Perfect — you've now reached **Layer 7: Governance & Compliance**, the layer that gives your entire Web3 security architecture **policy, accountability, and provable trust**.
It's where **rules, roles, and evidence** live — ensuring that every change, deployment, and decision is auditable, approved, and compliant.

Below is the **complete breakdown** — main types, subtypes, components, and features — designed for Web3 ecosystems (smart contracts, bridges, wallets, validators, dApps, APIs).

🏛 GOVERNANCE & COMPLIANCE LAYER — COMPLETE STRUCTURE

#	Main Type	Subtype	Core Features / Components	Purpose / Outcome	Example Tools / Stack
1	**Governance Policy & Framework**	Policy Definition	Security and change policies (CODEOWNERS, SECURITY.md)	Define decision authority and process	GitHub CODEOWNERS, OPA, ISO 27001 docs
	Governance Model	DAO charters, roles, voting rights	Describe who governs and how votes count	Snapshot, Aragon, Safe DAO	
	Delegation & Hierarchy	Owner → sub-DAO → guardian	Delegate authority safely	Compound Gov, Governor Bravo	
	Versioned Policies	Changelog and approval tracking	Keep auditable policy history	Git tags, semantic versioning	
2	**Access & Authorization Governance**	Role-Based Access Control (RBAC)	Roles → permissions mapping	Enforce least privilege	OpenZeppelin AccessControl, OPA policies
	Attribute-Based Access Control (ABAC)	Contextual policies (geo, device, time)	Dynamic authorization logic	OPA Rego	
	Key Custody Governance	MPC rotation, multisig thresholds	Manage cryptographic authority	Safe, Fireblocks, tKey	

#	Main Type	Subtype	Core Features / Components	Purpose / Outcome	Example Tools / Stack
	Separation of Duties	Approve / execute split	Mitigate insider risk	DAO 2-of-3 approvals	
3	**Change Management & Approval Flow**	Code Review Policies	Mandatory PR reviews, sign-off	Prevent unauthorized changes	GitHub branch rules, CODEOWNERS
	Security Review Gate	Security team approval for critical files	Formal sign-off	Protected branch + CI checks	
	Change Advisory Board (CAB)	Off-chain review committee	Govern protocol upgrades	DAO proposal → multisig vote	
	CI/CD Promotion Gates	Policy-as-code enforcement	Integrate approvals into pipeline	Open Policy Agent in GitHub Actions	
4	**Compliance & Regulatory Alignment**	Framework Mapping	Map controls → NIST, ISO, SOC2	Demonstrate standard alignment	Drata, Vanta
	Data Protection Compliance	GDPR, CCPA, PDPA rules	User data rights & consent tracking	Privacy APIs, de-identification	
	Financial / AML Compliance	KYC, sanctions list checks	Prevent illicit transactions	TRM Labs, Chainalysis, Merkle Science	
	Smart Contract Audit Compliance	External audit records	Prove contract security	CertiK, Trail of Bits	
	Reporting & Certification	SOC2, ISO certs, DAO proofs	Compliance artifacts	Audit reports, PDF evidence	
5	**Risk & Exception Management**	Risk Register	Track identified threats and owners	Visibility of risk surface	Jira, Notion Risk DB
	Exception Workflow	Record temporary policy bypass	Controlled risk acceptance	Signed risk acceptance forms	

#	Main Type	Subtype	Core Features / Components	Purpose / Outcome	Example Tools / Stack
	Compensating Controls	Temporary security measures	Mitigate accepted risk	Extra monitoring rule	
	Periodic Risk Review	Quarterly risk assessment	Re-evaluate threats	Audit committee review	
6	**Audit & Evidence Management**	Internal Audits	Review process & logs	Self-assurance	Internal audit scripts
	External Audits	Third-party assessment	Independent validation	Trail of Bits, Certora	
	Evidence Collection	Artifacts for controls	Prove compliance	Signed SBOM, attestations	
	Tamper-Evident Logs	Hash-chained records	Integrity of evidence	immudb, AWS QLDB	
7	**Policy-as-Code & Automation**	OPA Rego Policies	Automate approval logic	Continuous enforcement	Open Policy Agent, Conftest
	Infra Compliance Automation	Scan K8s / Terraform against rules	Prevent drift	Checkov, Terraform Sentinel	
	CI/CD Compliance Hooks	Pre-merge security gates	Enforce standards before deploy	GitHub Actions, GitLab CI	
8	**Transparency & Reporting**	Public Disclosure	Publish security.md & audit summaries	Build user trust	GitHub security.md
	Incident Disclosure	Post-mortems & RCA reports	Responsible communication	DAO blog posts	
	Metrics Dashboard	KPIs (SLA, MTTR, risk count)	Quantify governance health	Grafana Governance Board	
9	**DAO / On-Chain Governance (Web3-Specific)**	Proposal Lifecycle	Create → vote → queue → execute	Automate on-chain policy	Governor Bravo, SafeSnap

#	Main Type	Subtype	Core Features / Components	Purpose / Outcome	Example Tools / Stack
	Voting Mechanisms	Token weight, reputation, quadratic	Fair representation	Snapshot, Tally	
	Treasury Governance	Multi-sig approvals, fund release	Financial accountability	Gnosis Safe, Aragon	
	DAO Compliance	Legal entity wrappers	Regulatory recognition	Opolis, LexDAO	
10	**Education & Culture of Accountability**	Security Awareness Training	Periodic training & quiz	Empower team security culture	SecurityHub LMS
	Policy Onboarding	New member briefing	Ensure understanding	DAO onboarding portal	
	Gamified Compliance	Badges, scores for policy adherence	Incentivize good behavior	OpenBadge, Coordinape	

Hierarchy Summary

Main Type	Subtypes	Core Goal	Outcome
Governance Policy & Framework	4	Define structure and rules	Clear decision authority
Access & Authorization Governance	4	Enforce control of privileges	Least-privilege operations
Change Management & Approval Flow	4	Control code and protocol changes	Auditable review trail
Compliance & Regulatory Alignment	5	Meet industry standards	External trust and certification
Risk & Exception Management	4	Handle known risks formally	Reduced unknown exposure
Audit & Evidence Management	4	Prove security controls exist	Regulatory and DAO assurance

Main Type	Subtypes	Core Goal	Outcome
Policy-as-Code & Automation	3	Automate governance checks	Continuous compliance
Transparency & Reporting	3	Communicate performance & failures	Stakeholder trust
DAO / On-Chain Governance	4	Embed rules in smart contracts	Decentralized accountability
Education & Culture	3	Reinforce responsibility	Human compliance layer
TOTAL	**38 subtypes / 150 + features**		

⚙️ Rust / Web3 Integration Example

```
/governance_compliance/
  ├─ policy_framework.rs       # versioned CODEOWNERS, rules, sign-offs
  ├─ access_governance.rs      # RBAC / ABAC policies via OPA
  ├─ change_control.yaml       # PR approval + promotion gates
  ├─ compliance_mappings.yaml  # ISO/NIST/SOC2 mapping
  ├─ risk_register.json        # tracked risks & exceptions
  ├─ audit_evidence/           # signed SBOMs & reports
  ├─ policy_as_code/           # Rego policies for CI/CD
  ├─ transparency/             # dashboard metrics & disclosures
  ├─ dao_governance.rs         # on-chain proposals & votes
  └─ education_portal.md       # awareness & onboarding docs
```

Each commit, deployment, and vote produces **governance evidence** stored in your repository and audit vault.

📊 Governance & Compliance KPIs

Metric	Target	Meaning
Policy Coverage	≥ 95 % repos with CODEOWNERS	Governed repos
Change Approval Rate	100 % critical changes signed	No unauthorized push
Audit Finding Closure Time	≤ 14 days	Fix speed
Training Completion	≥ 90 % staff trained	Culture adoption
Compliance Drift	< 5 % of configs non-compliant	Automation effectiveness
DAO Proposal Participation	≥ 60 % quorum	Governance engagement

☑ Purpose in the Cyber-Defense Stack

Layer	Role
Security Layers	Define what must be protected
Protection Layers	Contain attacks in runtime
Detection & Response	See and react in real time
Resilience & Recovery	Bounce back from failure
➡ **Governance & Compliance**	Prove ownership, accountability, and trust

---

Would you like me to output this as a **CSV matrix**
(`layer,type,subtype,features,goal,tools,metrics,evidence`)
so you can merge it into your **Security + Detection + Resilience dashboards**?