BRIGHTBRIDGE LEARNING INTERNATIONAL

Governance Roadmap & Monitoring Plan

Prioritized 90-day, 6-month, and 12-month operating plan with maturity, KRIs, incidents, and board reporting

International Children's Education Nonprofit | Simulated AI Governance Consulting Engagement

Portfolio note

All organizational details, AI systems, roles, risks, scores, and data in this portfolio artifact are fictional or synthetic and are provided solely to demonstrate applied AI governance consulting methodology.

Version 1.0 | August 2026

1. Current-State Maturity Assessment

The simulated BrightBridge environment begins with decentralized AI adoption, partial vendor controls, and uneven evidence across regions. Maturity is scored from 1 (ad hoc) to 5 (optimized and independently assured).

Maturity Domain	Current Score / 5	Current-State Observation
Governance & accountability	2.0	Named leaders exist, but AI decision rights and committee process are not yet standardized.
AI inventory	1.5	Known strategic systems are visible, but embedded vendor AI and shadow AI are not fully registered.
Risk classification	1.5	No enterprise standard; reviews vary by team.
Child impact / safeguarding	2.5	Strong safeguarding culture, but AI-specific child impact assessment is new.
Privacy & data governance	3.0	Established privacy practices, but AI-specific data lineage/retention needs strengthening.
Fairness & accessibility	1.5	Testing occurs case-by-case; no common standard or thresholds.
Human oversight	2.0	Human review exists operationally but is inconsistently documented/evidenced.
Third-party AI risk	2.0	Vendor review exists, but AI-specific clauses and model-change controls are immature.
Monitoring & incidents	1.5	Operational incidents are handled, but AI-specific KRIs and taxonomy are limited.
AI literacy	2.0	General awareness exists; role-based high-risk training is not standardized.
Assurance & evidence	1.5	Evidence is dispersed; no formal AI control testing program.

Overall Simulated Maturity

Approximate current-state maturity: 2.0 / 5 - Emerging. Target after 12 months: 3.5 / 5 - Defined and consistently operated, with selected independent assurance.

2. Top Enterprise Gaps

Priority	Gap	Risk
1	No authoritative complete AI inventory	Unknown AI use and embedded vendor features create unmanaged risk.
2	No common risk classification standard	Teams cannot consistently determine required review and controls.
3	Child impact assessment not embedded	Child-affecting AI may be reviewed technically without structured rights/safeguarding analysis.
4	Human oversight evidence inconsistent	Review may occur but cannot always be demonstrated.
5	Vendor AI clauses incomplete	Model changes, data use, incident notice, and audit rights may be insufficient.
6	No unified control/evidence library	Safeguards are difficult to test and compare across systems.
7	AI-specific monitoring immature	Fairness, drift, vendor change, and oversight KRIs are not centralized.
8	Incident taxonomy and escalation incomplete	AI safety incidents may not reach governance

Priority	Gap	Risk
		leaders consistently.

3. 90-Day Action Plan

Action	Owner	Timing	Evidence of Completion
Approve Charter & Operating Model	CEO / COO	Weeks 1-4	Approved charter; committee named; decision rights published
Launch AI inventory campaign	AI Governance Lead	Weeks 1-8	>=95% of known systems registered; owners assigned
Adopt Risk Classification Standard	AI Governance Committee	Weeks 3-6	All registered systems tiered
Identify High-risk child-affecting systems	Safeguarding + AI Governance	Weeks 4-8	Priority assessment queue
Implement AI intake gate	Procurement + AI Governance	Weeks 4-8	No new AI purchase without intake
Create initial AI Risk Register	AI Governance Lead	Weeks 6-10	Top material risks assigned to owners
Issue interim acceptable-use/data rules	CIO + DPO	Weeks 2-6	Restricted data categories and approved tools communicated
Start first Child Impact Assessment	VP Education + Safeguarding	Weeks 6-12	Dropout Predictor CIA draft and conditions

4. 3-6 Month Plan

Action	Owner	6-Month Outcome
Complete high-risk assessments	System Owners + AI Governance	All High-risk systems have documented assessment and decision.
Deploy Control & Evidence Matrix	AI Governance Lead	Control owners, evidence, test methods, frequency, and gaps recorded.
Update AI vendor standard and contracts	Procurement + Legal	High-risk new vendors use standard clauses; legacy remediation plan.
Implement role-based AI literacy	People Ops	Safeguarding, program, procurement, privacy, security, HR, and system-owner modules.
Launch model/fairness monitoring	Model Risk Lead	Dashboard for High-risk models with thresholds.
Formalize AI incident process	CISO + Safeguarding + AI Governance	Taxonomy, reporting channel, severity and escalation rules.
Establish evidence repository	AI Governance Lead	Central controlled repository linked to inventory IDs.
Quarterly executive reporting	Executive Sponsor	First enterprise AI risk dashboard delivered.

5. 6-12 Month Plan

Action	Owner	12-Month Outcome
Test control effectiveness	Internal Assurance / Risk	Selected High-risk controls independently tested.
Expand country/local validation	Regional Program Leads	High-risk child models validated in each operating context.
Vendor reassessment program	Procurement	Annual reassessment and model-change tracking operational.
Incident tabletop exercises	Safeguarding + CISO	At least two simulations with documented lessons/actions.

Action	Owner	12-Month Outcome
Governance maturity reassessment	AI Governance Lead	Target >=3.5 / 5 in core domains.
Board risk appetite refinement	Executive Sponsor	AI risk tolerance and escalation thresholds formally reviewed.
Retirement/exit process	CIO + Procurement + DPO	Retired AI systems have closure/deletion evidence.
Annual governance report	AI Governance Committee	Portfolio, incidents, fairness, control effectiveness, roadmap, and next-year priorities.

6. Key Risk Indicators (KRIs) and Metrics

KRI / KPI	Measure	Target / Trigger	Frequency	Owner
Inventory completeness	Registered AI systems / discovered AI systems	>= 95%	Quarterly	AI Governance Lead
High-risk owner assignment	High-risk systems with named accountable owner	100%	Monthly	AI Governance Lead
High-risk approval currency	High-risk systems with current decision record	100%	Monthly	AI Governance Chair
Child-safeguarding AI incidents	Count and severity	0 Critical; all material incidents investigated	Monthly	Safeguarding Director
Human review completion	Required high-risk decisions with documented human review	>= 98%	Monthly	System Owners
Fairness threshold breaches	High-risk systems outside approved subgroup thresholds	0 unresolved >30 days	Quarterly	Model Risk Lead
Model performance	Systems below approved accuracy/safety threshold	0 unresolved	Monthly	Model Risk Lead
Vendor material changes	Material vendor changes reviewed before/within required window	100%	Monthly	Procurement
Sensitive-data incidents	Confirmed unauthorized AI data exposure	0 Critical	Monthly	DPO/CISO
Control evidence completeness	Required High-risk controls with current evidence	>= 95%	Quarterly	AI Governance Lead
Overdue remediation	High-risk actions overdue >30 days	< 5%; no Critical overdue	Monthly	Executive Sponsor
AI literacy completion	Required-role completion	>= 95%	Quarterly	People Ops

7. AI Incident Process

1. Detect and report through established security, safeguarding, program, or AI governance channels.
2. Triage severity based on child safety, privacy/security, discrimination, scale, duration, and reversibility.
3. Contain: pause feature, restrict access, disable automation, preserve evidence, or suspend vendor connection as needed.
4. Notify accountable owners and required governance leaders according to severity.
5. Investigate root cause, affected model/version, data, decisions, and impacted stakeholders.
6. Remediate and define compensating controls.
7. Retest relevant scenarios/controls before restart.
8. Update risk register, inventory, decision record, KRI thresholds, and training as required.

Illustrative Severity Levels

Severity	Example	Target Escalation
Critical	Child safety harm, safeguarding miss, major	Immediate containment and executive

Severity	Example	Target Escalation
	sensitive-data exposure, prohibited use	escalation
High	Material fairness failure, high-risk control failure, significant model regression	Same business day governance escalation
Moderate	Contained error or control gap with limited impact	Tracked remediation and monthly review
Low	Minor quality issue within tolerance	Operational correction and trend monitoring

8. Periodic Reassessment Triggers

- Annual review for High-risk systems at minimum.
- New country, new language, or material new user group.
- New data type or sensitive-data use.
- Change in decision role or automation level.
- Major model/vendor version change.
- Material incident or repeated KRI breach.
- Evidence of differential impact or accessibility failure.
- Purpose expansion beyond original approval.

9. Executive / Board Reporting Format

Board Section	Content
Portfolio	Total systems by tier, lifecycle, child-facing status, approval status
Material Risks	Top 5 enterprise/system risks, trend, residual risk, owner, treatment
Child Safety	Safeguarding incidents, High-risk child systems, CIA status, unresolved conditions
KRIs	Human review, fairness, performance, vendor change, data incidents, control evidence
Incidents	New material incidents, root cause, containment, remediation status
Controls	Effectiveness results, overdue high-risk remediation, exceptions
Roadmap	90-day/6-month/12-month progress, resource constraints, decisions required
Decisions Requested	Risk acceptance, funding, system suspension, policy change, or strategic choice

10. Resource Assumptions

- Dedicated AI Governance Lead or equivalent program owner.
- Part-time contributions from Safeguarding, DPO, CISO, Procurement, Legal, People Ops, and Regional Program Leads.
- Model/fairness evaluation capacity for High-risk systems, internal or external.
- Central evidence repository and inventory workflow.
- Budget for targeted independent assurance and vendor remediation.

Portfolio deliverable result

The roadmap converts assessment findings into a funded operating plan with owners, milestones, KRIs, incident escalation, reassessment triggers, and an executive reporting format - demonstrating how governance moves from design into sustained operation.