未来 Web Governance Console 演进蓝图（AI-First 生态治理界面）

> 定位声明： **Web Governance Console 不是“后台系统”，而是 AI-First Governance Platform API 的“制度可视化外壳”。** 权力永远在 API，界面只是让人类“看见、理解并合法签字”。

一、总体演进哲学（必须先统一认知）

三条不可动摇原则

1. **API Sovereignty（API 主权）**
   所有治理能力必须先存在于 Governance Platform API 中，UI 永远不得引入新权力。

2. **Read-Mostly, Sign-Only**
   90% 只读 + 10% 审批签字。UI 不做决策、不做计算、不做执行。

3. **Replaceable by Design**
   任意企业、第三方、甚至 K-OS 本身，都可以替换官方 UI，而不影响治理体系。

二、Web Governance Console 的最终角色

在生态中的位置

```
[ Human (Browser) ]
        ↓
[ Web Governance Console ]   ← 可替换、可定制
        ↓
[ Governance Platform API ]  ← 唯一权力中心
        ↓
[ AI-First Runtime ]
```

本质定义

> **Web Governance Console = Governance API 的“法律解释器 + 决策记录器”**

三、演进阶段总览（V0 → V4）

阶段	代号	核心目标	典型用户
V0	Shadow Mode	API 验证	内部工程师

阶段	代号	核心目标	典型用户
V1	Observatory	可视化治理	管理员 / 合规
V2	Decision Room	人类决策中枢	风控委员会
V3	Ecosystem Ops	能力生态运营	平台运营
V4	Federated Governance	跨组织治理	企业 / 联盟

四、各阶段详细设计

V0 · Shadow Mode（现在 → v3.1）

目标

- 验证 Governance API 是否“足够强大以支撑 UI”

形态

- CLI / TUI（你们已经完成）
- Swagger / Postman

关键指标

- UI 不存在，治理是否仍然成立
- 所有治理动作是否可被 API 驱动

✅你们当前已完成此阶段

V1 · Observatory（第一个 Web 版本）

定位

> **治理可观测，而非可操纵**

核心功能（100% 只读）

- Capability Health Map（热力图）
- Risk Level Distribution
- Signal Timeline（Rollback / Denied / Reject）
- Capability Demand Radar

设计要点

- 类 Grafana / Kibana
- 强时间轴、强因果链
- 不允许任何写操作

用户

- 企业 CTO
- 合规官
- 架构评审

V2 · Decision Room（治理决策室）

定位

> **人类介入 AI 的“合法签字室”**

新增能力

- Proposal Queue（FIX / SPLIT / FREEZE / PROMOTE）
- Proposal Diff View（为什么、基于什么）
- 双人 / 多人审批（4-eyes principle）
- 审批意见记录（Explainable Approval）

关键交互

- 每一次批准 = 一次“制度性事件”
- 自动生成 Governance Decision Record (GDR)

安全设计

- 强身份认证（SSO / MFA）
- 操作冷却时间（Anti-Impulse）

V3 · Ecosystem Ops（能力生态运营台）

定位

> **把“能力”当作产品来运营**

核心能力

- Capability Lifecycle Funnel
- Proposed → Active → Degrading → Frozen → Deprecated
- Capability ROI / Adoption
- AutoForge Pipeline 可视化
- Third-party Capability Review

新增角色

- Capability Operator
- Ecosystem PM

V4 · Federated Governance（联邦治理）

定位

> **多组织、多 Runtime 的治理协调层**

场景

- 集团公司
- 行业联盟
- 跨区域合规（EU / US / CN）

能力

- Governance Policy Federation
- Cross-Runtime Capability Trust
- Delegated Authority

五、与 K-OS / Ascend 的融合点

与 K-OS（认知中枢）

- 在 Proposal 中直接引用 Knowledge Package
- 审计视图可跳转到“知识依据”

与 Ascend（主动系统）

- Governance Console 作为 Ascend 的“理事会界面”
- 管理 Ascend 的 Intervention Policies

六、技术实现建议（给未来工程师）

技术栈建议

- Frontend：React / Next.js / SvelteKit（可替换）
- Data：Strict REST / GraphQL over Governance API
- Auth：OIDC / SAML

架构红线

- ❌前端不得缓存治理状态
- ❌前端不得计算 Health / Risk
- ❌前端不得直接访问 Runtime

七、终极判断标准（请写在 README 顶部）

> **If the UI disappears, governance must still work.**

这不是一个“好看的后台”，而是：

> **人类在 AI 系统中行使权力的宪法级入口。**

八、总结一句话

Web Governance Console 的终极形态不是“控制 AI”，而是：

> **让 AI 的行为第一次进入人类社会可理解、可审计、可问责的制度空间。**