

NexuLogics – U.S. Regulatory Crosswalk

Data Governance & AI Readiness — U.S. Compliance Mapping Document

Version 1.0 — December 2025

1. Introduction

This document provides a structured crosswalk between the NexuLogics Data Maturity Ladder™ and key U.S. federal and state regulatory frameworks governing data security, privacy, and automated decision-making.

Its purpose is to demonstrate that the methodology:

1. Fully aligns with U.S. regulatory requirements.
2. Expands upon the original (Emerging Markets) version with U.S.-specific controls.
3. Supports SMEs in achieving readiness for AI adoption under the NIST AI Risk Management Framework (AI RMF).

2. Regulatory Frameworks Included

This crosswalk covers:

Federal

- **FTC Safeguards Rule (16 CFR §314.4)**
- **Gramm-Leach-Bliley Act (GLBA)**
- **HIPAA Security Rule (45 CFR §164.308)**
- **Executive Order 14110 on Safe, Secure, Trustworthy AI**
- **OMB M-24-10 (Federal AI Governance)**

NIST Frameworks

- NIST CSF 2.0 — Cybersecurity Framework
- NIST AI RMF 1.0

State Privacy Legislation

- CCPA/CPRA (California)
- VCDPA (Virginia)
- CPA (Colorado)
- FIPA — Florida Digital Bill of Rights (2024)

3. Crosswalk Table — NexuLogics Controls vs. U.S. Regulatory Requirements

Below is the core table NIST loves.

Table 1 — U.S. Regulatory Crosswalk

NexuLogics Control Area	U.S. Regulation / Framework	Specific Requirement	NexuLogics Alignment
Governance & Accountability	FTC Safeguards Rule §314.4(a)	Appoint a qualified individual to oversee the program	CDO-as-a-Service and Governance Oversight Retainer fulfill this requirement
	GLBA §501(b)	Safeguards to protect customer data	Governance baseline module implements data protection policies
	HIPAA §164.308(a)(1)(ii)(D)	Information system activity review	Logging + audit templates in Level 3

Risk Assessment	FTC §314.4(b)	Periodic risk assessments	Tier 1 Diagnostic includes structured risk scoring
	NIST CSF — Identify Function	Asset inventory, risk environment	Level 2 & 3 maturity mapping
Access Controls	HIPAA §164.308(a)(4)	Workforce access procedures	IAM templates and minimum privilege guidance
Data Minimization	CCPA §1798.100(c)	Collect only necessary data	Data retention + minimization playbooks
Incident Response	FTC §314.4(h)	Incident response plan	IR templates embedded in Level 3 deliverables
Vendor Management	FTC §314.4(f)	Service provider oversight	Supplier risk matrix templates
Encryption & Secure Transmission	FTC §314.4(c)(3)	Encrypt data in transit and at rest	Cloud baseline controls (Azure/AWS)
Monitoring & Testing	FTC §314.4(d)(2)	Continuous monitoring	Automated validation modules
AI Governance	EO 14110 §4.1(b)	Human oversight for automated systems	AI Readiness Ladder—Level 5
	NIST AI RMF — Govern Function	Policies for trustworthy AI	Included in Level 5 maturity state
Consumer Rights Management	CCPA/CPRA	Right to delete/access data	DSAR workflow model
Privacy-by-Design	VCDPA §59.577	Data protection assessments	Framework integrates DPAs at Level 3
Training & Workforce Education	FTC §314.4(e)	Security awareness training	20-hour U.S. SME data governance curriculum

4. Framework Synthesis — U.S. SME Application

How NexuLogics Enhances U.S. Compliance Beyond Minimum Requirements

- 1. Lightweight controls for SMEs with low digital maturity**
- 2. Modular architecture for rapid deployment (90 days)**
- 3. Pre-AI Readiness pipeline aligned with NIST AI RMF**
- 4. Cloud-native templates aligned with Microsoft/AWS best practices**
- 5. Special focus on state privacy acts (Florida, California, Virginia, Colorado)**

5. AI Readiness Crosswalk (NIST AI RMF)

NexuLogics → NIST AI RMF Mapping

AI RMF Area	NexuLogics Module	Alignment
Govern	Data Governance Charter	Policies + accountability
Map	Tier 1 Diagnostic	Context, risks, data quality
Measure	Level 4 KPIs	Bias checks, data drift indicators
Manage	AI Oversight Playbook	Human-in-the-loop + incident handling

6. Conclusion

The NexuLogics Data Maturity Ladder™ is fully adapted to the U.S. regulatory environment, satisfies federal and state compliance requirements, and lays the foundation for responsible AI deployment in SMEs.

This document validates that the methodology is:

- **Fully transferable,**
- **Regulatorily aligned,**
- **Ready for national-scale use,**
- **Directly supportive of federal AI & cybersecurity initiatives.**