	An inventory, risk assessment and human-oversight arrangements.
9	How long do we keep data, and can we prove we delete it?	A retention schedule and evidence of disposal.
10	What would we tell customers or regulators after a serious data incident tomorrow?	A tested response plan with clear roles and decision rights.

[EXAMPLE] Fictional illustration — weak versus strong

[EXAMPLE] Weak answer to Q5: "Data quality is generally good and the team is working on improvements."

[EXAMPLE] Strong answer to Q5: "We have identified 42 critical data elements. 37 meet their agreed quality threshold this quarter, up from 31. The five below threshold relate to supplier bank details; the Procurement Director owns remediation, due in Q3."

A 90-day starting agenda for the board

A practical sequence for a board beginning to apply ISO/IEC 38505-1. It is our suggested approach, not a requirement of the standard.

When	Board action	Outcome
Days 1–30	Agree who on the board (or which committee) oversees data. Ask management for a baseline: critical data assets, owners, main risks and obligations.	Clear oversight route; a baseline to evaluate against.
Days 31–60	Evaluate the baseline against the six principles and six data activities. Run a structured board self-assessment.	An agreed view of strengths and gaps.
Days 61–90	Direct: confirm data accountability, approve priorities and a data risk appetite. Agree the measures the board will monitor and how often.	Direction set; a monitoring cycle in the board calendar.

Key terms

Term	Meaning in this briefing
Governing body	The board of directors or equivalent body accountable for the organisation.
Governance of data	How the governing body evaluates, directs and monitors the use of data — distinct from data management, which is management's job.
Data accountability	Clear assignment of who answers for decisions about specific data across its life.
Value / risk / constraints	The three lenses for judging any use of data: benefit created, harm possible, and limits that apply.

Next step

The dataintelligenceinsights.com **ISO/IEC 38505-1 Board Self-Assessment** (PRO) turns this briefing into a working tool: rate the board's oversight against each principle and data activity, see where the gaps are, and build an action plan.

Independence notice: this is original dataintelligenceinsights.com interpretation of ISO/IEC 38505-1. It is not affiliated with or endorsed by ISO or IEC, does not reproduce the text of the standard, and is not a substitute for it. Obtain the official standard from ISO or your national standards body for the authoritative requirements.

This briefing is general professional information for directors. It is not legal, regulatory or other professional advice, and it does not establish conformance with any standard. Version 1.0, October 2026.