MINIMUM VIABLE GOVERNANCE

The control stack, and the model to run it.

Governance is not one universal regime. For most companies it is a baseline control stack plus what your industry, states, customer contracts, and headcount trigger on top. This is the cross-functional map of what already governs you, the standards worth prioritizing, and a lean operating model to run it, sized to your risk and reviewed by leadership each quarter.

Set your values before AI sets them for you.

THE CORE GOVERNANCE MAP

What is commonly in scope by business function. Yours expands with industry, state, contract, and workforce-size triggers (page 3).

FUNCTION	REGULATIONS COMMONLY IN SCOPE	STANDARDS & FRAMEWORKS	PRACTICAL GOVERNANCE CONTROLS
Sales & Marketing	FTC ban on deceptive/unfair practices; CAN-SPAM; Telemarketing Sales Rule & Do-Not-Call where calling applies; copyright/trademark; state privacy & consumer-protection laws	FTC advertising guidance; privacy-by-design; optionally ISO 27701	Approved claims library; legal review for high-risk campaigns; consent/preference & suppression management; substantiation files; influencer/endorsement disclosures; marketing-vendor oversight
HR & People	FLSA; wage-and-hour & state pay laws; I-9/IRCA; Title VII, ADA, ADEA & other anti-discrimination laws; OSHA; FMLA/ACA & state leave at thresholds; state privacy laws	SHRM-style HR policy controls; NIST Privacy Framework concepts for workforce data	Worker classification; timekeeping/payroll approval; hiring & performance documentation; accommodation/leave workflow; harassment reporting & investigations; role-based HRIS access & retention schedule
Finance	IRS income, payroll & information-reporting; state sales/use, payroll & income taxes; beneficial-ownership when applicable; payment-card contractual requirements; sector-specific financial rules	GAAP where needed; COSO Internal Control; PCI DSS when accepting cards	Segregation of duties; approval matrix; bank reconciliation; expense/procurement thresholds; vendor master-data controls; tax calendar; audit trail & financial-record retention
IT & Security	State breach-notification & privacy laws; FTC security expectations; COPPA if serving children; GLBA Safeguards for covered financial institutions; HIPAA for covered entities/business associates; contractual security	NIST CSF 2.0; CIS Controls; SOC 2; ISO/IEC 27001; PCI DSS	Asset inventory; MFA; least privilege; patch & vulnerability management; backups & recovery tests; incident response; security awareness; vendor-risk review; data classification & retention
Customer Service	Consumer-protection & warranty rules; FTC rules on claims, refunds & recurring/negative-option; ADA Title III; privacy rights & breach-response obligations	CX quality standards; WCAG as a practical accessibility benchmark	Complaint & refund/escalation process; quality assurance; accessibility intake & accommodation; authentication before account disclosure; case-data retention; trend reporting to leadership
Operations	OSHA & workplace safety; environmental, licensing, zoning & health rules; product safety/recall; DOT/FDA/EPA or state/local rules for regulated operations; contract & supplier obligations	ISO 9001 quality; ISO 14001 environmental; ISO 45001 occupational health & safety; business-continuity	SOP ownership & versioning; safety training & incident logs; supplier qualification; business continuity; change management; quality checks; inventory/asset lifecycle; corrective-action tracking

WHAT APPLIES NEARLY EVERYWHERE

The foundations that hold regardless of size or industry.

1 · Corporate & decision governance

Entity records, delegated authorities, an approval matrix, conflict-of-interest expectations, contract-signature rules, policy ownership, and periodic leadership review.

2 · Financial & tax controls

Reliable income/expense records, payroll administration, tax reporting, and evidence of approvals. The IRS doesn't mandate a system, but records must clearly show income and expenses; keep employment-tax records at least four years.

3 · Employment & workplace controls

Worker classification, payroll/time records, minimum wage and overtime, anti-discrimination, workplace safety, and state-specific requirements. FLSA sets the floor; FMLA generally triggers at 50+ employees, which is why an applicability matrix matters.

4 · Data, privacy & security controls

Even with no sector-specific law, you hold employee, prospect, customer, and vendor data. A sensible default is NIST CSF 2.0, positioned as voluntary, adaptable guidance for organizations of any size and maturity.

5 · Truthful marketing & fair customer treatment

Commercial email must meet CAN-SPAM: truthful headers, a physical address, a working opt-out honored within 10 business days, applied to B2B as well as consumer email. Telemarketing adds disclosure, misrepresentation, calling-time, and Do-Not-Call controls.

6 · Accessible, safe delivery

Businesses open to the public provide equal access under ADA Title III, including policies, communications, and (per DOJ guidance) websites. OSHA duties apply wherever employees face workplace hazards.

STANDARDS TO PRIORITIZE

Don't certify against everything. Use standards as implementation tools, in this order.

PRIORITY	FRAMEWORK	BEST USE
Start here	**NIST CSF 2.0**	Organizes cyber governance around risk, accountability, protection, detection, response, and recovery.
Start here	**COSO Internal Control**	Finance, approvals, separation of duties, fraud prevention, and management oversight.
Start here	**CIS Controls**	A more prescriptive technical-security implementation baseline than NIST CSF.
When selling B2B	**SOC 2**	The customer-assurance report for SaaS, managed services, and data-handling firms.
International / enterprise-led	**ISO 27001**	A formal information-security management system, often requested by larger customers.
When card data is handled	**PCI DSS**	Contractual security standard required through payment-card relationships.
For operational maturity	**ISO 9001**	Repeatable service/product quality, documented processes, corrective actions.
For higher safety exposure	**ISO 45001**	Structured occupational health and safety management.

SECTOR-TRIGGERED REQUIREMENTS

The baseline expands quickly for certain business models. Map yours before you build.

Healthcare
HIPAA/HITECH, potentially FDA rules for regulated products, and state health-privacy laws.

Financial services, tax, lending, insurance, advice
GLBA Safeguards Rule, state licensing, and AML/BSA or regulator-specific rules by activity. Covered FTC-regulated institutions must safeguard customer information; certain breaches involving 500+ consumers are reported to the FTC within 30 days of discovery.

Government contractors
FAR/DFARS clauses, NIST SP 800-171 or CMMC where applicable, and procurement-integrity and flow-down controls.

E-commerce, subscription, consumer apps
Sales-tax nexus, state privacy laws, auto-renewal/negative-option rules, consumer refunds, product safety, and card security.

Manufacturing, construction, food, transport, chemicals
OSHA plus potentially EPA, FDA/USDA, DOT, state environmental permits, product-safety, and quality-system requirements.

Businesses processing children's data
COPPA and its heightened parental-consent and data-practice obligations.

Multi-state employers
State and local pay transparency, paid leave, wage-and-hour, worker classification, privacy, and personnel-file rules.

The distinction that saves money: NIST CSF, CIS Controls, SOC 2, ISO 27001, and ISO 9001 are frameworks, attestations, and voluntary standards, not laws. They become commercially mandatory the moment a customer contract, insurer, lender, partner, or regulator requires them. PCI DSS is the common exception, because payment-card acceptance agreements drive it. The control you skip is fine, right up until it is the deal you lose.

Then AI arrives, across all of it at once

AI doesn't pick one function. It enters hiring, marketing, finance, service, and operations at the same time, under the rules those functions already carry. The one new habit: each month, an owner pulls the actual decisions your AI made and reads all three layers of consequence. Not the vendor's dashboard, the decisions themselves. For an AI-specific reference, start with the NIST AI Risk Management Framework.

LAYER 1 · INTENDED
What was it built to do, and is it doing that, correctly?

LAYER 2 · BUSINESS
Who does it save money on, and who does it quietly cost?

LAYER 3 · UNSEEN
Would we stand behind these decisions if read back in a deposition?

THE OPERATING MODEL

Package the map as a minimum viable governance program, not a policy binder. Six moving parts, each with an owner and a review date.

1 · Applicability Register

- Jurisdictions, industries, headcount thresholds
- Data types, payment methods, regulated customers
- Customer & vendor contract obligations

OWNER + REVIEW DATE

2 · Risk Register

- Financial, legal, cyber, people, customer
- Operational, vendor, continuity
- Control + where the evidence lives

OWNER + REMEDIATION DATE

3 · Approval Matrix

- Spend, payroll, contracts, new vendors
- Pricing exceptions, access, data sharing
- Marketing claims, refunds, exceptions

NAMED ROLES, NOT "WHOEVER CLICKED"

4 · A Small Policy Set

- Conduct, information security, acceptable use
- Privacy/retention, HR/anti-harassment
- Procurement, incident response, continuity

ONE OWNER PER POLICY

5 · Evidence in the Workflow

- Approvals, logs, training, exceptions
- In HRIS, accounting, CRM, ticketing, IAM
- Not in email threads no one can find

SYSTEM OF RECORD, NOT THE INBOX

6 · Quarterly Governance Review

- Risk changes, incidents, access exceptions
- Overdue tests, vendor issues, complaints
- Finance anomalies, training, reg changes

C-SUITE TEAM, ONCE A QUARTER

Start here, this quarter

1. **Name the owner.** One person, with authority to pause a tool, owns the register and the monthly AI read.
2. **Build the applicability register first.** You cannot govern what you haven't mapped. It tells you which of the rules on page 1 and 3 are actually yours.
3. **Set the quarterly review.** Put it on the calendar, give it the risk register, and let the evidence come from the systems you already run.

The backbone

NIST CSF 2.0 + COSO
+ a legal applicability matrix

Use this as the spine for an SMB assessment or service catalog, then add HR, marketing, customer, and operations as function modules. A common language, without treating every framework as a mandatory law.

You've got the map. Standing it up is the work. *That's what we do. Let's talk.*

digitalbard.co/contact

General information, not legal advice. Confirm what applies to your business before you rely on it.