BRIGHTBRIDGE LEARNING INTERNATIONAL

Control & Evidence Matrix

Risk-tiered safeguards, accountable owners, evidence requirements, testing, and remediation

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. Control Framework Purpose

BrightBridge requires governance controls to be testable. A policy statement alone is not evidence that a safeguard operates. This matrix links risk tier and control objective to an accountable owner, implementation status, evidence, test method, frequency, and remediation requirement.

Control Domains

- Governance & accountability
- Child safeguarding
- Human oversight
- Privacy & data minimization
- Information security
- Fairness, bias & inclusion
- Accessibility
- Transparency & documentation
- Model evaluation & monitoring
- Third-party AI risk
- Incident management
- AI literacy & training
- Independent assurance

2. Enterprise Control & Evidence Matrix

Control ID	Tier	Control Requirement	Owner	Evidence Required	Testing Method	Frequency	Status	Gap / Remediation
GOV-01	All	AI system registration before pilot or purchase	AI Governance Lead	Inventory record + intake form	Quarterly inventory reconciliation	Quarterly	Implemented	None
GOV-02	High	Named accountable AI System Owner	Executive Sponsor	Approved owner register	Sample ownership verification	Quarterly	Implemented	None
GOV-03	High	Formal Go / Conditional Go / Redesign / No-Go decision	AI Governance Committee	Decision record + conditions	Decision record completeness review	Per approval	Implemented	None
GOV-04	All	Material change triggers reassessment	AI Governance Lead	Change log; vendor notices	Change-log sample	Quarterly	In progress	Automate vendor change intake
SAFE-01	High	Child-affecting AI requires safeguarding review	Global Safeguarding Director	Signed safeguarding review	100% approval check	Per approval	Implemented	None
SAFE-02	High	No automated closure of safeguarding cases	Safeguarding Operations Lead	Workflow configuration; case logs	Quarterly sample	Quarterly	Implemented	None
SAFE-03	High	High-severity AI incidents escalated within defined timeframe	AI Governance Lead	Incident tickets; escalation timestamps	Incident sample review	Quarterly	In progress	Formalize severity SLA
HUM-01	High	Human review before material child-affecting decision	Program Operations	Decision log; reviewer ID; override reason	Sample 30 decisions	Quarterly	Implemented	None
HUM-02	High	Reviewer has authority to override AI output	System Owner	Procedure; training; override logs	Interview + evidence sample	Semiannual	Implemented	None
HUM-03	Moderate	External communications require human approval	Business Function Owner	Content workflow record	Spot-check published content	Quarterly	Implemented	None

Control ID	Tier	Control Requirement	Owner	Evidence Required	Testing Method	Frequency	Status	Gap / Remediation
PRI-01	All	Data minimization documented	DPO	Data map; approved fields	Privacy review	Annual + change	In progress	Complete legacy tools
PRI-02	High	Sensitive child data restricted to approved systems	DPO + CISO	Access list; DLP policy; system configuration	Access review	Quarterly	Implemented	None
PRI-03	High	Retention and deletion schedule defined	DPO	Retention schedule; deletion evidence	Deletion test	Annual	In progress	Vendor deletion evidence gaps
PRI-04	High	Cross-border data flow documented	DPO	Data transfer map; contractual safeguards	Annual review	Annual	In progress	Regional mapping incomplete
SEC-01	High	Least-privilege access and MFA	CISO	IAM config; access review logs	Access control test	Quarterly	Implemented	None
SEC-02	High	Security incident logging and auditability	CISO	Logs; SIEM evidence; incident tickets	Log sample	Quarterly	Implemented	None
FAI-01	High	Subgroup performance/fairness testing before deployment	Model Risk Lead	Fairness report	Independent review	Pre-deploy + quarterly	In progress	Standardize metrics
FAI-02	High	Local/country validation for multi-country child-affecting models	Regional Program Lead	Validation report by country	Governance review	Pre-deploy + annual	In progress	Small-country sample strategy
ACC-01	High	Accessibility testing for child-facing interfaces	Inclusive Education Lead	Accessibility test report	Specialist review	Pre-deploy + annual	Implemented	None
TRN-01	High	Documented intended use, limitations, and prohibited uses	System Owner	System card / model card	Document review	Annual + change	Implemented	None
TRN-02	High	Affected users receive appropriate AI notice where applicable	Program Lead	Notice text; implementation evidence	Field verification	Annual	In progress	Standard notice template
MOD-01	High	Model performance monitoring with thresholds	Model Risk Lead	Monitoring dashboard	Threshold review	Monthly	In progress	Automate alerts
MOD-02	High	Drift detection and retraining/change approval	Model Risk Lead	Drift report; change approval	Quarterly review	Quarterly	In progress	Define drift thresholds
VEN-01	All	AI vendor due diligence completed before contract	Procurement Lead	Completed questionnaire; evidence pack	Procurement audit sample	Per contract	Implemented	None
VEN-02	High	Contract requires material model-change notification	Legal + Procurement	Executed contract clause	Contract review	Per contract	In progress	Legacy contracts
VEN-03	High	Vendor incident notification SLA	Legal + Procurement	Contract clause; incident procedure	Contract review	Per contract	In progress	Standardize SLA
VEN-04	High	Vendor deletion/exit plan documented	Procurement Lead	Exit plan; deletion terms	Annual vendor review	Annual	In progress	Evidence of deletion
DOC-01	All	Central evidence repository for approvals and tests	AI Governance Lead	Repository index	Completeness sample	Quarterly	Implemented	None
DOC-02	High	Decision and override evidence retained	System Owner	Decision logs; override reasons	Sample review	Quarterly	Implemented	None
INC-01	All	AI incident taxonomy and reporting channel	AI Governance Lead	Policy; reporting form	Process test	Annual	In progress	Run tabletop exercise
LIT-01	All	Role-based AI literacy training	People Ops + AI Governance	Training materials; completion records	Completion audit	Annual	In progress	High-risk role modules
AUD-01	High	Independent assurance over	Internal Audit	Assurance plan; report	Audit committee review	Annual	Planned	First review year 2

Control ID	Tier	Control Requirement	Owner	Evidence Required	Testing Method	Frequency	Status	Gap / Remediation
		selected controls						

3. Control Testing Standard

1. Identify the control objective and the risk(s) it addresses.
2. Confirm the named control owner and the period under review.
3. Define evidence population and sample method before testing.
4. Test design effectiveness: would the control, if performed as designed, meaningfully reduce the risk?
5. Test operating effectiveness: was the control actually performed, by the right person, at the required frequency, with sufficient evidence?
6. Record exceptions and determine whether they are isolated, systematic, or evidence of control failure.
7. Assign effectiveness rating: Effective, Partially Effective, Ineffective, or Not Tested.
8. Create remediation action with owner, due date, compensating control, and retest requirement.

Effectiveness Ratings

Rating	Definition
Effective	Control is appropriately designed and operating evidence shows consistent performance.
Partially Effective	Control generally operates but has gaps, inconsistent evidence, or limited coverage.
Ineffective	Control design or operation does not sufficiently reduce the identified risk.
Not Tested	Insufficient evidence or testing not yet performed.

4. Sample Detailed Control Tests

Control	Test Objective	Procedure	Exception Rule
HUM-01	Human review before material child-affecting decision	Population: all dropout-model interventions in quarter. Sample: 30 decisions across at least 3 countries. Pass: reviewer ID, AI recommendation, final decision, and override rationale where applicable present for 100% of sample.	Any decision without identifiable human review is a control exception; repeated exceptions trigger High severity remediation.
FAI-01	Subgroup fairness testing	Obtain quarterly fairness report; verify approved subgroup metrics, sample sizes, thresholds, and documented review. Recalculate one metric from source output.	Missing subgroup analysis or threshold breach without action = Partially Effective or Ineffective.
VEN-02	Vendor material-change notification	Sample High-risk vendor contracts and recent vendor releases. Verify contract clause and evidence that material updates were reviewed.	No clause on legacy High-risk vendor = remediation; unreviewed material change = escalation.
PRI-03	Retention and deletion	Select systems handling child/safeguarding data; verify schedule, configured retention, and deletion evidence.	Retention without documented purpose or deletion proof = exception.

Control	Test Objective	Procedure	Exception Rule
INC-01	AI incident reporting	Run annual tabletop. Verify reporting channel, severity classification, notification roles, containment decision, and evidence capture.	Failure to identify critical escalation path = control failure.

5. Evidence Quality Standard

- Evidence must be traceable to the control, period, owner, and system.
- Screenshots without dates, source, or identifiable system context are weak evidence.
- Self-attestation alone is insufficient for High-risk operating effectiveness when system logs or independent evidence should exist.
- Evidence should be retained in a central repository with access controls and retention rules.
- Where vendor evidence is relied upon, record its scope, date, independence, and limitations.

6. Control Gap and Remediation Workflow

9. Tester records gap, affected system(s), control objective, and risk consequence.
10. Control owner assigns severity and immediate compensating action if needed.
11. AI Governance Lead determines whether approval conditions or residual risk change.
12. High/critical gaps are escalated and may restrict or suspend system use.
13. Owner completes remediation and uploads evidence.
14. Independent reviewer retests the control.
15. Risk register, decision record, and monitoring thresholds are updated if required.

Portfolio deliverable result

The Control & Evidence Matrix demonstrates that BrightBridge governance can be audited: every required safeguard has an owner, evidence expectation, testing method, frequency, status, and remediation path.