A3INFOSEC EXECUTIVE PLAYBOOK

AI Governance Operating Model

How SaaS organizations can establish clear AI accountability, risk-based lifecycle governance, AIBOM traceability, and continuous assurance.

FOR SAAS EXECUTIVES, CISOs, AI LEADERS & GRC TEAMS

A PRACTICAL GOVERNANCE ARCHITECTURE

DECISION RIGHTS

Who may approve, accept, or escalate AI risk

LIFECYCLE CONTROLS

How governance follows AI from intake to retireme

CONTINUOUS ASSURANCE

How evidence and signals sustain oversight

A3INFOSEC

GRC Advisory for Confident, Scalable Growth

www.a3infosecllc.site

A3INFOSEC

00

How to Use This Playbook

A practical reference for designing, implementing, and scaling AI governance as an operating capability.

This playbook is intended for SaaS executives, CISOs, CIOs, product and engineering leaders, legal and privacy teams, GRC leaders, internal audit partners, and AI governance stakeholders.

Use case	Recommended approach	Expected output
Executive alignment	Use Sections 1-4 to define scope, principles, accountability, and decision authority.	An executive mandate and governance charter.
Program design	Use Sections 5-10 to build the inventory, lifecycle, vendor, control, and assurance architecture.	A practical target operating model.
Implementation	Use the roadmap, maturity model, and worksheets.	A 90-day pilot and scaling plan.
Program optimization	Use the metrics, failure patterns, and continuous-assurance sections.	A prioritized improvement backlog.

CORE PRINCIPLE

AI governance should enable responsible adoption and defensible decisions. It should not become a policy layer disconnected from product, engineering, data, security, privacy, procurement, and customer commitments.

00

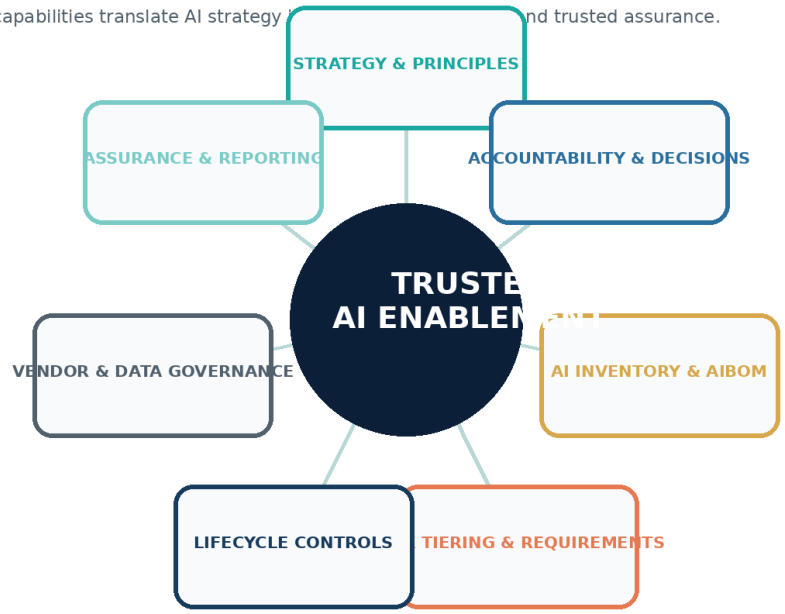
Executive Summary

AI governance becomes durable only when it is embedded in how the organization approves, builds, buys, changes, monitors, and retires AI.

A3INFOSEC

THE AI GOVERNANCE OPERATING MODEL

Seven connected capabilities translate AI strategy [illegible] nd trusted assurance.



Many organizations begin AI governance with a committee, a policy, or an inventory exercise. Those are useful starting points, but they do not create an operating model. An operating model connects executive intent to recurring decisions, named owners, lifecycle workflows, controls, evidence, escalation, metrics, and continuous assurance.

- ☐ Establish executive authority and a clear business mandate.
- ☐ Maintain a reliable inventory and AIBOM for material AI use.
- ☐ Apply proportional governance through risk tiers and decision thresholds.
- ☐ Integrate governance into product, engineering, vendor, data, and change workflows.
- ☐ Define evidence and assurance requirements that continue after approval.
- ☐ Report AI exposure, confidence, exceptions, and decisions to executives.

EXECUTIVE TAKEAWAY

The goal is not to eliminate AI risk. The goal is to make AI risk visible, owned, governed, and proportionate to business value and potential harm.

A3INFOSEC

Why AI Governance Needs an Operating Model

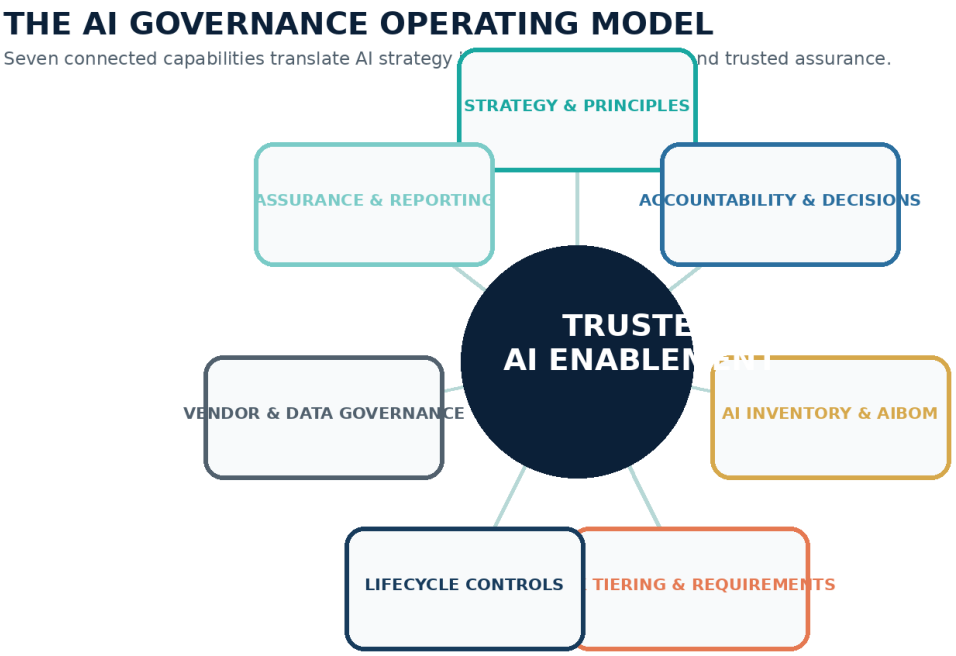
Common starting point	Why it is insufficient
AI policy	Describes expectations but does not create intake, review, decisions, ownership, or evidence.
AI committee	Creates discussion but may lack defined authority, service levels, and follow-through.
AI inventory	Shows what exists but not whether risk is acceptable or controls remain effective.
Legal review only	May miss technical, security, privacy, resilience, vendor, and operational risks.
Model monitoring only	Measures technical behavior but not governance conditions, approvals, or business impact.
Framework mapping	Supports completeness but does not define how work moves through the organization.

OPERATING-MODEL TEST

Can the organization consistently identify a material AI use case, classify it, assign owners, make an authorized decision, enforce conditions, monitor change, respond to failure, and prove what happened?

A3INFOSEC

The A3INFOSEC AI Governance Operating Model



Capability	Purpose	Primary outputs
Strategy and principles	Define where AI creates value and which boundaries apply.	AI principles, prohibited uses, priorities, risk appetite.
Accountability and decisions	Assign authority and escalation based on materiality.	Charter, roles, decision matrix, governance forums.
AI inventory and AIBOM	Create traceability across use cases, models, data, vendors, and dependencies.	Inventory, AIBOM, ownership, criticality.
Risk tiering and requirements	Apply proportional review and control depth.	Risk tiers, review paths, mandatory controls.
Lifecycle controls	Embed governance from intake through retirement.	Approvals, testing, change controls, closure evidence.
Vendor and data governance	Manage external AI, customer data, subprocessors, and contractual conditions.	Diligence, clauses, restrictions, reassessment.
Assurance and reporting	Evaluate whether governance remains effective.	Metrics, signals, exceptions, executive reporting.

03

Executive Mandate, Principles, and Scope

A durable program begins with an executive mandate that explains why AI governance exists, which decisions it supports, and what authority it has.

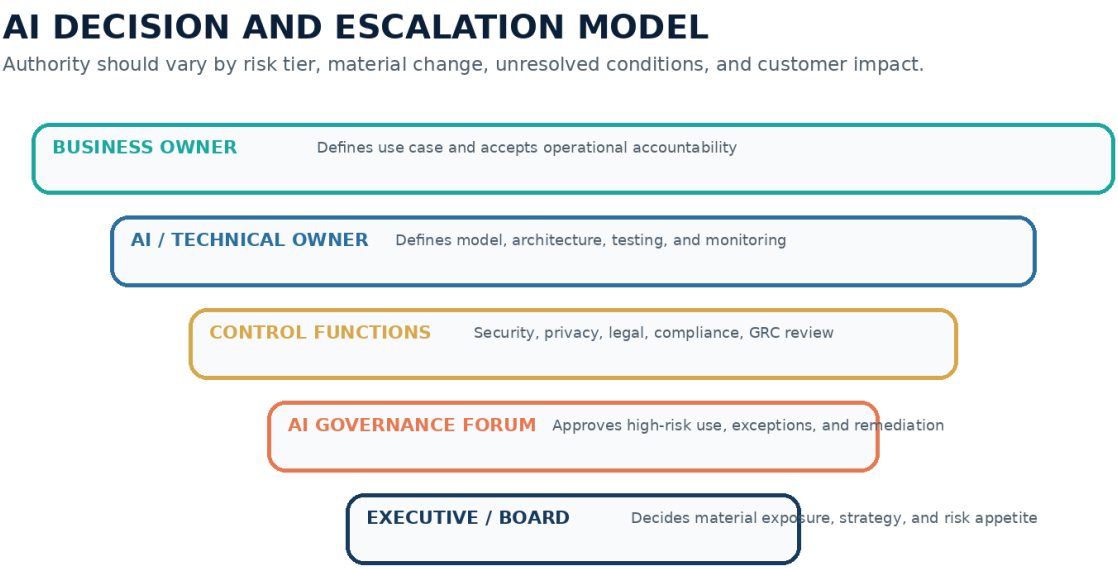
Design element	Questions to resolve
Business purpose	Which AI-enabled outcomes are strategic, experimental, operational, or prohibited?
Scope	Which internal tools, product features, vendors, models, agents, and automated decisions are covered?
Principles	What commitments apply to customer trust, privacy, security, transparency, reliability, and human oversight?
Risk appetite	Which impacts or uncertainties require restriction, executive acceptance, or prohibition?
Authority	Who may approve, conditionally approve, suspend, or accept residual AI risk?
Evidence	What must be documented so decisions remain defensible?

PRACTICAL SCOPE RULE

Govern the business use of AI, not only the underlying model. A low-risk model can still support a high-impact business process.

04

AI Accountability and Decision Rights



Role	Operating responsibility
Executive sponsor	Sets direction, resolves cross-functional conflict, and accepts material exposure.
AI governance lead / GRC	Owns the operating model, methods, governance cadence, and reporting.
Business owner	Defines purpose, value, users, affected stakeholders, and operating accountability.
Technical / model owner	Owns architecture, configuration, testing, monitoring, and technical change.
Data owner / privacy	Approves data use, retention, transfer, training, and privacy conditions.
Security	Evaluates architecture, access, abuse, supply chain, logging, and incident readiness.
Legal / compliance	Assesses obligations, claims, contracts, intellectual property, and regulatory exposure.
Internal audit / assurance	Provides independent challenge without assuming management ownership.

A3INFOSEC

AI Inventory and AIBOM Architecture

The inventory is the system of record for governance. The AIBOM provides deeper traceability into the components and dependencies that may change the risk profile.

Inventory domain	Example attributes
Use case	Purpose, users, decision supported, customer impact, owner, status.
Model / service	Provider, model name, version, hosting, fine-tuning, configuration.
Data	Input categories, customer data, sensitive data, training use, retention, residency.
Architecture	APIs, agents, tools, vector databases, retrieval sources, subprocessors.
Risk and decision	Tier, assessment date, conditions, approver, acceptance, next review.
Controls and evidence	Testing, access, monitoring, logs, human review, incident plan.
Change history	Model updates, prompt or workflow changes, new data, provider changes.

AIBOM VALUE

An AIBOM is valuable when it supports impact analysis, vendor oversight, incident response, customer assurance, change governance, and reassessment - not when it is only a static technical list.

06

Risk Tiering and Proportional Governance

Tier	Typical characteristics	Governance response
Tier 1 - Limited	Internal productivity, low sensitivity, reversible output, no material decisions.	Owner registration, approved tools, basic data and usage controls.
Tier 2 - Moderate	Operational workflow, customer-facing assistance,	Cross-functional review, testing, monitoring, change

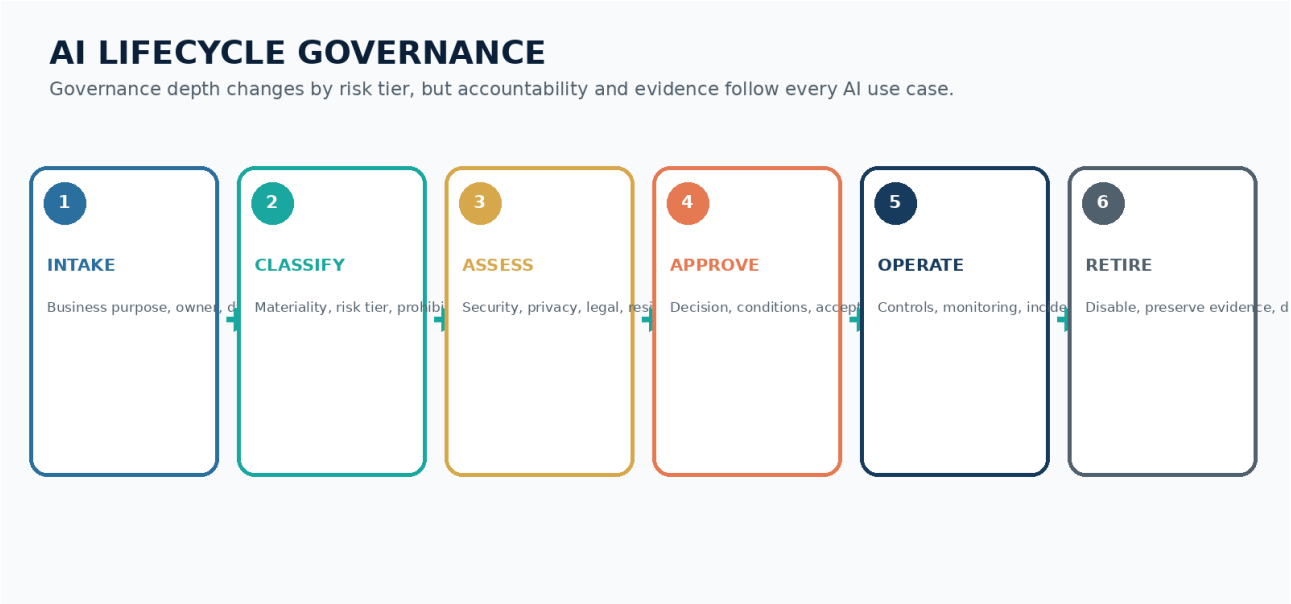
Tier	Typical characteristics	Governance response
	moderate data or reliability concerns.	notification.
Tier 3 - High	Material customer, legal, financial, security, privacy, or safety impact.	Formal approval, documented controls, executive visibility, enhanced assurance.
Prohibited / restricted	Unacceptable purpose, data use, autonomy, opacity, or unresolved exposure.	Do not deploy unless the restriction is changed by authorized leadership.

Risk dimensions

- ☐ Impact on customers, employees, or the public.
- ☐ Sensitivity and permitted use of data.
- ☐ Degree of autonomy and human review.
- ☐ Reliability, explainability, and reversibility.
- ☐ Security, abuse, and supply-chain exposure.
- ☐ Regulatory, contractual, and reputational consequences.
- ☐ Uncertainty, model change, and vendor transparency.

07

AI Lifecycle Governance



Lifecycle stage	Required governance outcome
Intake	A complete business, data, architecture, vendor, and ownership record.
Classify	A documented risk tier, required reviewers, and prohibited-condition check.
Assess	A decision-useful evaluation of material risks, controls, uncertainty, and evidence.
Approve	A named authority, decision rationale, conditions, exceptions, and review date.
Operate	Ongoing monitoring, incident readiness, owner attestation, and change governance.
Retire	Controlled shutdown, data disposition, dependency update, and preserved evidence.

08

AI Change Governance

AI risk can change without a new product launch. Model versions, prompts, retrieval sources, tools, datasets, vendors, and user populations can materially alter behavior or exposure.

Change trigger	Examples	Required response
Model change	Provider update, model replacement, fine-tuning, parameter change.	Impact review, targeted retesting, AIBOM update, approval if material.
Data change	New customer data, sensitive data, training use, retention, source.	Privacy and security review, contract validation, control update.
Architecture change	Agent, tool use, vector database, API, autonomous action.	Threat review, access design, logging, failure containment.
Business-use change	New users, decisions, geography, customer promises, scale.	Reclassify risk, update owner and obligations, reassess controls.
Vendor change	Subprocessor, terms, location, model policy, incident.	Third-party reassessment and contractual response.

09

AI Vendor and Subprocessor Governance

Governance area	Practical requirements
Transparency	Model/service identity, hosting, subprocessors, locations, material dependencies.
Data use	Training use, retention, deletion, isolation, access, transfer, and customer options.
Security	Access control, logging, testing, incident notification, vulnerability and abuse management.
Reliability	Service levels, model changes, limitations, testing support, rollback or substitution.
Contract	Audit rights, change notice, breach obligations, data rights, indemnity, exit support.
Ongoing oversight	Reassessment triggers, external signals, incidents, performance, and customer concerns.

VENDOR-GOVERNANCE PRINCIPLE

The organization remains accountable for how third-party AI is used, even when it cannot inspect or control every model component.

10

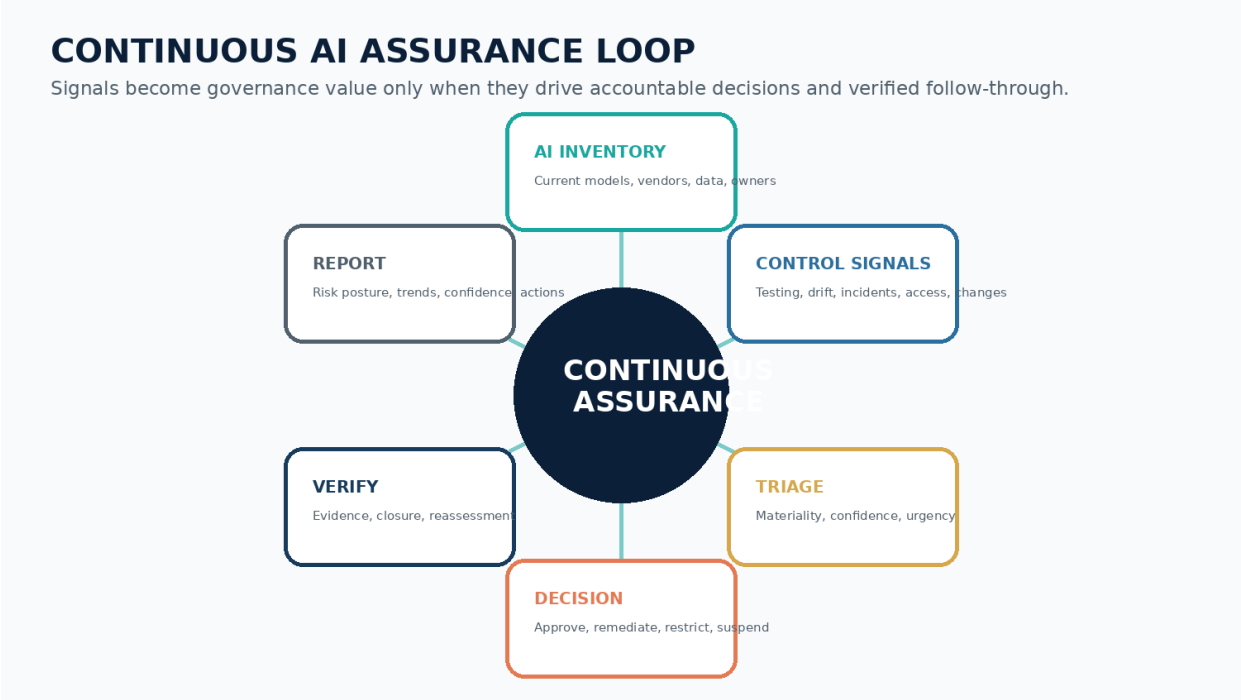
AI Control and Evidence Architecture

Control domain	Example control objective	Evidence examples
Governance	Material AI use is authorized and periodically reviewed.	Charter, minutes, approvals, decision log.
Inventory	AI uses and dependencies remain complete and current.	Inventory records, AIBOM, owner attestations.
Data	Data use is approved, minimized, protected, and retained appropriately.	Data-flow review, configurations, contracts, logs.
Security	AI access, architecture, tools, and abuse paths are controlled.	Threat model, access review, test results, monitoring.
Reliability	Performance and failure conditions are evaluated for intended use.	Evaluation plan, benchmarks, red-team results,

Control domain	Example control objective	Evidence examples
		thresholds.
Human oversight	Required human review and intervention remain effective.	Workflow records, overrides, sampled decisions.
Change	Material changes are identified, assessed, approved, and evidenced.	Change tickets, retest results, updated AIBOM.
Incident and exception	Failures, policy deviations, and accepted risk are governed.	Incident records, exceptions, remediation, closure proof.

11

Continuous AI Assurance



Continuous assurance combines technical and governance signals with human review, materiality, decision authority, and verified follow-through.

Signal category	Examples
Inventory and ownership	Unowned use cases, stale records, missing AIBOM components.

Signal category	Examples
Model and performance	Drift, benchmark decline, unsafe output, reliability threshold failure.
Security and abuse	Unauthorized use, prompt injection, tool misuse, exposed data, abnormal access.
Vendor and dependency	Provider change, incident, new subprocessor, policy or location change.
Governance execution	Expired approval, overdue review, missing evidence, unresolved condition.
Customer and business impact	Complaints, incorrect decisions, contractual conflict, operational disruption.

12

Executive Metrics and Reporting

Executive question	Decision-useful measures
Where is AI creating material exposure?	High-risk use cases, prohibited conditions, concentration, customer impact.
Is ownership working?	Unowned assets, overdue reviews, unresolved decisions, owner actions.
Are controls trustworthy?	Control coverage, evidence confidence, failed tests, repeat conditions.
What is changing?	Material model, data, vendor, architecture, and business-use changes.
Are we responding effectively?	Incident severity, issue aging, exception duration, remediation completion.
Is governance enabling the business?	Review cycle time, approved innovation, customer assurance, reuse of controls.

REPORTING RULE

Executives need decisions, exposure, trend, confidence, and ownership - not a catalog of AI activities.

A3INFOSEC

13

Common AI Governance Failure Patterns

Failure pattern	Why it fails	Better practice
Policy without workflow	Expectations are not translated into execution.	Define lifecycle triggers, owners, decisions, evidence, and closure.
Committee without authority	Issues are discussed but not resolved.	Document decision rights, thresholds, and escalation.
Inventory without ownership	Records become stale and risk remains unmanaged.	Require named business and technical owners with attestations.
One review for all AI	Low-risk work is slowed while high-risk work lacks depth.	Use risk tiers and proportional requirements.
Approval as the finish line	Risk changes after launch.	Use change governance and continuous assurance.
Vendor reliance	Provider claims substitute for internal accountability.	Define internal controls, contract conditions, and reassessment.
Framework-first design	Control lists replace operating logic.	Design the business operating model first, then map frameworks.
Premature automation	Poor definitions and workflows are embedded in tools.	Pilot, standardize, and measure before automating.

14

AI Governance Maturity Model

Level	Characteristics	Next priority
1 - Reactive	AI use is discovered informally; accountability and records are inconsistent.	Establish mandate, scope, inventory, and immediate restrictions.
2 - Repeatable	Basic policy, intake, and reviews exist but vary by team.	Standardize tiers, roles, decisions, lifecycle, and evidence.
3 - Integrated	AI governance is embedded in product, engineering, vendor, data, and change workflows.	Strengthen controls, metrics, and cross-functional assurance.

Level	Characteristics	Next priority
4 - Assured	Continuous signals, trusted evidence, and executive reporting support timely action.	Improve automation, confidence, and exception governance.
5 - Adaptive	Governance anticipates strategic change and supports responsible AI at scale.	Maintain agility, resilience, and measurable business value.

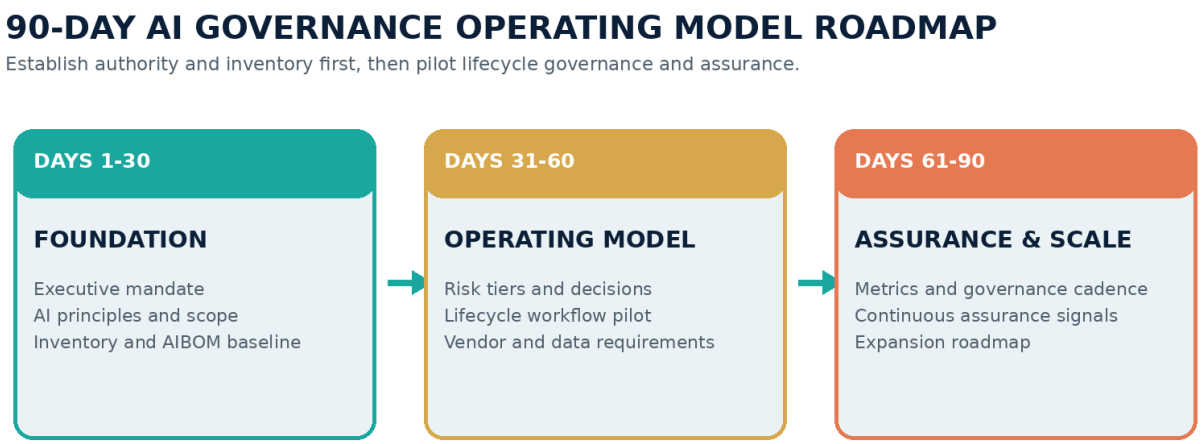
AI Governance Self-Assessment

#	Statement	Score 1-5
1	Executive sponsorship and authority are documented.	___
2	AI principles and prohibited uses are understood.	___
3	Scope includes internal, product, vendor, and embedded AI.	___
4	Material AI use cases have business and technical owners.	___
5	The AI inventory is complete enough to support decisions.	___
6	AIBOM information is maintained for material dependencies.	___
7	Risk tiers and review requirements are standardized.	___
8	Decision and risk-acceptance authority are clear.	___
9	Product and engineering workflows include AI governance triggers.	___
10	Material model, data, vendor, and architecture changes trigger reassessment.	___
11	Vendor AI diligence and contract requirements are defined.	___
12	Customer-data use and training conditions are controlled.	___
13	High-risk AI has documented testing and human oversight.	___
14	AI incidents and exceptions follow defined workflows.	___

#	Statement	Score 1-5
15	Control evidence is retained and traceable.	___
16	Continuous-assurance signals are triaged by materiality.	___
17	Executive metrics show exposure, confidence, and ownership.	___
18	Governance forums produce decisions and follow-through.	___
19	Automation is applied only to stable workflows and trusted data.	___
20	The program can demonstrate responsible AI enablement and measurable improvement.	___

Score	Current state	Recommended focus
20-39	Reactive	Establish authority, inventory, restrictions, and priority ownership.
40-59	Repeatable	Standardize risk tiers, lifecycle decisions, vendor/data controls, and evidence.
60-79	Integrated	Embed governance into business workflows and strengthen assurance.
80-100	Assured / adaptive	Improve automation, intelligence, resilience, and strategic value.

Practical 90-Day Roadmap



Phase	Primary objective	Key actions	Outputs
Days 1-30	Create authority and visibility.	Confirm sponsor and scope; approve principles; identify owners; establish inventory and AIBOM baseline; define immediate restrictions.	Charter, principles, initial inventory, priority risk list.
Days 31-60	Pilot the operating model.	Define risk tiers, review paths, decisions, lifecycle workflow, vendor/data requirements, control evidence; pilot real use cases.	Risk model, workflow, decision matrix, pilot records.
Days 61-90	Establish assurance and scaling.	Launch governance cadence; define metrics and signals; formalize change, incident, and exception governance; prioritize integrations and expansion.	Scorecard, assurance plan, improvement backlog, next-quarter roadmap.

Guided Worksheets

Editable tools for implementing the operating model.

A3INFOSEC

Worksheet 1 - Executive AI Governance Charter

Field	Your design
Business purpose	
Executive sponsor	
Scope	
Principles	
Prohibited uses	
Risk appetite	
Decision forums	
Reporting cadence	
Success measures	

Worksheet 2 - AI Use-Case Intake

Field	Response
Use case and purpose	
Business owner	
Technical owner	
Users and affected parties	
Model / vendor	

Field	Response
Data used	
Decision or output	
Human oversight	
Customer impact	
Target launch / status	

Worksheet 3 - AIBOM Record

Component	Provider / source	Version / location	Owner	Change trigger
Model / service				
Dataset / retrieval				
Prompt / agent / workflow				
Tool / API				
Vector database				
Subprocessor				

Worksheet 4 - AI Risk Tiering

Risk dimension	Assessment	Evidence	Result
Business impact			

Risk dimension	Assessment	Evidence	Result
Customer / employee impact			
Data sensitivity			
Autonomy / human review			
Reliability / reversibility			
Security / abuse			
Legal / regulatory			
Vendor / dependency			
Uncertainty / change			

Worksheet 5 - Decision Rights Matrix

Decision	Recommend	Approve	Execute	Verify / challenge	Escalate
Approve Tier 1 use					
Approve Tier 2 use					
Approve Tier 3 use					
Accept residual risk					
Approve exception					
Suspend AI use					
Approve material change					

A3INFOSEC

Worksheet 6 - Lifecycle Control Plan

Stage	Control / requirement	Owner	Evidence	Frequency
Intake				
Classification				
Assessment				
Approval				
Operation				
Change				
Incident / exception				
Retirement				

Worksheet 7 - Vendor AI Review

Area	Questions / requirements	Evidence / result
Service and model transparency		
Data use and training		
Security and access		
Reliability and change notice		
Subprocessors and locations		
Contract and exit		

Area	Questions / requirements	Evidence / result
Ongoing monitoring		

Worksheet 8 - Continuous Assurance Planner

Signal	Source	Threshold	Owner	Response

Worksheet 9 - Executive AI Scorecard

Metric / signal	Why it matters	Threshold	Owner	Decision

Metric / signal	Why it matters	Threshold	Owner	Decision

Worksheet 10 - 90-Day Action Plan

Period	Outcome	Actions	Owner	Measure	Review decision
Days 1-30					
Days 31-60					
Days 61-90					

Leadership Takeaways

01 AI governance must be designed as an operating model, not only a policy or committee.

02 Business and technical owners remain accountable for AI use and outcomes.

03 Inventory and AIBOM traceability are foundational to risk, change, incident, and assurance processes.

04 Risk tiers should determine review depth, decision authority, and control requirements.

05 Governance must be integrated into product, engineering, vendor, data, and change workflows.

06 Approval is not the finish line; AI risk changes after deployment.

07 Vendor AI does not transfer accountability away from the SaaS organization.

08 Continuous assurance combines technical signals with governance decisions and verified follow-through.

09 Executive reporting should emphasize exposure, ownership, trend, confidence, and decisions.

10 A focused 90-day pilot can establish a reusable model without overbuilding the program.

How A3INFOSEC Can Help

Practical advisory support for building and scaling responsible, audit-ready AI governance.

At A3INFOSEC, we help organizations build and scale GRC programs that do more than check boxes - we embed governance into the fabric of the business.

Our services are designed to reduce complexity, strengthen accountability, and align security and compliance with strategic growth.

Core service	How it helps
AI Governance & AIBOM Readiness Evaluation	Assess AI inventory, risk tiering, vendor transparency, data use, change governance, exceptions, evidence, and executive reporting.
GRC Program Design & Maturity Roadmaps	Build tailored governance structures that align with the business model and scale with operational needs.
Compliance Readiness & Automation	Align SOC 2, ISO 27001, NIST, and other requirements with streamlined, audit-ready workflows.
Third-Party Risk Management	Strengthen vendor oversight, automated assessments, SLA tracking, and platform integration.
Policy & Control Frameworks	Create centralized, framework-aligned policies and controls built for clarity, adoption, and defensibility.
GRC Platform Implementation	Evaluate, configure, and optimize platforms such as ServiceNow, RiskConnect, and OneTrust.

We partner with security and compliance leaders to operationalize trust, drive continuous assurance, and support growth with confidence.

A3INFOSEC

GRC ADVISORY FOR CONFIDENT, SCALABLE GROWTH

Start with a focused AI governance and AIBOM readiness discussion.

www.a3infosecllc.site