CTRL THE FUTURE LLC

GOVERNANCE READINESS GUIDE

A practical self-review for leadership oversight, accountability, policy, risk ownership, and performance monitoring

Purpose: This guide helps organizations review foundational governance practices that support sound technology, cybersecurity, compliance, and risk decisions. It is intended as an initial readiness resource and does not constitute a formal audit, certification, or legal determination.

Organization: _____

Completed by: _____

Date: _____

How to Use This Guide

Review each governance area with appropriate leadership and operational stakeholders. Mark the response that best reflects the organization's current state and record evidence, ownership questions, or follow-up actions in the Notes column.

ESTABLISHED	PARTIAL	NOT ESTABLISHED	N/A
Consistently operating	Some elements exist	Absent or unknown	Not applicable

1. Leadership Oversight

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Leadership has defined responsibility for oversight of technology, cybersecurity, compliance, and organizational risk.	■	■	■	■	
Governance priorities are connected to business objectives and organizational strategy.	■	■	■	■	
Leadership receives timely information needed to make informed risk and technology decisions.	■	■	■	■	
Significant technology or risk decisions have a documented approval and escalation path.	■	■	■	■	
Governance responsibilities remain clear when organizational roles or leadership change.	■	■	■	■	

2. Roles, Accountability & Decision Rights

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Key governance roles and responsibilities are documented.	■	■	■	■	
Decision-making authority is defined for important technology, security, compliance, and risk matters.	■	■	■	■	
Risk owners are assigned for significant identified risks.	■	■	■	■	
Accountability for corrective actions and improvement initiatives is documented.	■	■	■	■	
Conflicts, exceptions, or unresolved issues can be escalated to an appropriate decision-maker.	■	■	■	■	

3. Policy & Procedure Governance

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Core organizational policies are inventoried and assigned owners.	■	■	■	■	
Policies are formally approved and reviewed on a defined schedule.	■	■	■	■	
Procedures support implementation of policy requirements in day-to-day operations.	■	■	■	■	
Policy exceptions are documented, approved, time-bound where appropriate, and reviewed.	■	■	■	■	
Employees can access the policies and procedures relevant to their responsibilities.	■	■	■	■	

4. Risk Governance

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
The organization has a consistent method for identifying and evaluating risk.	■	■	■	■	
Material risks are documented in a risk register or equivalent tracking mechanism.	■	■	■	■	
Risk treatment decisions - mitigate, transfer, avoid, or accept - are documented.	■	■	■	■	
Risk acceptance requires approval at an appropriate level of authority.	■	■	■	■	
Leadership periodically reviews significant risks and remediation progress.	■	■	■	■	

5. Compliance & Obligations

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Applicable legal, regulatory, contractual, and industry obligations are identified.	■	■	■	■	
Responsibility for monitoring relevant compliance obligations is assigned.	■	■	■	■	
Compliance requirements are translated into policies, controls, procedures, or operational practices.	■	■	■	■	
Evidence needed to demonstrate important requirements is retained and organized.	■	■	■	■	
Known compliance gaps are tracked through remediation or documented risk decisions.	■	■	■	■	

6. Third-Party Governance

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Important vendors and third parties are inventoried and assigned internal owners.	■	■	■	■	
Risk is considered before onboarding vendors that handle sensitive information or critical services.	■	■	■	■	
Contracts contain appropriate confidentiality, security, service, and incident-notification expectations.	■	■	■	■	
Critical or higher-risk vendors are periodically reviewed.	■	■	■	■	
Vendor termination or offboarding includes removal of access and appropriate handling of organizational data.	■	■	■	■	

7. Performance Monitoring & Reporting

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Leadership has defined meaningful governance, risk, compliance, or security indicators.	■	■	■	■	
Reports focus on decisions, trends, risks, and actions rather than activity counts alone.	■	■	■	■	
Material issues are reported to the appropriate level of leadership.	■	■	■	■	
Remediation commitments are tracked against owners and target dates.	■	■	■	■	
Governance metrics and reporting are periodically reviewed for continued usefulness.	■	■	■	■	

8. Documentation & Records

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Important governance decisions are documented sufficiently to establish accountability.	■	■	■	■	
Meeting decisions, approvals, exceptions, and action items are retained when appropriate.	■	■	■	■	
Records have defined retention and disposal expectations.	■	■	■	■	
Sensitive governance records are protected from unauthorized access or alteration.	■	■	■	■	
Documentation is organized so important evidence can be located when needed.	■	■	■	■	

9. Change & Technology Governance

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Significant technology initiatives receive appropriate business, risk, security, and compliance review.	■	■	■	■	
Technology changes have defined ownership and approval requirements.	■	■	■	■	
New systems, cloud services, or AI capabilities are evaluated before adoption when they may create material risk.	■	■	■	■	
Major changes include consideration of data, access, vendor, resilience, and regulatory impacts.	■	■	■	■	
Post-implementation issues and lessons learned are incorporated into future decisions.	■	■	■	■	

10. Continuous Improvement

Governance readiness statement	Established	Partial	Not Est.	N/A	Notes
Governance practices are periodically assessed for effectiveness.	■	■	■	■	
Audit findings, incidents, assessments, and lessons learned inform improvement priorities.	■	■	■	■	
Improvement initiatives have owners, resources, and realistic target dates.	■	■	■	■	
Leadership periodically reassesses governance priorities as risks, regulations, and technology change.	■	■	■	■	
The organization maintains a practical roadmap for strengthening governance maturity.	■	■	■	■	

Governance Readiness Summary

Use this summary to identify the governance areas that warrant leadership attention. Readiness results should be interpreted in organizational context; they are not a certification or compliance determination.

Priority Area	Observation / Gap	Accountable Owner	Target Date
1.			
2.			
3.			
4.			
5.			

Suggested Next Steps

1. Discuss Partial and Not Established responses with the leaders responsible for those areas.

2. Identify governance gaps that could materially affect organizational objectives, regulatory obligations, technology decisions, or risk management.

3. Assign accountable owners and define practical corrective actions.

4. Establish target dates, evidence expectations, and a method for monitoring progress.

5. Reassess governance readiness periodically and after significant organizational or technology changes.

Need help strengthening governance?
CTRL The Future LLC can help organizations clarify governance structures, strengthen policies and accountability, organize risk ownership, improve oversight, and develop practical governance improvement roadmaps.

Disclaimer: This guide is provided for general informational and readiness purposes only. It does not constitute legal advice, regulatory certification, a formal audit, or a guarantee of governance effectiveness. Organizations should evaluate requirements applicable to their specific circumstances.