Enterprise Privacy, AI Governance & Third-Party Risk Assessment

BDC-PRIV-001 | Consolidated case study | Version 2.2 | 11 November 2026

Prepared by: Olumuyiwa Michael, CIPP/US, CIPP/EU, CIPM, AIGP, CompTIA Security+

Published by: BloomDale Capital LLC
Assessed enterprise: Meridian Digital Holdings (fictional)

EXECUTIVE OVERVIEW

This synthetic case study evaluates a fictional U.S.-headquartered enterprise across GDPR/UK GDPR, CCPA/CPRA, U.S. state privacy laws, HIPAA, GLBA, AI governance, automated decision-making technology (ADMT), and third-party risk management. It combines applicability screening, control testing, 25 illustrative findings, accountable owners, and 90-day remediation plans.

The most urgent modeled risks involve undocumented automated lending governance, business associate agreement verification, and inconsistent propagation of advertising opt-out signals.

ASSESSMENT AT A GLANCE

Critical	High	Moderate	Total findings
4	15	6	25

Risk interpretation: Findings are scored as illustrative inherent risk (likelihood × impact). Overall residual risk is **not calculated** because control effectiveness and post-remediation testing have not been established.

SIMULATION DISCLOSURE: All business units, vendors, records, findings, scores, owners and dates are fictional. This is a portfolio demonstration, not an actual audit, client engagement or legal opinion. Legal applicability and future effective dates require independent verification before this work is used as compliance guidance.

Reader guide & version 2.2 editorial notes

Document navigation

Enterprise profile, scope and methodology | Page 3

GDPR and CCPA/CPRA | Page 4–5

U.S. State Privacy Laws | Page 6–8

HIPAA and GLBA | Page 8–10

AI Governance and ADMT | Page 11–13

Third-Party Risk Management | Page 14–16

Author and primary references | Page 17

Editorial changes from version 2.1

1. Credential confirmation: CIPP/EU is retained as active based on the author's confirmation.

2. Risk language: The cover no longer asserts an overall residual risk rating. All numerical finding scores in the original assessment modules are treated as illustrative inherent risk. The reference to "overall residual risk HIGH" in the Third-Party Risk Management executive assessment should be read as an *illustrative pre-remediation assessment rating*, not a measured residual-risk conclusion.

3. Finding totals: The consolidated 25 findings comprise 4 Critical, 15 High and 6 Moderate. Related findings across modules may describe the same underlying control deficiency; counts are not deduplicated enterprise incidents.

4. Regulatory validation: The underlying modules are preserved from the approved v2.1 source. Specific statutory thresholds, exemptions, rulemaking status and 2027–2028 effective dates, particularly those in the state-law horizon watch and AI/ADMT sections, have **not been independently reverified** for this revision. They should be checked against current official sources before external reliance.

5. Navigation: This edition adds a reader guide and page references while preserving the approved assessment text, findings, evidence matrices and source list.

Publication quality note

This version is suitable for editorial review. Before presenting it as a fully validated regulatory reference, complete the source-date verification identified above and review the source module tables that span pages. The portfolio demonstration disclaimer applies throughout.

Source preservation

Pages 3–17 reproduce pages 2–16 of the author-approved v2.1 PDF without substantive alteration. The original v2.1 cover is replaced by the updated cover on page 1; this reader guide is new.

Enterprise profile

All five modules use these invented modeling inputs.

Attribute	Assumption	Used in
Business units	HealthTech (patient portal operated for a HIPAA covered entity); Financial Services (consumer lending, nonbank financial institution under FTC jurisdiction); Digital Learning (online courses); Digital Platforms (advertising-supported online services)	All modules
Revenue	$45 million annual global gross revenue	CCPA and state thresholds
U.S. consumers	180,000 in total: California 65,000; Texas 30,000; Connecticut 18,000; New Jersey 15,000; Colorado 12,000; Virginia 12,000; Oregon 8,000; Maryland 6,000; other states 14,000	State privacy laws
EU and UK	Digital Learning and Digital Platforms target EU and UK customers	GDPR, UK GDPR, EU AI Act
Data practices	Targeted advertising; processes health data (sensitive under all state comprehensive laws) and financial data (sensitive under some, e.g. California and Connecticut); no sale of personal data for money	All modules
AI systems	Credit decisioning, applicant ranking, learning recommendations, support summarization, fraud detection	AI Governance, TPRM

Scope and methodology

- Determine jurisdiction, covered entity role, applicable statutory thresholds and exemptions before treating a requirement as mandatory.
- Map obligations to policies, workflows, technical safeguards, contractual controls and testable evidence.
- Score every finding on one scale: likelihood (1–5) × impact (1–5), banded Low 1–5, Moderate 6–12, High 13–19, Critical 20–25. Bands are a portfolio convention, not statutory thresholds.
- Assign proposed remediation owners and test closure evidence before changing risk status.
- Separate mandatory law from voluntary guidance (including NIST AI RMF and ISO/IEC 42001).

Consolidated workstreams

Module	Regulatory / operational focus	Finding IDs
GDPR and CCPA/CPRA	Territorial scope, consumer rights, ROPA, DPIAs, vendor contracts	GC-F01 to GC-F05
U.S. State Privacy Laws	State applicability, profiling, opt-outs, assessments	US-F01 to US-F05
HIPAA and GLBA	Entity classification, PHI/customer information, safeguards	HG-F01 to HG-F05
AI Governance and ADMT	AI inventory, consequential decisions, oversight, impact assessments	AI-F01 to AI-F05
Third-Party Risk Management	Vendor lifecycle, contracts, subprocessors, transfers	TP-F01 to TP-F05

Cross-cutting executive recommendations

1. Establish a single processing and AI system inventory with accountable business owners and legal-role classification.
2. Standardize rights-request and opt-out orchestration across channels and vendors, including distinct GPC and ADMT workflows.
3. Implement documented assessment triggers for DPIAs, profiling, consequential decisions and third-party AI procurement.

4. Create a risk-tiered vendor review process with DPA/BAA and transfer safeguards where applicable.
5. Report evidence-backed closure rates, overdue high-risk actions and control-testing results to a governance committee.

GDPR and CCPA/CPRA

1. Executive assessment

Meridian targets EU and UK customers and processes California residents' information. GDPR and UK GDPR apply to the relevant activities under their territorial-scope tests. The CCPA applies because Meridian's $45 million annual gross revenue exceeds the $26,625,000 threshold (CPI-adjusted from $25 million in January 2025); with 65,000 California consumers it does not meet the 100,000-consumer test. This module identifies five illustrative gaps and assigns remediation owners.

2. Applicability decision record

Regime	Assumed trigger	Decision / qualification
EU GDPR	EU-directed digital services and monitoring	Applicable to in-scope processing under Article 3(2) (offering services to, or monitoring, individuals in the EU). Article 27 requires an EU representative.
UK GDPR	UK-directed digital services	Applicable under UK GDPR Article 3(2) (UK GDPR as amended by the Data (Use and Access) Act 2025). Article 27 requires a UK representative.
CCPA/CPRA	Annual gross revenue of $45 million exceeds the $26,625,000 threshold	Applicable to California processing. GLBA- and FCRA-covered data and HIPAA PHI fall under data-level exemptions.

3. GDPR control-to-evidence mapping

Control ID / legal basis	Expected operating control	Synthetic evidence / finding
G-01 | Arts. 5, 6	Maintain processing-purpose and lawful-basis register; provide transparency	E-001: 4 of 12 sampled activities lack documented lawful basis.
G-02 | Arts. 12–22	Rights intake, identity checks, exceptions, response tracking	E-002: 3 of 10 sampled requests lack documented closure review.
G-03 | Art. 28	Processor diligence and signed agreements with required terms	E-003: 2 of 8 sampled processors lack documented subprocessor authorization terms.
G-04 | Art. 30	Current ROPA with required fields and accountable owners	E-004: Marketing and analytics flows missing from ROPA sample.
G-05 | Arts. 32, 35	Risk-based security and DPIA screening for likely high-risk processing	E-005: One high-risk profiling use case lacks recorded DPIA screening.

4. CCPA/CPRA control-to-evidence mapping

Control ID / legal area	Expected operating control	Synthetic evidence / finding
C-01 | Notice at collection	Category, purpose, retention and required notice disclosures	E-006: One of four sampled forms omits a required retention disclosure.
C-02 | Consumer rights	Access/know, deletion, correction, portability where applicable	E-007: 2 of 10 sampled requests have incomplete system-level fulfillment records.
C-03 | Sale/share opt-out	Honor applicable opt-out preference signals such as GPC	E-008: Simulated test shows opt-out not propagated to one advertising tag.

C-04 | Sensitive PI	Classify uses; offer limitation right when statutory conditions apply	E-009: Sensitive-data purpose inventory is incomplete.
C-05 | Service-provider/contractor contracts	Required use restrictions and assistance provisions	E-010: 2 of 7 vendor contracts missing selected required provisions.

5. Illustrative risk register

Finding	Likelihood × Impact	Score	Owner / target
GC-F01 Incomplete ROPA / lawful basis	4 × 4	16 High	Privacy Lead / 45 days
GC-F02 GPC signal not propagated	4 × 4	16 High	Digital Platforms Privacy Lead / 30 days
GC-F03 Processor contract gaps	3 × 5	15 High	Legal + TPRM / 60 days
GC-F04 DPIA screening gap	3 × 5	15 High	AI Governance + Privacy / 30 days
GC-F05 Rights fulfillment evidence gaps	3 × 4	12 Moderate	Privacy Operations / 45 days

Risk method: inherent risk = likelihood (1–5) × impact (1–5), using the document-wide bands (Low 1–5, Moderate 6–12, High 13–19, Critical 20–25). Residual risk is reassessed after evidence-backed control testing.

6. 90-day remediation and validation

Period	Actions	Acceptance evidence
Days 1–30	Repair GPC signal propagation; document profiling DPIA screening; assign owners	Tag test logs; DPIA screening decision; issue tracker
Days 31–60	Complete ROPA/lawful-basis inventory; revise processor contracts; strengthen DSAR QA	Approved ROPA entries; signed addenda; QA checklist
Days 61–90	Retest controls, report residual risk, approve ongoing monitoring cadence	Retest results; risk acceptance records; steering report

7. Assessment limitations

- Confirm whether Meridian is controller, processor, business, service provider or contractor for each activity; roles are activity-specific.
- CCPA applicability rests on the assumed revenue figure. A real assessment would substantiate it with financial records and test each statutory exemption.
- EU and UK analysis assumes active targeting. Member-state rules, transfer arrangements and DPIA triggers would need confirmation against actual processing.
- CPPA regulations effective 1 January 2026 add risk-assessment duties for new high-risk processing (existing processing must be assessed by 31 December 2027) and ADMT requirements from 1 January 2027. ADMT is covered in the AI Governance module.
- No actual vendor agreements, consumer records, OneTrust exports, employer procedures or personal data are included.

U.S. State Privacy Laws

1. Executive assessment

This module screens Meridian's U.S. consumer-facing processing (analytics, targeted advertising, customer support and vendor integrations) against eight state laws, using the enterprise profile, then maps controls and synthetic deficiencies for the states in scope.

2. Applicability assumptions and decision rules

- Consumer counts by state come from the enterprise profile: $45 million revenue and 180,000 U.S. consumers, including 65,000 in California. These are invented modeling inputs.
- Meridian conducts business in each state below and engages in targeted advertising. Meridian Financial Services is a GLBA-covered financial institution and Meridian HealthTech is a HIPAA business associate, so entity-level and data-level exemptions are applied state by state.
- California: the CCPA applies on the revenue test ($45 million exceeds $26,625,000), not the 100,000-consumer test.
- Other states count consumers resident in that state, typically 100,000 (or 25,000 with revenue from data sales). Since 1 July 2026, Connecticut applies at 35,000 consumers, and separately to any controller that processes sensitive data or sells personal data, with no volume minimum for those triggers. Maryland applies at 35,000 consumers. Texas and Nebraska have no volume threshold and exempt SBA-defined small businesses; Meridian is assumed not to qualify under the applicable NAICS size standard, measured with affiliates. Texas also exempts GLBA financial institutions and HIPAA covered entities and business associates at entity level. Remaining states were screened against the 14,000 consumers in other states; Nebraska is monitored on the same basis as Texas.

3. State-by-state screening register

State	Law	Screening outcome	Control focus
California	CCPA/CPRA	In scope: revenue test met	Notice; access/delete/correct; sale/share opt-out; GPC; vendor terms
Colorado	CPA	Out of scope: 12,000 consumers, below 100,000. Monitor.	Universal opt-out mechanism; sensitive-data consent; assessments
Connecticut	CTDPA	In scope from 1 July 2026: processes sensitive data (no volume minimum for that trigger). The narrowed GLBA exemption no longer covers Financial Services at entity level	Consumer rights; consent; assessments; opt-out preference signals
Virginia	VCDPA	Out of scope: 12,000 consumers, below 100,000. Monitor.	Rights; sensitive-data consent; targeted-advertising opt-out; assessments
Texas	TDPSA	In scope for Digital Learning and Digital Platforms; Financial Services and HealthTech entity-exempt (GLBA, HIPAA) as separate legal entities	Privacy notice; rights; sensitive-data consent; controller/processor contracts
Oregon	OCPA	Out of scope: 8,000 consumers, below 100,000. Monitor.	Rights; sensitive data; controller/processor duties
New Jersey	NJDPA	Out of scope: 15,000 consumers, below 100,000. Monitor.	Rights; targeted-advertising opt-out;

			assessments; universal opt-out
Maryland	MODPA	Out of scope: 6,000 consumers, below 35,000. Monitor.	Heightened data minimization; sensitive-data restrictions; assessments

Findings below apply to the in-scope states (California, Connecticut and Texas). Out-of-scope states stay on a monitoring list and are rescreened each year against updated consumer counts. Control focus shows what would apply if a state comes into scope.

4. Synthetic control findings

ID / area	Likelihood × Impact	Synthetic evidence	Owner / corrective action
US-F01 Preference signals	4 × 4 = 16 High	GPC/universal opt-out signals honored on some websites but not consistently transmitted to downstream ad-tech partners.	Digital Platforms Privacy Lead: Implement centralized signal capture, downstream propagation, and monthly test evidence.
US-F02 State rights workflow	3 × 5 = 15 High	Request intake captures a single state template and misses some state-specific appeal and verification steps.	Privacy Operations Manager: Implement jurisdiction-aware workflow, appeal routing, and exception log.
US-F03 Sensitive data	3 × 5 = 15 High	No unified classification of sensitive data across healthcare and fintech integrations.	Data Governance Lead: Inventory categories, document processing purpose and required consent/restrictions.
US-F04 Data protection assessments	3 × 4 = 12 Moderate	Targeted advertising and profiling activities lack consistent assessment trigger documentation.	Privacy Counsel / Product: Adopt state-specific assessment screening and approval gates.
US-F05 Processor contracting	3 × 4 = 12 Moderate	Sample vendor agreements omit some required processing instructions and audit/assistance provisions.	Vendor Risk Manager: Refresh templates, prioritize high-risk vendors, and track signed addenda.

Risk scoring: illustrative likelihood × impact on a 1–5 scale. Scores are scenario assumptions, not empirical findings.

5. Control-to-evidence testing plan

- Opt-out signal testing: Browser-based GPC test log, CMP configuration screenshots, downstream vendor suppression records.
- Rights fulfillment: Synthetic intake tickets, identity verification steps, state-specific SLA and appeal logs.
- Sensitive-data governance: Data inventory, classification dictionary, consent event log, purpose limitation records.
- Assessments: DPIA/assessment trigger register, approved assessments, mitigation decisions.
- Vendor oversight: Contract clause matrix, DPA templates, vendor inventory, remediation tickets.

6. Proposed 90-day remediation

- Days 1–30: Confirm statutory scope and exemption analysis with counsel; inventory sites, ad-tech, rights workflows, and sensitive data.
- Days 31–60: Implement jurisdiction-specific rights rules, GPC/UOOM tests, processor contract remediation, and assessment triggers.
- Days 61–90: Retest controls, sample evidence, report open risks, obtain business-owner sign-off, and set quarterly monitoring.

7. 2027 horizon watch

Confirmed future-effective provisions to track: California ADMT requirements (1 January 2027), first CPPA risk-assessment submissions (1 April 2028) and, if the significant-risk test is met, a first cybersecurity audit (1 April 2030 for businesses under $50 million revenue); Colorado SB 26-189 (1 January 2027); Louisiana Data Privacy Act (1 January 2027; applies above $25 million annual gross revenue, so likely in scope if Meridian does business in Louisiana); Oklahoma Consumer Data Privacy Act (1 January 2027; 100,000-consumer threshold, not expected to apply); Alabama Personal Data Protection Act (1 May 2027); Vermont Data Privacy and Online Surveillance Act (1 January 2028). Each register entry records citation, effective date, impacted processing, owner and readiness status. Proposed bills are tracked separately and are not treated as obligations.

HIPAA and GLBA

1. Executive assessment

Objective: assess whether Meridian HealthTech and Meridian Financial Services fall within HIPAA and GLBA regimes; test selected privacy, security, vendor and incident-response controls; and prioritize remediation. Legal coverage must be confirmed before any finding is classified as a statutory violation.

2. Synthetic enterprise facts and coverage decisions

Unit	Assumed activity	Preliminary regulatory treatment
Meridian HealthTech	Hosts a patient portal and processes ePHI on behalf of a HIPAA-covered healthcare provider.	Assume business associate status for contracted services; validate BAA, data flows, and any separate covered-entity functions.
Meridian Financial Services	Offers consumer financial products and maintains customer information; assumed to be a nonbank financial institution within FTC jurisdiction.	Subject to the FTC Safeguards Rule (16 CFR Part 314) and CFPB Regulation P (12 CFR Part 1016) for privacy notices; FCRA and ECOA/Regulation B apply to lending decisions.

Scope caveat: Not every health technology company is a HIPAA covered entity or business associate, and not every business handling financial data is governed by the FTC Safeguards Rule. Entity role, activity and regulator determine which rules apply. Consumer-facing HealthTech features outside the business associate relationship may instead fall under the FTC Health Breach Notification Rule or Washington's My Health My Data Act.

3. HIPAA control mapping: Meridian HealthTech

Control area / authority	Expected control	Synthetic evidence and test
Business associate contracts; 45 CFR 164.502(e), 164.504(e)	Executed BAAs covering permitted uses, safeguards, reporting, subcontractors and return/destruction.	HT-01: sample 8 provider/subcontractor relationships; verify BAA execution and clauses.
Security risk analysis; 45 CFR 164.308(a)(1)	Accurate assessment of risks and vulnerabilities to ePHI; risk management actions.	HT-02: inspect risk register, systems inventory, assessment methodology and mitigation closure.
Access controls and audit controls; 45 CFR 164.312(a), (b)	Unique access, appropriate authentication, access logging and review based on risk.	HT-03: sample 20 accounts, privileged access, terminations and audit-log review records.
Incident and breach procedures; 45 CFR 164.308(a)(6), 164.410	Security incident response and timely business-associate notification of breaches to covered entity.	HT-04: tabletop simulation and sample incident records; validate contractual escalation timelines.
Minimum necessary, where applicable; 45 CFR 164.502(b)	Role-appropriate limitations on PHI uses and disclosures, subject to exceptions.	HT-05: inspect role matrices and sample permitted-use scenarios.

4. GLBA control mapping: Meridian Financial Services

Control area / authority	Expected control	Synthetic evidence and test
Information security program; 16 CFR 314.4	Written safeguards program with qualified individual, risk assessment, controls, testing, oversight and reporting as applicable.	FS-01: inspect program charter, risk assessment, board report and control ownership.
Access, encryption, MFA; 16 CFR 314.4(c)	Appropriate safeguards, including encryption and multifactor authentication subject to rule provisions.	FS-02: sample critical applications, encryption exceptions and privileged access.
Service-provider oversight; 16 CFR 314.4(f)	Reasonable selection, contractual safeguards and periodic assessment of providers.	FS-03: sample 10 high-risk providers and contract/monitoring records.
Incident response and notification; 16 CFR 314.4(h), 314.4(j)	Written incident response plan where required; assess FTC notification obligations for qualifying notification events.	FS-04: review incident playbook and simulated notification threshold analysis.
Privacy notices and sharing; Regulation P, 12 CFR Part 1016	Initial and annual privacy notices (subject to the annual-notice exception) and opt-out rights for sharing with nonaffiliated third parties where required.	FS-05: compare product flows, sharing categories, notices and exception analysis.

5. Synthetic findings and risk prioritization

Scoring: likelihood (1–5) × impact (1–5), using the document-wide bands (Low 1–5, Moderate 6–12, High 13–19, Critical 20–25).

ID	Illustrative gap	L × I	Rating	Owner
HG-F01	Two sampled subcontractor relationships lack documented BAA verification. See also TP-F01.	4 × 4 = 16	High	HealthTech Privacy / Procurement
HG-F02	Privileged ePHI access review evidence incomplete for two quarters.	3 × 5 = 15	High	HealthTech Security
HG-F03	Service-provider monitoring evidence missing for 4 of 10 sampled vendors.	4 × 4 = 16	High	Financial Services TPRM
HG-F04	Safeguards program risk assessment omits a new customer-data integration.	3 × 5 = 15	High	Qualified Individual / Security
HG-F05	Incident playbooks do not clearly distinguish HIPAA and FTC notification analyses.	3 × 4 = 12	Moderate	Legal / Incident Response

6. Evidence-to-finding examples

HG-F01: Contract verification gap

Evidence: HT-01 simulated sample of eight vendor relationships; two have no centrally retrievable executed BAA. Interpretation: absence of evidence in the sample is not conclusive proof that no agreement exists.

Next test: Legal and Procurement reconcile signed agreements and verify each entity's business-associate/subcontractor role.

HG-F03: Third-party oversight gap

Evidence: FS-03 simulated sample of ten providers; four lack a documented periodic reassessment. Interpretation: evaluate whether monitoring frequency and depth are reasonable for each provider's risk before concluding noncompliance.

7. Proposed 90-day remediation plan

Window	Action / acceptance criterion	Accountable role
Days 1–30	Confirm legal entity roles and regulators; reconcile all missing BAAs; identify critical access and vendor oversight exceptions.	Legal, Privacy, Procurement
Days 31–60	Complete access recertification; update risk analysis and vendor monitoring; document evidence and escalation triggers.	Security, Qualified Individual, TPRM
Days 61–90	Run dual-regime incident tabletop; validate FTC/HIPAA decision trees; retest gaps and report residual risks.	Incident Response, Privacy, Legal

8. Governance and limitations

The Privacy Lead coordinates assessment, maintains evidence and reports trends. Legal determines applicability, contract interpretation and notification duties. Security and the Qualified Individual own technical safeguards; Procurement/TPRM own vendor monitoring; business unit leaders accept or escalate residual risk under governance policy.

Limitations: findings assume FTC jurisdiction over Meridian Financial Services and business associate status for Meridian HealthTech. A real assessment would confirm the functional regulator, covered-entity versus business-associate responsibilities and any rule exemptions, with organization-specific legal review.

AI Governance and ADMT

1. Executive assessment

This module covers Meridian's AI systems in consumer lending, hiring, digital learning, customer support and fraud detection across the United States, EU and UK. It identifies governance weaknesses in automated lending decisions, applicant screening, vendor model oversight and third-party generative AI. Legal applicability depends on entity roles, jurisdictions, actual processing and statutory exemptions.

2. Governance scope and reference framework

Source	Use in assessment	Classification
NIST AI RMF 1.0	Govern, Map, Measure, Manage functions	Voluntary risk-management framework
ISO/IEC 42001:2023	AI management-system governance, lifecycle and auditability	Voluntary standard unless contractually required
EU AI Act	Provider/deployer roles, prohibited practices, high-risk classifications and phased duties	Binding where applicable. Prohibitions apply since 2 February 2025 and Article 50 transparency duties since 2 August 2026; Annex III high-risk duties apply from 2 December 2027 (Regulation (EU) 2026/1744)
GDPR / UK GDPR	Lawful basis, transparency, DPIAs; EU GDPR Article 22 and UK GDPR Articles 22A–22D (in force 5 February 2026)	Binding where applicable
California CCPA ADMT regulations	ADMT used for significant decisions: pre-use notice, opt-out and access rights, risk assessment	Binding: regulations effective 1 January 2026; ADMT compliance from 1 January 2027
Colorado SB 26-189 (replaced SB 24-205)	Notice, adverse-decision disclosure, human review and record keeping for consequential automated decisions	Effective 1 January 2027; enforcement stayed by stipulation in X.AI v. Weiser pending Attorney General rules and a court ruling
Other U.S. state privacy laws	Profiling opt-outs and data protection assessments for qualifying decisions	State-specific coverage and exceptions

3. Synthetic AI system inventory

ID / system	Business use	Data / role	Initial risk
AI-01 Credit decision engine	Automated consumer loan eligibility and pricing	Financial and identity data; deployer	Critical
AI-02 Applicant ranking	Ranks employment applicants for human review	Resume and employment data; deployer	High
AI-03 Learning recommendations	Personalized course suggestions	Usage and learning data; deployer	Moderate
AI-04 Customer support assistant	Summarizes customer interactions	Customer support transcripts; deployer	High
AI-05 Vendor-supplied fraud detection	Flags suspicious transactions	Behavioral and transaction data; deployer	High

4. Jurisdictional applicability screening

Jurisdiction	Screening question	Proposed assessment action
California	Does Meridian use ADMT to make a significant decision about a California consumer, applicant or employee?	Provide pre-use notices and opt-out and access rights (subject to the regulatory exceptions) by 1 January 2027. Complete risk

		assessments before any new ADMT use, and for existing uses by 31 December 2027. GLBA- and FCRA-covered data used by AI-01 falls under CCPA data-level exemptions; AI-02 hiring decisions are in scope.
Colorado	Does Meridian use automated decision-making for a consequential decision about a Colorado consumer?	Prepare notice, adverse-decision disclosure, human review and record keeping under SB 26-189 (effective 1 January 2027; enforcement currently stayed pending litigation and rulemaking). SB 26-189 does not require impact assessments.
Connecticut / Texas (in-scope states; others monitored)	Is qualifying profiling used to make decisions with legal or similarly significant effects?	Map profiling opt-out rights, consent rules and exemptions by state. Connecticut also requires impact assessments for covered profiling activities created on or after 1 August 2026.
EU / EEA	Is Meridian a provider or deployer of a high-risk system, and does GDPR Article 22 apply?	Not expected on the current profile, because lending and hiring serve U.S. individuals only. If AI-01 (creditworthiness) or AI-02 (recruitment) extends to EU individuals, it is Annex III high-risk from 2 December 2027; AI-05 fraud detection is excluded from the credit-scoring category. Assess GDPR DPIA, lawful basis, transparency and Article 22 safeguards.
United Kingdom	Does processing involve significant decisions based solely on automated processing?	Apply UK GDPR Articles 22A–22D safeguards (information, representations, human intervention and the right to contest) to any UK significant decisions; not expected for lending or hiring on the current profile. Special category data remains restricted.

5. Synthetic findings and risk register

ID / finding	Likelihood × Impact	Owner	Required remediation
AI-F01 Missing ADMT decision inventory	4 × 5 = 20 Critical	AI Governance Lead	Inventory decision purpose, automation level, jurisdictions and data categories.
AI-F02 Lending model lacks documented notice, adverse-action and appeal screening	4 × 5 = 20 Critical	Financial Services / Legal	Assess notice, rights, adverse-action (ECOA/Regulation B, FCRA), appeal and human-review requirements. See also TP-F02.
AI-F03 Incomplete bias testing evidence	3 × 5 = 15 High	Model Risk Manager	Set testing methodology, metrics, monitoring and escalation thresholds.
AI-F04 Vendor model change notification absent	4 × 4 = 16 High	TPRM Lead	Add change notices, audit evidence and incident escalation provisions.

AI-F05 GenAI support transcripts over-retained	3 × 4 = 12 Moderate	Privacy Engineering	Apply retention, access, redaction and deletion controls.

6. Evidence and control testing

Control	Synthetic evidence to request	Pass criterion
AI system register	AI inventory export, ownership attestations	All in-scope systems and material uses documented
ADMT legal screening	Jurisdiction/use-case decision trees, counsel sign-off	Classification and exceptions recorded per system
Impact assessment	Privacy and algorithmic risk assessments	Risk, affected persons and mitigations traceable
Human oversight	Review SOP, override logs, appeal records	Meaningful review available where legally required
Fairness / performance	Validation reports, drift and bias monitoring	Approved thresholds and escalation process documented
Vendor governance	DPA, security assessment, AI addendum	Responsibilities, subprocessors and changes covered
Consumer communications	Notices, rights intake and response logs	Required disclosures and rights handled on time

7. Remediation roadmap

Period	Actions	Exit evidence
Days 1–30	Establish AI oversight committee; inventory systems; triage consequential decisions; verify jurisdiction-specific effective dates.	Signed inventory and applicability register
Days 31–60	Complete impact assessments; revise vendor contracts; design consumer-rights and human-review workflows.	Approved assessments, contract redlines and SOPs
Days 61–90	Test notices, appeals, bias monitoring and retention controls; report residual risk to leadership.	Test results, risk acceptance and executive dashboard

8. Proposed governance metrics

Inventory coverage (% of discovered systems registered); percentage of consequential-decision systems with signed legal screening; high-risk AI assessments completed; overdue high-severity remediation actions; vendor AI review coverage; appeals handled within applicable timelines; model monitoring exceptions and resolution time.

9. Limitations

Consumer privacy opt-out mechanisms such as GPC are distinct from ADMT-specific rights. Lending and hiring scenarios also require review under FCRA, ECOA/Regulation B, Title VII and state employment AI laws. Classifications are illustrative and would be confirmed by counsel for real systems.

Third-Party Risk Management

1. Executive assessment

Meridian Digital Holdings operates fictional HealthTech, Financial Services, Digital Learning, and Digital Platforms units. This simulated assessment evaluates whether vendor onboarding, privacy contracting, information-security due diligence, AI oversight, cross-border transfers, monitoring, and offboarding are consistently governed. The illustrative overall residual risk is HIGH pending remediation; it is not a finding about any real organization.

2. Scope, roles, and regulatory screening

Review vendors that process personal data, protected health information (PHI), customer information, or information used by automated decision-making systems. Determine Meridian's legal role and each vendor's role by processing activity, not by vendor label alone.

Framework	Conditional applicability / review point
GDPR / UK GDPR	Controller-processor Article 28 terms; Article 32 security; Chapter V transfer mechanism (adequacy, including the EU-U.S. Data Privacy Framework for certified recipients, SCCs or the UK Addendum/IDTA) and transfer impact analysis where needed; subprocessor authorization.
CCPA/CPRA	Determine business/service provider/contractor/third-party status; evaluate required contractual restrictions, purposes, consumer-rights support and onward disclosures.
HIPAA	If vendor creates, receives, maintains or transmits PHI for a covered entity or business associate, evaluate business associate status and BAA requirements; exceptions may apply.
GLBA	For a covered financial institution, evaluate applicable Safeguards Rule service-provider selection, contractual safeguards, and periodic assessment.
AI governance / ADMT	Assess AI supplier role, model/data provenance, testing, human oversight, explainability, and jurisdiction-specific automated decision-making duties; distinguish legal requirements from voluntary NIST AI RMF / ISO 42001 practices.

3. Synthetic vendor inventory and inherent risk

ID / fictional vendor	Service / data	Inherent risk	Primary owner
V-101 / HarborCloud Systems	Cloud hosting; customer profiles, identifiers	High	IT Infrastructure
V-102 / CareLink Analytics	Healthcare analytics; PHI under assumed BAA relationship	Critical	HealthTech
V-103 / LedgerBridge Processing	Financial servicing; customer information	High	Financial Services
V-104 / DecisionPilot AI	AI-assisted credit eligibility scoring; sensitive financial inputs	Critical	AI Governance / Finance
V-105 / BrightReach Media	Marketing analytics; online identifiers	Moderate	Digital Platforms
V-106 / AtlasSupport Global	Customer support; potential offshore access	High	Customer Operations

4. Risk methodology

Inherent risk uses Likelihood (1–5) × Impact (1–5), considering data sensitivity, scale, criticality, access, jurisdiction, automation and vendor concentration, with the document-wide bands (Low 1–5, Moderate 6–12, High 13–19, Critical 20–25). Residual risk is reassessed after verified control effectiveness.

5. Control testing and synthetic findings

Finding / synthetic evidence	Score	Owner / proposed corrective action
TP-F01: V-102 BAA signature not traceable to vendor master; E-BAA-02	20 Critical	Legal + HealthTech: confirm BA status; execute/locate BAA before PHI sharing; block processing until resolved.
TP-F02: V-104 AI model testing, appeal/human-review and data lineage evidence incomplete; E-AI-07	20 Critical	AI Governance: complete use-case screening, testing and oversight; restrict consequential use pending approval.
TP-F03: V-106 cross-border access inventory and transfer assessment incomplete; E-XFER-03	16 High	Privacy + IT: map access locations; validate transfer mechanism and supplementary measures if needed.
TP-F04: V-101 security assessment expired; E-SEC-11	15 High	Security: refresh due diligence, review independent assurance and remediation status.
TP-F05: V-105 service-provider classification and contractual use restrictions undocumented; E-DPA-09	12 Moderate	Privacy + Legal: classify disclosures; amend contract as appropriate; verify opt-out propagation.

6. Required evidence and test procedures

Control	Example evidence	Validation procedure
Vendor inventory	Owner, processing purpose, data categories, locations, tier	Reconcile procurement/AP, SSO, security and privacy inventories.
Pre-contract due diligence	Questionnaire, SOC 2/ISO evidence, pen-test summary, incident history	Sample high-risk vendors; confirm review, exceptions and approval dates.
Privacy terms	DPA, BAA when required, SCCs/UK addendum where relevant	Check parties, roles, purposes, onward transfers, breach notice and deletion.
AI supplier governance	Model card, test results, training-data provenance, human review design	Verify decision context, discrimination/privacy testing and monitoring.
Ongoing monitoring	Review calendar, control attestations, incident/issue log	Check overdue assessments and documented escalations.
Offboarding	Deletion/return certificate, access revocation, retention exceptions	Trace termination through access, storage, subprocessors and evidence closure.

7. 90-day remediation roadmap

Window	Deliverables	Acceptance criteria
Days 1–30	Contain critical exposure; validate PHI/AI vendor status; reconcile high-risk vendor list	No unapproved PHI transfers; critical AI use decisions documented; owners assigned.
Days 31–60	Execute missing agreements; complete transfer mapping; refresh high-risk security reviews	Contract register complete for sampled vendors; transfer and due diligence evidence approved.
Days 61–90	Implement tiered review cadence, vendor scorecards, offboarding testing	Risk committee signs off residual risk; control tests and exceptions recorded.

8. Governance, reporting, and escalation

Accountable executive: Chief Risk Officer. Privacy owns regulatory screening and data-processing controls; Legal owns contract advice; Security evaluates technical safeguards; Procurement enforces onboarding gates; business owners accept operational risk within delegated authority; AI Governance reviews consequential AI use. Critical risks escalate before activation and remain blocked or formally exceptioned according to policy.

Illustrative KPIs: 100% critical vendors assessed before go-live; ≥95% high-risk vendors reviewed within cadence; 100% applicable BAAs/DPAs traceable; zero unapproved consequential AI deployments; 100% terminated vendors with verified access revocation. These are proposed targets, not actual results.

9. Limitations

This is a synthetic assessment, not legal advice. NIST AI RMF and ISO/IEC 42001 are voluntary unless a contract or regulator requires them.

About the author

Olumuyiwa Michael, CIPP/US, CIPP/EU, CIPM, AIGP, CompTIA Security+

Privacy and compliance professional with more than seven years of experience in privacy operations, privacy impact assessments, data subject rights, incident management and regulatory compliance, and a technical background in database administration and information security.

This case study is part of the BloomDale Capital LLC Data Privacy & AI Governance Portfolio: https://mikeolu700-gif.github.io/bloomdale-privacy-ai-governance/

Primary legal references

Reviewed as of 11 November 2026.

- EU GDPR, Regulation (EU) 2016/679: https://eur-lex.europa.eu/eli/reg/2016/679/oj
- EU AI Act, Regulation (EU) 2024/1689: https://eur-lex.europa.eu/eli/reg/2024/1689/oj; amended by Regulation (EU) 2026/1744: https://eur-lex.europa.eu/eli/reg/2026/1744/oj
- UK GDPR and Data (Use and Access) Act 2025, ICO guidance: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/
- Data (Use and Access) Act 2025: https://www.legislation.gov.uk/ukpga/2025/18
- California Civil Code §1798.100 et seq.: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&chapter=1.&part=4.&lawCode=CIV&title=1.81.5
- California Privacy Protection Agency regulations (ADMT, risk assessments, cybersecurity audits): https://cppa.ca.gov/regulations/
- Colorado Privacy Act, Colorado Attorney General: https://coag.gov/resources/colorado-privacy-act/
- Colorado SB 26-189, Colorado General Assembly: https://leg.colorado.gov/
- Connecticut Attorney General: https://portal.ct.gov/ag
- Virginia Attorney General: https://www.oag.state.va.us/
- Texas Attorney General: https://www.texasattorneygeneral.gov/
- Texas Data Privacy and Security Act, Tex. Bus. & Com. Code ch. 541: https://texas.public.law/statutes/tex._bus._&_com._code_section_541.002
- Oregon Department of Justice: https://www.doj.state.or.us/
- New Jersey Division of Consumer Affairs: https://www.njconsumeraffairs.gov/
- Maryland Attorney General: https://www.marylandattorneygeneral.gov/
- HIPAA Administrative Simplification, 45 CFR Parts 160 and 164: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C
- HHS HIPAA guidance: https://www.hhs.gov/hipaa/for-professionals/index.html
- FTC Safeguards Rule, 16 CFR Part 314: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314
- CFPB Regulation P, 12 CFR Part 1016: https://www.ecfr.gov/current/title-12/chapter-X/part-1016
- CFPB Regulation B (ECOA), 12 CFR Part 1002: https://www.ecfr.gov/current/title-12/chapter-X/part-1002
- Fair Credit Reporting Act, 15 U.S.C. §1681 et seq.: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act
- FTC GLBA guidance: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
- NIST AI Risk Management Framework 1.0: https://www.nist.gov/itl/ai-risk-management-framework
- ISO/IEC 42001:2023: https://www.iso.org/standard/81230.html

Regulatory verification addendum | Version 2.2

BDC-PRIV-001 | 11 November 2026 | Synthetic portfolio demonstration

This addendum records targeted checks against official sources. It does not constitute a complete legal audit of every jurisdiction or a legal opinion. Where the underlying module contains a statement inconsistent with this addendum, use the qualified interpretation below.

Topic	Verified interpretation
California ADMT	CPPA regulations became effective 1 January 2026. Covered businesses must comply with the ADMT requirements beginning 1 January 2027; applicability and exceptions require use-case analysis.
California risk assessments	Applicable risk-assessment obligations begin 1 January 2026. Initial submissions to the CPPA are due 1 April 2028, subject to regulatory scope.
Colorado SB 26-189	The enacted statute replaces the prior SB 24-205 framework. The legislature states covered ADMT requirements begin 1 January 2027. The litigation-related enforcement stay described in the assessment has NOT been independently verified in this review and must not be treated as a confirmed current enforcement position.
EU AI Act	Regulation (EU) 2026/1744 amended the schedule. Chapter III high-risk duties for Annex III systems apply 2 December 2027; Annex I product-related high-risk systems apply 2 August 2028. Other provisions have different application dates.
Risk methodology	Finding scores represent synthetic inherent risk assumptions. An overall measured residual-risk rating has not been established without control-effectiveness testing.

Official sources checked

https://cppa.ca.gov/announcements/2025/20250923.html

https://leg.colorado.gov/bills/sb26-189

https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202601744

Publication note: Additional jurisdiction-specific claims, including the 2027 horizon watch and state applicability thresholds, should be reconfirmed against primary sources before being relied on outside this synthetic demonstration.