

(32) The citizens' / owners' rights framework, attachments

13 out of 39 rights have more technical descriptions with examples. Those detailed description in some cases with examples are described.

Operational Note: Users must strictly review the "Disclaimer" (Document 53) [REF:D53] regarding operational risk assessments and liability limitations prior to deployment.

Rights Classification Labels

TCORF Rights are labeled using two categories to improve clarity and adoption:

- **[AUDIT EFFECT]:** rights require intake, documentation, publication, and preservation of evidence, but do not automatically block execution.
- **[HARD CONTROL]** rights allow an Owner to block, suspend, or refuse applicability of an action until defined conditions are met + [AUDIT EFFECT]

Both categories are audit benchmarks, not legal entitlements.

Both categories are audit benchmarks, not legal entitlements. In Active Mode, any real-world request must be grounded in applicable law, policy, contract, or stakeholder obligations—not in TCORF text alone.

On Numeric Thresholds

Where this framework specifies numeric thresholds (e.g., days, limits, quantities), these values are minimum audit thresholds, not claims of optimal policy design. Numeric values are required to ensure measurability and comparability. Any threshold necessarily involves normative choice; the absence of a number would make compliance non-auditable. Unless explicitly stated otherwise, values represent conservative lower bounds. Longer periods, higher standards, or stricter protections remain compliant.

Contents

Category 1: Foundational Governance	3
Category 2: Vital Protections	3
Category 3: Citizenship & Migration Control	3
Category 4: Mandate Authorization	3
13. Enforce High Standards for Voting [AUDIT EFFECT]	3
Category 5: Executive Accountability	5
15. Require Regular Q&A with the Press [AUDIT EFFECT]	5
Category 6: Systemic Transparency	8
16. Full Transparency of Public Orgs [AUDIT EFFECT]	8
17. Public Economic & Social Data [AUDIT EFFECT]	11
18. Transparent Tax Impact Metric [AUDIT EFFECT].....	16
Category 7: Environmental Integrity	17
22. Prevent Deforestation and Protect Nature [AUDIT EFFECT]	17
23. Open Access to Global Warming-related Data [AUDIT EFFECT]	19
Category 8: Economic Risk Governance	22
25. Mandatory Insurance for High-Risk Industry [AUDIT EFFECT]	22
26. Prevent the Abuse of Monopolies [AUDIT EFFECT]	27
27. Tariff Stability Safeguard [AUDIT EFFECT].....	31
Category 9: State Structure & Security	34
35. The Right to Surveillance Warnings [AUDIT EFFECT]	34
38. Voter Approval for Border Changes [AUDIT EFFECT]	37
39. Fair Pay to Prevent Corruption [AUDIT EFFECT]	40

Category 1: Foundational Governance

Category 2: Vital Protections

Category 3: Citizenship & Migration Control

Category 4: Mandate Authorization

13. Enforce High Standards for Voting [AUDIT EFFECT]

Extension ID: D32-R13-EXT

This **Shadow Audit Checklist** supports an evidence-based evaluation of a vote.

1) Voting Rules + Equal Conditions (0–500 days)

[] Indicators of a clear vote

- Voting laws/rules/conditions are stable and not materially changed within **~500 days** (~1.5 years) before the election
- Comparable voters face comparable rules (registration, deadlines, ID/eligibility checks, rejection reasons)

[] Indicators of an unclear vote

- Material rule changes inside ~500 days without clear justification and traceable review
- Similar voters face inconsistent rules by region/group without transparent explanation

[] Indicators of an unfair vote

- Authorities (police, tax/IRS, regulators, security services) suddenly investigate or pressure political rivals within ~500 days in a selective pattern

2) Voting Channels (In-Person / Mail / Digital)

[] Indicators of a clear vote

- Practical access existed (capacity, locations, timing allow realistic participation)
- If mail/digital is used: published traceability exists (requested → issued → delivered → returned → accepted → rejected + reason codes)
- If mail/digital is used: **≥ 90%** delivered and processed in time, and no region/group falls below **85%** without documented reasons

[] Indicators of an unclear vote

- Registration/ballot access delivered too late to matter
- Mail/digital rejection reasons are vague or missing
- Mail/digital metrics are unavailable or inconsistent with reported outcomes

[] Indicators of an unfair vote

- **Sudden large-scale granting of citizenship/voting rights within ~500 days** before the election, especially if concentrated in specific regions or groups and not clearly justified by transparent, rule-based criteria.
- Workplace pressure or retaliation threats tied to voting choice
- Vote buying (money, goods, services, or benefits in exchange for votes)
- Organized partisan transport of voters with opaque shuttle patterns
- Sudden massive relocation into specific voting circles shortly before voting without credible explanation

3) Candidate Field + Media Environment

[] Indicators of a clear vote

- Candidate/option list is published
- Removals/disqualifications are traceable (rule reference + reason + timing)

- Media access is not structurally monopolized and allows meaningful competition

[] **Indicators of an unclear vote**

- Major candidates/options disappear close to the election without a transparent evidence trail
- Media balance cannot be assessed because data, recordings, or logs are unavailable

[] **Indicators of an unfair vote**

- Only one candidate exists, or only “token” opponents exist without realistic ability to win
- Strong media imbalance systematically favors the ruling side (especially via state-linked channels)
- Unbalanced hostility / smear campaign targets political rivals, especially when amplified by state resources
- Political rivals are arrested or removed during the election period or within days after, without transparent due process evidence

4) Evidence Publication + QA Timing

[] **Indicators of a clear vote**

- Key evidence and datasets are published in a form third parties can review (not only statements)
- Independent QA review occurs before the result becomes official
- A meaningful QA window exists before official declaration (e.g., up to **24 hours**)

[] **Indicators of an unclear vote**

- Results become official immediately (“0-hour QA”), and review only happens afterward
- Only press statements exist without underlying evidence

[] **Indicators of an unfair vote**

- Independent reviewers are blocked or pressured from publishing findings

5) Counting, Audits, and Complaint Response

[] **Indicators of a clear vote**

- Precinct/location results were visible before central reporting
- Traceable custody exists (tamper-evident sealing / chain-of-custody evidence)
- Close-margin precincts received manual verification with public QA evidence
(simple guideline: margin $\leq 1\%$ triggers manual verification)
- A random manual audit occurred (e.g., **1 in 20 precincts (5%)** of remaining locations)
- If discrepancies exceed **2%** or show a pattern, verification expands toward a broader recount
- After complaints, the voting authority provides data/evidence quickly and enables inspection

[] **Indicators of an unclear vote**

- Results appear only centrally with no precinct-level visibility
- Audits/recounts are blocked, delayed, discretionary, or non-reproducible
- Complaint handling shows delay/refusal/minimal cooperation or missing evidence

[] **Indicators of an unfair vote**

- Organized chain voting (pre-marked ballots / ballot handoffs / ballot swapping)
- Multiple voting / repeat voting anomalies without transparent resolution
- Irregular security presence (police/security/military) at voting sites, counting centers, or auditor locations suggesting acceptance by pressure rather than clarity

Category 5: Executive Accountability

15. Require Regular Q&A with the Press [AUDIT EFFECT]

Extension ID: D32-R15-EXT

Preamble (economic rationale + scope):

In high-impact organizations, a core risk is **information asymmetry** — where those affected by decisions cannot observe how leadership acts or whether it delivers on its mandate. This leads to **principal-agent problems**, where decision-makers may shift costs, avoid feedback, or prioritize internal interests.

In any critical system **periodic operational monitoring** is normal: owners check reports, inspect performance, and ask questions.

In public-impact organizations, **citizens act as collective owners**. Because direct inspection by millions isn't feasible, the **only scalable substitute is structured, recorded Q&A** with the actual decision-makers.

These sessions create a time-stamped trail of:

- What the leadership **intended to do**,
- What it **actually did**, and
- What results followed.

This extension targets **decision authority**. “Leadership Q&A” means live participation by office-holders or executives with real approval power (or a clearly documented delegate). Sessions led only by PR staff or spokespeople are treated as **partial compliance**, unless the accountable leader appears regularly and accepts questions directly.

This **Shadow Audit checklist** helps an Owner evaluate whether senior leadership regularly faced real public questioning — and whether the interaction was informative, accessible, and unfiltered enough to be useful. Failure does not prove wrongdoing — it proves **information opacity and accountability avoidance risk**.

A) Practical Baseline: Frequency & Duration (by impact tier)

Impact Tiers (choose the closest match)

Tier 1 (highest impact): national leaders, cabinet-level roles, heads of police/intelligence, monopoly/dominant-market CEOs, top regulators

Tier 2: major agencies, regional leaders, large state entities, system-wide public service operators

Tier 3: local leaders, essential service providers, medium/large org leadership

Frequency requirement (minimum)

- **Tier 1:** at least **monthly**
- **Tier 2:** at least **quarterly**
- **Tier 3:** at least **bi-annually**

Duration requirement (keep it real, not symbolic)

A valid session should be **60–90 minutes total**, and include both:

- **Status report:** 10–30 minutes (operational baseline)
- **Live Q&A:** at least **45 minutes** (or **≥50%** of total time, whichever is greater)

Failure pattern: Q&A shrinks when controversy rises.

B) Topic Allocation Rules (minimum % of Q&A time)

The Q&A portion must show meaningful coverage of **mandate vs reality**.

Required topic categories (Q&A segment only)

1. **Mandate / Program / Authorization**

What leadership claimed it would do; what it is empowered to do; why current actions match the authorized program.

2. **Current Activity / Operations / Incidents**

What is happening now: performance, failures, incidents, delivery, backlog, safety, etc..

Minimum allocation (hard floor)

- **Mandate / Program / Authorization:** ≥30% of Q&A time
- **Current Activity / Operations / Incidents:** ≥30% of Q&A time
- Remaining ≤40% may cover any mix of: budgets, staffing, integrity/ethics, procurement, external affairs, strategic plans, emergencies, or other topics.

C) Shadow Audit Checklist — Press Q&A Clarity Indicators

1) Frequency & Occurrence (Did it happen often enough?)

Clear

- A recurring schedule exists and can be verified via dates, recordings, and archives.
- Sessions meet the minimum tier frequency (monthly/quarterly/bi-annual).

Unclear

- Irregular sessions or no publicly verifiable schedule.
- Q&A disappears during controversy or crisis.
- Partial archives (missing dates / missing recordings).

Unfair

- “Q&A” exists mainly as appearance: nominal format without real questioning.

2) Format & Time Allocation (Was time meaningful, not symbolic?)

Clear

- Total session is **60–90 minutes**
- **Q&A at least 45 minutes** (or ≥50% of total time, whichever is greater)
- Consistent duration patterns over time.

Unclear

- Q&A repeatedly shortened, rushed, or canceled.
- “Speech-only” sessions with minimal questions.
- Q&A time reduced when scrutiny rises.

Unfair

- “Q&A” exists but is structurally controlled (scripted prompts; no real questioning).

3) Topic Allocation (Did it cover mandate *and* current activity?)

Clear

- ≥30% of Q&A addresses **Mandate/Program/Authorization**.
- ≥30% addresses **Current Activity/Operations/Incidents**.
- Clear linkage between commitments/authority and real actions.

Unclear

- Status is vague; mandate is not discussed; operational facts are thin.
- Heavy drift into messaging with minimal measurable content.

Unfair

- Systematic avoidance of mandate alignment and operational facts (narrative-only Q&A).

4) Invitation Neutrality & Access (Who can ask?)

Clear

- Broad participation across major outlets; predictable access rules.
- Invitations and access details are published in advance.

Unclear

- Invite rules are hidden; participant list is unknown.
- Invite list changes without explanation.

Unfair

- Repeated exclusion of critical outlets while welcoming friendly ones.
- “Technical” barriers applied selectively (late links, selective seat limits).

5) Q&A Openness (Were questions real and unscripted?)

Clear

- Questions appear unscripted and include challenging topics.
- Multiple outlets participate; follow-ups sometimes allowed.

Unclear

- Questions are shallow due to constraints (strict time caps, no follow-ups).
- Session ends right as hard topics begin.

Unfair

- Pre-screened questions; advance submission required without transparency.
- Microphones cut, interruptions increase, or pressure escalates during sensitive questions.

6) Follow-up Mechanics (Do unanswered questions get resolved?)

Clear

- Clear follow-up channel exists (documents, deadlines, written responses).
- Corrections issued when mistakes are found.

Unclear

- “We’ll follow up” is common, but follow-ups don’t appear.
- Chronic deflection on operational questions.

Unfair

- Follow-ups are used selectively to reward friendly outlets and punish critics.

7) Personal Presence (Did the accountable leader show up?)

Clear

- Primary leader of the Organization attends most sessions; delegation is occasional and explained.

Unclear

- Frequent substitution by spokespersons without accountability follow-through.
- Leader appears mainly in low-pressure settings.

Unfair

- Systematic avoidance of direct questioning while relying on controlled messaging channels.

8) Transparency, Recording, and Archiving (Can Owners review later?)

Clear

- Recordings are accessible and uploaded reliably.
- Archives are stable over time (not quietly removed or altered).
- If edits occur (technical trimming), they are disclosed.

Unclear

- Missing recordings, broken links, partial footage (especially missing Q&A portion).

Unfair

- Recordings disappear after controversy.
- Re-uploads show missing sections without explanation.
- Access restricted behind paywalls/registration barriers for public entities.

9) Response Behavior Under Scrutiny (Do answers resolve questions?)

[] Clear

- Answers include commitments, timelines, documents, or verifiable next steps.
- Contradictions are acknowledged and addressed.

[] Unclear

- Repeated non-answers (“no comment,” vague deflection) on high-impact operational issues.

[] Unfair

- Retaliation, intimidation, or systematic exclusion follows tough questions.
- Visible chilling effect: fewer critical questions over time due to perceived punishment.

Category 6: Systemic Transparency

16. Full Transparency of Public Orgs [AUDIT EFFECT]

Extension ID: D32-R16-EXT

If stakeholders (“Owners” in TCORF terms) can automatically access the complete Activities & Agreements (A&A) dataset at the required granularity, update frequency, and organizational scope—through a central, public, searchable system that supports bulk download, machine processing, stable definitions, and independent QA/audit verification—then stakeholders are meaningfully informed about operational activity and spending.

This **Shadow Audit** tests four things:

1. Dataset exists (coverage + completeness)
2. Central access (public, searchable, stable)
3. Processability (bulk download + usable formats + clear definitions)
4. Verification (independent QA/audit)

Definitions (Plain Language)

A&A = “Activities & Agreements” (what should be disclosed)

A&A is a catch-all record set for any transaction, obligation, or operational commitment initiated by the organization, including (at minimum):

- Procurement & contracts: tenders, contracts, purchase orders, subcontracts
- Invoices & payments: invoices, receipts, disbursement orders, payment confirmations
- Financial obligations: loans, credits, guarantees, debt instruments, leasing obligations
- Projects & operations: operational projects, budgets per project, cost evolution
- Assets & structures: subsidiaries, outsourcing agreements, investments
- Transfers: donations, giveaways, grants/subsidies, forgiven debts
- Personnel spend: compensation structures and relevant commitments
- Domestic + international scope: records should identify whether counterparties/recipients are domestic or international (when applicable)

Exclusion (narrow): Only strictly deep military or intelligence operations may be exempt.

Boundary rule: Disclosure remains mandatory if something is merely labeled “military” but does not meet deep strategic confidentiality criteria.

DMS = Document Management System (what the portal should be)

A public, searchable Document Management System (DMS) is an online system that lets stakeholders:

- find A&A records centrally (not scattered across agencies),

- open the record,
- download documents and metadata,
- export records in bulk for analysis.

Shadow Audit Checklist — A&A Transparency

1) Dataset Existence + Central Access

Test: Does A&A exist as a usable public service in one central place?

PASS indicators

- One official portal exists where A&A records are centrally searchable
- Works without fees, registration, or tracking barriers

FAIL indicators

- Data exists only in scattered agency pages
- “Transparency” is PDF dumps without search or structured records

2) Scope Completeness (Coverage Test)

Test: Does A&A cover the organization’s full operational footprint?

PASS indicators

- A&A includes procurement + payments + obligations + subsidiaries + outsourcing + investments + transfers + personnel spend
- International / domestic classification exists where relevant

FAIL indicators

- Large categories missing (e.g., subcontracts, transfers, debt instruments)
- High-spend areas grouped under vague labels (“misc.” / “special initiative”)

3) Exclusion Clause Check (Deep Military / Intelligence Only)

Test: Are exemptions narrow and consistently justified?

PASS indicators

- Only “deep” military/intelligence operations are excluded
- Non-deep military labeled items remain disclosed (normal procurement, facilities, admin, etc.)

FAIL indicators

- Blanket “military” labeling used to hide ordinary spending
- Exemptions applied without boundary criteria

4) Record Metadata Integrity (Minimum Fields)

Test: Is each A&A entry auditable by default?

Each record should include these metadata fields:

1. Contractual Parties: Full identification of entities + subcontractors
2. Timeline: Signing date, effective date, duration
3. Purpose: Objectives + justification + assigned data owner
4. Geographic Impact: ZIP codes or geodata where executed
5. Financial Integrity: Total amount + involved assets + scanned originals
6. Lifecycle History: Extensions / modifications attached to original entry

PASS indicators

- Metadata fields are consistently present
- Extensions don’t “replace” prior records (history remains intact)

FAIL indicators

- Missing parties/subcontractors, missing amounts, no originals, no lifecycle history

5) Access Conditions + Data Portability

Test: Can stakeholders analyze the dataset locally, at scale?

Mandatory requirements

- Globally accessible, no fees / no registration / no tracking
- Bulk/batch download in common, unchangeable formats for local analysis

PASS indicators

- CSV/JSON exports (or equivalent)

- Bulk export available by year / agency / category

FAIL indicators

- Only one-by-one viewing
- No bulk export (or throttled / blocked without justification)

6) Timeliness + Archive Depth + Reporting Frequency

Test: Is the system current, and historically complete?

Mandatory timing rules

- New A&A should be searchable within 30 days of initiation
- 25-year searchable archive should exist
- Comprehensive updates at least quarterly

PASS indicators

- New records appear within 30 days consistently
- Archive depth demonstrable (old years accessible)
- Quarterly update cadence observable

FAIL indicators

- Delays cluster during controversy
- Archive gaps / broken historical access
- “Updates” exist but aren’t comprehensive

7) Owner-Relatable Spending Metrics (5-Value Model)

Test: Are totals normalized so stakeholders can interpret impact instantly?

For any major total (debt, assets, spending, transfers), reporting should include:

1. Total amount
2. Per inhabitant (per capita)
3. Per citizen / Owner
4. Per taxpayer (active taxpayers, 18–65 as defined)
5. Per citizen-taxpayer

PASS indicators

- Most categories show these five values automatically
- Denominators are defined and published consistently

FAIL indicators

- Only totals shown; no per-person breakdown
- Denominators undefined or inconsistently changed

8) Operational Example Check (Debt Transparency)

Test: Can the organization produce correct 5-Value output for debt?

Example reference calculation:

If debt = \$50B, population = 5M, citizens = 4M, taxpayers = 3M, citizen-taxpayers = 2.5M, then:

- Total Debt = \$50,000,000,000
- Debt / Person = \$10,000
- Debt / Citizen = \$12,500
- Debt / Taxpayer = \$16,667
- Debt / Citizen-Taxpayer = \$20,000

PASS indicator

- Organization publishes this style of output consistently (not just once)

17. Public Economic & Social Data [AUDIT EFFECT]

Extension ID: D32-R17-EXT

If Owners can automatically access this data at the required granularity, periodicity, and organizational scope, they are meaningfully informed about real performance. This **Shadow Audit** evaluates the existence of the data, its central and easy access, its processability (usable formats and definitions), and the presence of QA/audit verification.

Enable Owners to audit social, economic, and administrative reality using neutral, structured, auditable public data—not narratives. This right prevents “information fog” by requiring standardized dashboards and bulk datasets that are comparable over time, independently QA-audited, and relatable at human scale.

If Owners can obtain the following dataset automatically, in a central, easy-to-access, bulk-downloadable, machine-processable form with independent QA/audit, they are well-informed for evidence-based Shadow Audit.

Shadow Audit checklist

A) Reporting Frequency & Quality Assurance

A1) Reporting Frequency (minimum)

- **National and State entities: Quarterly**
- **Local governance (county/community): Yearly**

A2) Publication Deadlines (recommended)

- **Monthly releases:** publish within **30 days** after month-end
- **Quarterly releases:** publish within **45 days** after quarter-end

A3) Pre-Publication Audit (required)

All dashboards and datasets should pass an **independent Quality Assurance (QA) audit** before public release.

QA audit should include:

- completeness checks (all required fields present)
- reconciliation checks (subtotals match totals)
- continuity checks (no unexplained breaks in time series)
- format checks (download works, definitions included)
- revision log checks (changes explained)

B) Data Format & Public Access Requirements

Each release should include all of the following:

B1) Dashboard View (required)

- time-series charts (rolling window, see Section C)
- clear definitions and formulas
- consistent units and timestamping

B2) Bulk Download Dataset (required)

- open formats e.g.: **CSV, JSON**
- **no registration, no paywall, no tracking** required for access
- stable URLs and stable archives

B3) Data Dictionary (required)

- definitions, inclusion rules, known exclusions
- units, rounding rules
- source systems (what internal systems produced the numbers)
- clear field glossary

B4) Version & Archive Integrity (required)

- older releases should remain publicly accessible (no silent deletion)
- revisions require:
 - what changed
 - why it changed
 - when it changed
- prior versions should remain retrievable (no silent overwrite)

C) Time Series & Historical Depth Requirements

C1) Rolling Visibility (required)

- **Monthly series:** charts should display at least the previous **24 months**
- **Quarterly series:** charts should display at least the previous **8 quarters**

C2) Long-Term Downloadable Archives (required)

- at least **10 years** of downloadable historical data should remain accessible (or full history since inception)

D) Owner Relatability Standard (Mandatory Normalization Layer)

Raw totals are often not relatable. Therefore:

D1) Mandatory Denominators (required for large totals)

For every large total (debt, assets, spending, giveaways, taxes, major projects), the Organization should publish:

1. **Total amount**
2. **Per inhabitant (per capita)**
3. **Per citizen/Owner**
4. **Per taxpayer**
5. **Per citizen-taxpayer**

D2) Denominator Definitions (should be published)

The dataset should define and publish the counts used:

- **Population:** total residents
- **Owners/Citizens:** citizens legally included in the Owner set
- **Taxpayers:** residents who paid ≥ 1 unit of tax in the last reporting year
- **Citizen-taxpayers:** Owners \cap taxpayers

E) Reconciliation Rules (Anti-Manipulation Checks)

E1) Population Reconciliation

All population subgroups should sum to total population:

- by age group
- by citizenship status
- by employment status

E2) Spending Reconciliation

All spending categories should sum to total spending:

- domestic + international = total
- operational + investment + debt service + transfers = total (if applicable)

E3) Detention Reconciliation

All detention categories should sum to total detained population:

- by reason
- by duration bracket

F) Required Datasets (Minimum Categories)

F1) Demographic & Population Metrics (Stakeholder Base)

The Organization shall provide **detailed monthly statistics** and **historical charts spanning the previous 24 months** regarding the stakeholder base.

Categorization: All data should be categorized by:

- **Age group**
- **Citizenship status**
- **Employment status**

Income and Assistance Standards (Monthly)

Publish:

- **Average monthly compensation** for active employees
- **Average pension disbursements**
- **Average unemployment assistance payments**
- **Total number of beneficiaries** for:
 - social assistance programs
 - nutritional support programs

Social and Protective Indicators (Monthly)

Publish:

- **Number of children** in foster care and state-directed residency
- **Number of individuals with documented disabilities**, categorized by age group
- **Current census of homeless populations**

Standardized Vital Statistics (Monthly)

Publish **totals and by age group**:

- births
- deaths
- homicides
- suicides

F2) Migration and Detention (Monthly)

Emigration and Immigration Volumes (Monthly)

Publish emigration and immigration volumes categorized by:

- **Sex**
- **Age group**
- **Citizenship status**

Detention / Imprisonment Census (Monthly)

Publish current census of individuals in **state-directed detention or imprisonment**, categorized by:

- **Reason**
- **Duration of stay (brackets)**

Privacy rule: publish aggregate counts only (no personal identifiers).

F3) Economic Health and Asset Management (Monthly; rolling 24 months)

Comprehensive reporting on fiscal stability should be updated monthly and displayed as a rolling 24-month series.

Asset Categorization (Monthly)

Report:

- property (land/buildings)
- liquidity (cash/bank accounts)
- securities
- outstanding receivables

Standardized Fiscal Ratios (Required)

- **Debt-to-Revenue Ratio**
= Total Debt of the org / Yearly Income of the org
- **Debt per Owner**
= Total Debt of the org / Number of Owners of the org
- **Interest Coverage Ratio**
= Yearly Interest Payments of the org / Yearly Income of the org
- **Net Organizational Equity per Owner**
= (Total Assets – Total Debt) / Number of Owners of the org

F4) External Transfers (Monthly)

Giveaways (Required)

Public assets or demands forgiven/transferred without market compensation.

Publish:

- total giveaways
- giveaways per capita
- giveaways per citizen/Owner
- giveaways per taxpayer
- giveaways per citizen-taxpayer

Donations and Contributions (Required)

All incoming funds/assets received, categorized by source and type.

Publish:

- totals by category
- totals per the mandatory denominators (Section D)

Expenditures (Required)

All organizational spending categorized by:

- destination: domestic vs international
- recipient type: public / private / NGO / individual / other

Publish:

- totals by category
- totals per the mandatory denominators (Section D)

F5) Organizational & Administrative Performance

Personnel Census (Monthly; quarterly local acceptable)

- internal employee count
- external contractor count

Vendor Transparency (Monthly; quarterly local acceptable)

Disclose the five largest suppliers/vendors by total contract value.

Legal and Media Metrics (Monthly; quarterly local acceptable)

Publish:

- number of active judicial proceedings
- number of media-related trials
- number of mandatory public rectifications/corrections

F6) Fiscal Transparency (National and State Level)

A comprehensive rolling history of **60 months** is required for all tax and tariff data.

Tax and Tariff Catalog (Required)

The Organization should publish a complete catalog of every tax, tariff, fee, and mandatory levy, including:

For each tax/tariff:

- Name / Identifier
- Type: income / payroll / VAT/sales / excise / property / corporate / import/export / service fee / other
- Who pays: individual / employer / business / importer / owner / consumer
- Tax base: what is taxed (income category, goods category, property value, transaction type, etc.)
- Rate structure: flat / progressive / tiered (with thresholds)
- Exemptions & special cases
- Collection method: withholding / self-reporting / point-of-sale / customs / periodic filing
- Legal reference / authority (title + effective date)
- Earmarking status: general budget vs purpose-based (dedicated)

Tax Collection Efficiency (Required)

Publish both ratios (to prevent definition gaming):

- **Cost-of-Collection Ratio (%)**
= 100 * Total Cost of Collection / Total Value Collected

(Rule: whichever ratio is featured should remain consistent across time.)

Dedicated Tax Audit (Required)

For purpose-specific taxes (e.g., infrastructure or unemployment insurance):

- compare collected revenue vs purpose-specific spending
- disclose **over-collection** (surplus used outside the original mandate)

Effective Tax Rate Analysis (Required)

Effective Tax Rate = Total Tax Due / Total Income

Publish highest, lowest, and average effective tax rates for:

- Top 1%
- Top 2%–5%
- Top 6%–50%
- Bottom 50% (51%–100%)

Consumption Impact Analysis (Required)

Break down embedded taxes in essential consumer goods (fuel, food, electricity, gas, water), including:

- VAT / sales taxes
- tariffs
- environmental levies
- indirect revenue taxes

18. Transparent Tax Impact Metric [AUDIT EFFECT]

Extension ID: D32-R18-EXT

This metric (**The Service Self-Purchase Ratio - SSR**) simplifies complex tax codes to demonstrate the real work-hour impact of taxation on an Owner's income. **The Service Self-Purchase Ratio** determines how many hours an Owner should work as an employee to afford one hour of their own professional services.

SSR is a single metric that helps Owners and businesses compare the real economic friction of operating in different countries, states, or cities. It supports location decisions (residency, hiring, investment, business formation) and improves international comparability beyond headline tax rates. SSR can also correct reputational distortions: a jurisdiction may appear "high tax" but still have a low SSR due to efficiency and purchasing power. By making tax friction measurable and comparable, SSR creates an incentive for jurisdictions to reduce extraction and improve competitiveness.

The calculation accounts for the following layers:

- Consumption Taxes: Value Added Tax (VAT) or sales tax applied to services.
- Corporate/Revenue Taxes: Any mandatory fees or taxes the business should pay regardless of profit.
- Employer-Side Mandatory Costs: Health, unemployment, and pension insurance paid by the employer.
- Employee-Side Mandatory Costs: Insurances and social security deducted directly from the payroll.
- Personal Income Tax: All income-based taxes applied to the remaining salary.

Taxes and taxation logic may vary locally, therefore the calculation has to be adjusted (e.g. Personal Income Tax before or after deduction of insurance costs).

Technical Example:

Total Consumer Cost: \$55.00 (Service Rate of \$50.00 + 10% VAT).

- **Revenue-Based Corporate Tax: \$0.50** (1% of service rate).
- **Total Salary Pool: \$49.50** (representing 115% of the gross salary).
- **Employer-Side Mandatory Costs: \$6.457** (15% insurance/social costs).
- **Gross Salary on Payroll: \$43.043** ($\$49.50 / 1.15$).
- **Employee-Side Mandatory Costs: \$6.457** (15% insurance/social costs).
- **Personal Income Tax: \$8.608** (20% of the gross salary if insurance is not deductible).
- **Final Net Income: \$27.98** ($\$43.043 - \$6.457 - \8.608).

The Service Self-Purchase Ratio - SSR: $\$55.00 / \$27.98 = 1.97$

This indicates the Owner should work **1.97 hours** to purchase **1 hour** of their own service within this fiscal environment.

Category 7: Environmental Integrity

22. Prevent Deforestation and Protect Nature [AUDIT EFFECT]

Extension ID: D32-R22-EXT

If Owners can automatically access the required environmental integrity dataset at the specified **granularity, update frequency, and organizational scope**, they are meaningfully informed about real-world environmental performance and risk exposure.

This **Shadow Audit** evaluates four things:

1. **Dataset existence** (the required indicators actually exist and are complete),
2. **Central and easy access** (a single official point of access, stable and public),
3. **Processability** (bulk-downloadable, machine-readable formats, clear definitions), and
4. **Verification** (QA controls and independent audit validation where applicable).

If Owners can obtain the full **D32-R22-EXT dataset automatically**, through a central, easy-to-access, bulk-downloadable, machine-processable system with stable definitions and independent QA/audit verification, then Owners' need for evidence-based environmental oversight is fulfilled.

Shadow Audit Benchmarks

Schedule

- **Quarterly** reporting (or **Yearly** for small local entities)
- **Yearly** independent audit of the dataset

Data format

For each category/subcategory below, publish:

- **Area** (sq km or sq ft) by category, subcategory (the whole hierarchy)
- **And the metrics below**

Reconciliation rule: All categories must sum to **100% of Total Territory**.

Categories

- **1. Unutilized Surface (top level)**
 - **1.1. Proxy for heat-island mitigation (level -1)**
 - **1.1.1. Proxy for cooling + heat absorption buffer (level -2)**
 - Lakes / Reservoirs (level -3)
 - Rivers / Streams (level -3)
 - Glacier / Permanent snow cover (level -3)
 - **1.1.2. Proxy for CO₂ absorption + O₂ generation (level -3)**
 - Forest/Woodland/Bush (level -4)
 - Swamp / Wetland (level -4)
 - **1.2 Desert / Arid land (level -1)**
 - **1.3 Others (level -1)**
 - Prairie / Grassland (level -2)
 - Mountains / Alpine land (level -2)
 - Parks / Protected nature areas (level -2) e.g. urban parks / golf courses
 - Other natural surface (level -2)
- **2. Utilized Surface – "Human footprint" (top level)**
 - **2.1 Uncovered / Unsealed Utilized Surface (restorable) (level -1)**

Utilized land that is not sealed and is typically ready for rewilding / reforestation with low structural removal work.

- Soil / exposed ground (e.g. cropland, agriculture) (level -2)
- Empty uncovered plots (level -2)
- Post-industrial open land (e.g., reclaimed pits / recreational mine areas) (level -2)
- Other restorable utilized surface (level -2)
- **2.2. Covered / Sealed Utilized Surface** (not restorable short-term) (level -1)
 - Utilized land that is sealed or structurally built, typically not ready for rewilding without major removal / demolition.
 - Roads (level -2)
 - Rail infrastructure (level -2)
 - Buildings (level -2)
 - Asphalted / paved areas (non-road) (level -2)
 - Industrial sites (level -2)
 - Waste depot / landfill (level -2)
 - Other sealed surface, e.g. infrastructure (level -2)
 - **2.2.1 High-Hazard / High-Containment Surface** (level -2)
 - This category reduces the suitability score because it represents land that is typically incompatible with residential use and long-term low-risk development.
 - Nuclear plant sites (level -3)
 - Nuclear waste storage / repositories (level -3)
 - Chemical plants / processing, Oil refineries and similar (level -3)
 - Chemical depots / hazardous storage yards (level -3)
 - Dangerous mine waste / tailings (level -3)
 - Military hazardous zones (munitions, secured facilities, etc.) (level -3)

Metrics to deliver

Explanation: {1.} = Category "1. Unutilized Surface"

{2.1.} = SubCategory "2.1 Uncovered / Unsealed Utilized Surface"

R1= "Unutilized Surface" / "Total Territory" = {1.} / ({1.} + {2.})

R2= "Proxy for CO₂ absorption + O₂ generation" / "Total Territory" = {1.1.2.} / ({1.} + {2.})

R3= "Proxy for heat-island mitigation" / "Total Territory" = {1.1.} / ({1.} + {2.})

R4= "High-Hazard / High-Containment Surface" / "Total Territory" = {2.2.1.} / ({1.} + {2.})

Incentive metric R5 (between -10 and 100 by construction)

$$\frac{({1.1.2.} * 100 + ({1.1.} - {1.1.2.}) * 75 + {1.2.} * 6 + {1.3.} * 30 + {2.1.} * 10 + ({2.2.} - {2.2.1.}) * 1 + {2.2.1.} * -10)}{({1.} + {2.})}$$

23. Open Access to Global Warming-related Data [AUDIT EFFECT]

Extension ID: D32-R23-EXT

To ensure the long-term viability of the territory and to provide Owners with the raw data necessary for objective risk assessment, the Organization should maintain a transparent, audited database of environmental and climatic performance metrics (within the country and locally). This data should be provided as a neutral service, strictly excluding ideological commentary, administrative filtering, or tracking.

If Owners can obtain the following environmental and climate dataset automatically, in a central, bulk-downloadable, easy-to-access, machine-processable form with independent QA/audit, they are well-informed for evidence-based risk decisions (housing, insurance, agriculture, infrastructure, health, and long-term territorial viability).

This **Shadow Audit** checklist helps an Owner evaluate whether climate and environmental data is real, complete, neutral, auditable, and tamper-resistant.

Shadow Audit Checklist — Climate Data Clarity Indicators

1) Dataset Existence + Central Access (Does it exist as a usable public service?)

Indicators of a clear dataset

- A single official portal exists where environmental + climate datasets can be found centrally (not scattered).
- Data is available free, registration-free, and without tracking.
- Data is published as a neutral service (raw measurements + definitions), not as ideology or messaging.

Indicators of an unclear dataset

- Data exists but is fragmented across agencies, difficult to find, or inconsistently maintained.
- Access requires unclear steps (accounts, approvals, vague “request processes”).

Indicators of a manipulated/unfair dataset

- Access is paywalled, requires identity verification, or includes third-party tracking/analytics.
- Datasets disappear, become restricted, or degrade during controversy or extreme events.

2) Minimum Environmental Data Matrix (Is the required coverage included?)

Daily schedule rule (meteorology-aligned, long-term comparable):

Daily values should include minimum + maximum, plus fixed-time measurements at 06:00 UTC and 18:00 UTC. These timestamps should remain consistent across years to enable long-term comparability and historical “flashback” audits.

Indicators of a clear dataset

The system publishes all required domains with the required periodicity:

A) Surface Temperature (Soil & Sealed Infrastructure)

Natural surfaces (soil)

- measured at surface and 1 foot (~30 cm) below ground
- locations include: urban, forested, agricultural

Sealed infrastructure (roads & rooftops)

- measured at surface level on unshaded areas
- roads: city center (CBD), suburban, rural/country
- rooftops: measurement exists for CBD + suburban

B) Hydrographic Temperature (Water)

- scope: primary rivers, major lakes, and where applicable coastal sea/ocean
- depths: 1 foot, 6 feet, 30 feet below surface

C) Atmospheric & Integrity Metrics

Air temperature (multi-layer):

- ground level (2m standard where available)
- ~5,000 feet above ground (AGL) (*≈ 1 mile*)
- ~30,000 feet (*commercial aviation altitude band*)

Ozone thickness: in Dobson Units (DU)

Precipitation: audited total volume per measurement point

Humidity / water stress indicators:

- atmospheric relative humidity at ground
- soil moisture at 1 foot and 6 feet below ground

[] Indicators of an unclear dataset

- Some domains exist but not daily, not synchronized, or lack min/max.
- “Climate reporting” exists mainly as summaries, slides, or commentary without datasets.

[] Indicators of a manipulated/unfair dataset

- High-impact domains (urban heat, rooftop/road temps, water temps) are systematically missing.
- Data becomes incomplete exactly when risk spikes (heatwaves, droughts, floods).

3) Geographic Consistency (Can Owners compare over time without “moving the sensors”?)

[] Indicators of a clear dataset

- Measurement zones use fixed coordinates (publicly disclosed).
- Measurements occur at the same coordinates over time, enabling comparability.

[] Indicators of an unclear dataset

- Locations are vague (“metro area”), coordinates are missing, or stations are frequently redefined.

[] Indicators of a manipulated/unfair dataset

- Stations move over time without explanation (suspected data gaming or re-benchmarking).

4) Publishing SLA (Is it current enough to be operationally useful?)

[] Indicators of a clear dataset

- Target: new daily data is published within 24 hours of capture (consistent SLA performance).
- Any delays are logged with a simple public outage log (date, scope, reason, restoration time).

[] Indicators of an unclear dataset

- Publication delays are frequent, unexplained, or inconsistent by region/zone.

[] Indicators of a manipulated/unfair dataset

- “Selective delay”: publication slows down when political or financial stakes rise.

5) Data Portability + Processability (Can Owners actually analyze it?)

[] Indicators of a clear dataset

- Owners can bulk-download the entire dataset (not just view charts).
- Data is provided in machine-readable formats suitable for independent analysis.
- Stable station identifiers allow time-series merging across years.

[] Indicators of an unclear dataset

- Data is only offered as view-only dashboards or heavily aggregated charts.

[] Indicators of a manipulated/unfair dataset

- Data access is throttled, blocked, or intentionally made hard to process at scale.

6) Historical Baseline Depth (Does it allow long-term trend judgment?)

[] Indicators of a clear dataset

- At least 50 years of historical data is available where feasible.
- A 100-year archive exists as the preferred benchmark where historically possible.

[] Indicators of an unclear dataset

- Historical depth exists but is discontinuous, incomplete, or undocumented.

[] Indicators of a manipulated/unfair dataset

- Older data disappears, is overwritten, or becomes inaccessible without explanation.

7) Anti-Manipulation & Tamper-Evidence (Can retroactive edits be detected?)

[] Indicators of a clear integrity protocol

- An independent QA function exists to validate data integrity and detect tampering.
- Data older than 30 days should be preserved in a tamper-evident, non-rewritable archive, so retroactive edits are detectable.

Acceptable implementations include:

- WORM storage
- Object-lock / append-only storage
- Cryptographic release hashing + public timestamping
- Blockchain-based timestamp ledger

[] Indicators of an unclear integrity protocol

- No formal integrity protocol exists; corrections are undocumented or inconsistent.

[] Indicators of a manipulated/unfair dataset

- Retroactive edits occur without traceable change logs.
- “Revisions” repeatedly reduce perceived extremes (temperature spikes, drought indicators) without explanation.

8) Neutrality Standard (Is the service informational, not propaganda?)

[] Indicators of a clear dataset

- Datasets are published as raw measurements + definitions, clearly separated from commentary.
- Labels and metadata remain technical and stable over time.

[] Indicators of an unclear dataset

- Data is mixed with messaging content or selectively framed without separation.

[] Indicators of a manipulated/unfair dataset

- Dataset publication appears designed to shape perception rather than preserve an auditable record.

Category 8: Economic Risk Governance

25. Mandatory Insurance for High-Risk Industry [AUDIT EFFECT]

Extension ID: D32-R25-EXT

If Owners can **publicly verify** that high-impact activities are covered by enforceable private liability insurance—at the required coverage level, lifecycle scope, and transparency standard—then Owners can reasonably conclude that catastrophic-risk exposure is **financially pre-funded** and that restitution is not primarily dependent on emergency taxpayer funding.

This follows standard economic risk-transfer logic: if an entity poses systemic or irreversible harm, it must internalize that risk not just through accountability, but through insurable instruments — because the scale of potential harm may exceed its ability to compensate after the fact.

Public verifiability is essential:

If the existence, validity, and coverage limits of the insurance cannot be confirmed through a public registry (or equivalent official dataset), then there is **no reliable guarantee** that coverage exists when needed.

This **Shadow Audit** evaluates four things:

1. **Coverage exists** (policies are active for all applicable operations)
2. **Coverage is adequate** (limits reflect documented risk analysis)
3. **Coverage is continuous** (design + production + operation, including long-tail/legacy liability)
4. **Coverage is transparent and verifiable** (central registry + traceability + QA controls)
 - **Definitions (Plain Language)**

High-Impact Activities (what should be insured)

High-impact activities are operations capable of large-scale systemic harm, including but not limited to:

Non-military sectors

- Nuclear, hydroelectric, fossil fuel power generation
- Chemical facilities and hazardous materials handling
- Biological research / bio-risk facilities
- Mining and heavy industry
- Mass transportation systems (rail, metro, ferries, aviation, shipping)
- Large infrastructure (bridges, tunnels, dams)
- Pharmaceutical manufacturing
- Space industries / launches
- Critical food & beverage supply chains (systemic contamination risk)
- Energy storage / battery manufacturing and large storage sites

Military high-impact production & storage

- Production/storage of munitions
- Nuclear weapon-related production/storage
- Chemical or biological agent production/storage
- Military-grade space infrastructure

PML / MPL / EML (insurance contract risk terms)

Insurance coverage adequacy should be supported by a documented risk analysis using standard insurance terminology:

- **PML — Probable Maximum Loss:** the largest loss reasonably expected under severe but plausible conditions (assuming key protections work as intended).
- **MPL — Maximum Possible Loss:** the worst-case loss if protections fail and adverse conditions cascade.

- **EML — Estimated Maximum Loss:** a quantified maximum-loss estimate (often used in engineering risk reports).

For Shadow Audit purposes, coverage limits should be justifiable against the operation’s documented **PML and/or MPL** (EML acceptable where used by the market).

Insurance Registry (what should be publicly visible)

A central public database (or equivalent official dataset) listing the insurance status of all high-impact activities, including:

- policy status (active/expired)
- coverage limits (ceiling amounts)
- insurer identity
- operator/policyholder identity
- a reference to the underlying PML/MPL/EML risk analysis basis

Shadow Audit Checklist — Insurance Coverage Clarity Indicators

How to use: For each checkpoint, mark **PASS / FAIL / PARTIAL**, and capture evidence (registry location, sample entries, dates, missing categories).

1) Public Verifiability (Registry Exists + Central Access)

Test: Is there a public, central, searchable source confirming insurance existence?

PASS indicators

- A single official portal/dataset exists for insurance status of high-impact activities
- Access is free and does not require registration

FAIL indicators

- Insurance is claimed but not publicly verifiable
- Data is fragmented, manual, or “available on request only”

2) Scope Coverage (All High-Impact Activities Included)

Test: Does coverage apply to the full high-impact footprint?

PASS indicators

- Registry includes all major high-impact sectors
- Coverage applies nationally and locally where relevant
- No unexplained category exclusions

FAIL indicators

- Whole categories missing (e.g., chemicals, transport, dams, storage sites)
- “Selective” coverage that omits comparable-risk sectors

3) Policy Status + Coverage Limits (Visible and Current)

Test: Can Owners verify each operation’s coverage status and limits?

PASS indicators

- Each operation shows active/expired status
- Coverage ceiling amounts are visible
- Update cadence is consistent and recent

FAIL indicators

- Coverage limits hidden behind vague language
- No clear validity status (active vs expired unclear)
- Long gaps or irregular updates

4) Responsibility Traceability (Insurer + Operator / Policyholder)

Test: Is accountability traceable to real entities?

PASS indicators

- Insurer identity is visible and verifiable

- Operator/policyholder identity is visible and consistent
- Subcontractors are not used as anonymity shields

FAIL indicators

- Shell entities obscure who actually holds the risk
- Insurer identity missing, non-verifiable, or unstable

5) Adequacy Basis (PML/MPL/EML Referenced)

Test: Is coverage linked to a documented maximum-loss analysis?

PASS indicators

- PML and/or MPL (or EML where standard locally) is referenced per operation
- Risk analysis scope includes people, property, and business/system continuity
- Coverage limit is plausibly aligned with that risk basis

FAIL indicators

- Coverage exists without a visible risk basis
- “Compliance language” exists but no quantified PML/MPL/EML anchor

6) Minimum Life-Loss Coverage Baseline

Test: Is human life explicitly insured above a minimum floor?

Recommended baseline

- Each loss of life should be insured for at least:
10 years of the national average median salary, payable to beneficiaries.

PASS indicators

- Life-loss payout terms exist and meet/exceed baseline
- Beneficiary payment mechanism is defined

FAIL indicators

- Life-loss coverage missing or undefined
- Coverage relies on discretionary public compensation instead of insured payout

7) Lifecycle Coverage (Design + Production + Operation)

Test: Does liability coverage follow the full lifecycle, not only the operating phase?

Coverage should include all three phases:

- **Design** (architectural/engineering liability)
- **Production** (manufacturing/construction liability)
- **Operation** (ownership/usage liability)

Interpretation rule (future harm coverage):

Design and production insurance should cover **future harms caused by latent defects**, even if failure occurs years later (e.g., structural collapse, material fatigue, hidden engineering faults).

PASS indicators

- Policies explicitly cover Design, Production, and Operation
- Design/production liability includes delayed-failure scenarios
- Coverage is not limited to a short “warranty-like” window when the asset’s risk persists

FAIL indicators

- Coverage starts only at operation stage
- Design/production defects are excluded
- Policies treat long-term defect risk as “not insurable” or “expired by default”

8) Long-Tail / Legacy Liability (Contractor Disappearance Protection)

Test: Does liability remain enforceable even if original design/production entities no longer exist?

Problem this control prevents:

If a bridge, tunnel, dam, or similar asset fails years later, the original designer/constructor may have dissolved, been acquired, or reorganized—creating a practical “liability vacuum.” This control ensures responsibility remains financially real.

Legacy protection should exist (ideal goal):

Design and production liability coverage should remain valid across the asset's expected lifespan, and should not depend on the continued existence of the original contractor. This can be achieved via either:

- **Pre-paid long-tail insurance** for design/production risks across the asset lifespan, **or**
- **Transfer of legacy liability** into the current operator's primary liability insurance (explicitly including historical design/production defect risk).

PASS indicators

- Long-tail liability remains valid even if the contractor dissolves
- The operator's policy explicitly includes legacy design/production defect exposure
- There is no "build-and-vanish" liability escape path

FAIL indicators

- Liability collapses when a contractor dissolves
- Operator policy excludes historical design/production defects
- Long-term failure becomes "taxpayer-funded by default" due to insurance gaps

9) Coverage Quality (Exclusions and Trigger Reality Check)

Test: Is coverage meaningful when catastrophe occurs?

PASS indicators

- Key catastrophic triggers are covered (not excluded by default)
- Exclusions do not gut the policy (e.g., broad "force majeure" misuse)
- Claims process and payout obligations are unambiguous

FAIL indicators

- Exclusions are broad enough to deny expected worst-case scenarios
- Coverage exists "on paper" but becomes non-payable in practice

10) Implementation Timing (Transition Rules)

Test: Is there a clear and measurable compliance rollout?

Recommended timing logic

- **New projects** should meet standards at initiation
- **Existing operations** should reach full compliance within a defined transition window
- Transition allowances may exist to avoid destabilizing critical infrastructure, but must be time-bounded

PASS indicators

- Transition timelines are public and measurable
- New projects show compliance from day one
- Existing operations show a tracked progress plan

FAIL indicators

- "Transition" used as indefinite delay
- New projects begin without verifiable coverage
- Deadlines are missing or routinely waived

11) Anti-Manipulation Safeguard (Credible International Insurance Allowed)

Test: Can coverage be sourced internationally if local markets obstruct access—without allowing pseudo-insurers that cannot pay claims?

Credible International Insurer Qualification (any one of the following)

An international insurer should qualify if **at least one** of these credibility proofs is met:

A) Regulated + Solvency Proof

- Licensed and supervised by a recognized insurance regulator in a major jurisdiction, and
- Publishes audited financial statements, and
- Meets applicable solvency/capital adequacy standards in its home jurisdiction.

B) Claims-Paying Strength Rating

- Holds an investment-grade insurer financial strength rating (or equivalent) from a recognized rating agency.

C) Capacity Guarantee / Reinsurance Backing

- Demonstrates credible claims-paying capacity through reinsurance backing, guarantee structures, or documented capital reserves sufficient for catastrophic loss events.

FAIL (Pseudo-insurer risk indicators)

Coverage should be treated as non-credible if:

- the insurer is unregulated or lightly regulated without solvency proof, or
- audited financial statements are absent or non-transparent, or
- the insurer cannot demonstrate credible claims-paying capacity for catastrophic loss events.

12) QA Verification (Independent Confirmation)

Test: Is there independent confirmation of registry completeness and integrity?

PASS indicators

- Registry completeness is periodically verified
- High-impact categories are tested for omissions and false reporting
- Verification artifacts are publicly accessible

FAIL indicators

- “Verified” claims exist without proof
- High-risk categories are excluded from checks

26. Monopoly Power Transparency Safeguard [AUDIT EFFECT]

Extension ID: D32-R26-EXT

What qualifies as a monopoly or monopoly-like condition?

A service provider, governance actor, or infrastructure owner is considered a **monopoly** or functionally **monopoly-like** within the scope of TCORF if **one or more of the following apply**:

- 1. Market dominance and fragility:**
 - A provider with **≥50% market share** in a given region or function is presumed monopoly-like.
 - Even a **≥20% share** may qualify if the sector is structurally fragile, tightly regulated, or known for coordination failures (e.g., banking, healthcare insurance).
- 2. There are no feasible alternatives** for users, either:
 - **Technically**, because no competitor exists within a reasonable geographic radius or capacity.
 - **Economically**, because switching would require unreasonable cost or effort from the user (e.g., installing an off-grid water system or private wastewater treatment).
 - **Legally or contractually**, due to statutory monopolies, concessions, or mandatory enrollment.
- 3. The service is non-substitutable:** Avoiding it or “opting out” would:
 - Result in **serious degradation of health, safety, housing, mobility, or economic function**, or
 - Require a **long-term life disruption**, such as selling property to escape a governance actor (e.g., HOA).
- 4. The service or actor is critical infrastructure**, defined as:
 - If it fails or becomes unavailable, **no adequate substitute exists that can fully absorb demand or replace function within 180 days**.

Sector-based classification: typical monopolies and roles

To assist evaluation, TCORF recognizes that monopoly-like conditions vary by **sector** and **role**. Below is a non-exhaustive classification:

Electricity / Energy

- **Generation:** Power plants, large-scale renewable operators.
- **Infrastructure:** Transmission grid owners.
- **Retail / Billing:** End-user-facing providers (especially single-provider zones).

Oil & Gas (Fuel, Heating, and Petrochemical Systems)

- **Upstream control:** Holders of oil/gas extraction licenses, national oil companies, state-granted concessions, or entities controlling offshore/onshore production rights.
- **Midstream infrastructure:** Refining, pipeline transport, LNG terminals, storage facilities.
- **Downstream distribution:** Fuel wholesalers, heating gas utilities, gas station networks, end-user billing providers.
- **Import/market access control:** Gatekeepers of national or regional energy imports, including foreign supply contracts and exclusive trading rights.

Water & Wastewater

- **Supply:** Water utilities, wells with area exclusivity.
- **Treatment:** Wastewater management entities.
- **Infrastructure:** Pipe networks, metering, emergency backups.

Healthcare

- **Facilities:** Hospitals, emergency care centers (especially sole providers within 50 km).
- **Coverage:** Health insurers or state payers.
- **Pharmaceuticals:** dominant suppliers.
- **Medical transport:** Ambulance or emergency helicopter services.

Transport & Mobility

- **Public Transport:** Buses, subways, trains (regional monopolies).

- **Infrastructure:** Toll highways, ferry crossings, bridges.

Finance & Payments

- **Banks:** Retail banks with large public share or exclusive deposit access.
- **Payments:** Mobile money, credit/debit networks, wallets, with >20% regional share.

Communications

- **Telephony:** Local exchange carriers, landline monopolies.
- **Mobile Network:** Dominant MNOs.
- **Internet Access:** Only available or affordable ISP in an area.

Postal & Delivery

- **National Postal Services**
- **Package Delivery:** Dominant cross-border couriers.

Governance actors with mandatory scope

- **HOAs / Condo Boards:** User must sell property to exit.

Food Systems (Agricultural Land, Production, Processing, Retail)

Structural Roles and Thresholds

- **Farmland Concentration (Regional)**
 - A single entity controlling **≥20% of total national farmland (in the state or in the country)**
- **Primary Production and Processing**
 - Entities controlling **≥40% of output** in key sectors
- **Food Chains and Retail**
 - Food retailers or distributors with **≥40% market share** in a national market.
- **Critical Input Monopolies**
 - Single-source providers of **seeds, fertilizer, pesticides** may be flagged if:
 - **≥50% market share**

Clarification

TCORF does not classify family farms, independent grocers, or regional cooperatives as monopoly risks, regardless of size, unless they engage in systemic exclusion, opaque pricing, or dominant control over access.

This section applies **only** to cases of **concentration + control + limited alternatives**.

Indicators of Abusive, Wasteful, or Inefficient Monopoly Behavior

TCORF recognizes that monopoly or monopoly-like conditions often lead to serious harm — not only through **corruption or favoritism**, but also through **inefficiency, waste, negligence, or poor management**.

Abuse doesn't always require bad intent. A monopoly can cause public harm simply by being **inefficient, disorganized, opaque, or structurally incapable of delivering fair and effective service**.

The following are considered **strong indicators** of unacceptable conduct in monopoly-controlled environments — whether caused by **malice, self-interest, or institutional dysfunction**.

1. Deliberate High-Cost Procurement

Purchasing core resources (e.g., electricity, gas, oil) at **consistently inflated prices** from preferred or affiliated suppliers **without competitive tenders**, when market rates are significantly lower.

- **Audit Trigger:** Price paid vs. regional wholesale average over trailing 3–6 months.
- **Disclosure Requirement:** Justify cost basis, supplier selection, and procurement terms.

2. "Friends Discount + Public Overcharge" Model

Charging **inflated list prices** to the general public while offering **non-transparent discounts** or soft rebates to insiders, politically connected entities, or friendly business partners.

- **Audit Trigger:** Discrepancy between group pricing vs. actual usage concentration.

- **Disclosure Requirement:** Publish anonymized volume-weighted pricing per group.

3. Excessively Harsh Service Terms

Imposing **no guaranteed service levels, disconnection without due process, or monetary penalties** unrelated to actual service delivery (e.g., predatory billing practices).

- **Audit Trigger:** Absence of minimum performance guarantees or user protection mechanisms.

4. Excessive or Hidden Profit Extraction

Generating **profit margins far beyond sector norms**, or channeling surplus via:

- **Unnecessary contracts**
- **Overpriced services**
- **Affiliated consulting**
- **Unjustified "management fees"**
- **Audit Trigger:** Profit-to-cost ratio, number and value of non-transparent "internal" contracts.

5. Multi-Layer Subcontractor Obfuscation

Using **3+ layers of subcontractors**, each taking a margin, with no visibility into who delivers actual services.

Creates:

- Lack of accountability
- Dilution of responsibility
- Masking of real beneficiaries
- **Audit Trigger:** More than two layers of subcontracting for core services.

6. Withholding Volume-Weighted Contractor Data

Refusing to publish the **distribution of contract volume or value** among contractors and subcontractors, making it impossible to detect insider favoritism or artificial markup chains.

- **Required Transparency Metric: "Weighted Subcontractor Distribution Disclosure"**

Each monopoly-like actor must publish a summary disclosure of:

- **Total number of contractors/subcontractors**
- **Number of layers** (e.g., contractor → subcontractor → sub-subcontractor)
- **Volume-weighted share of contracts for each level**

"Monopoly Pricing Fairness and Transparency"

1. Full pricing structure disclosure:

Any actor subject to monopoly-like conditions must publish:

- All active pricing groups or customer classes (e.g., residential, business, institutional, internal, VIP)
- Associated base rates, volume tiers, surcharges, and discounts
- Eligibility criteria for each group or class (e.g., income, geography, usage pattern)

2. Disclosure of discount types:

All pricing exceptions—e.g., "volume discount," "legacy customer," "partnership pricing," or "pilot program"—must be clearly listed and described.

3. Disclosure of number of recipients (per group):

For each group or pricing class, publish:

- Number of current active customers
- Total usage or volume billed to that group (monthly or quarterly average)

4. Disclosure of "non-public pricing arrangements":

If any customer or group receives pricing that deviates from the published rates:

- This must be disclosed as a special arrangement;

- A non-personalized identifier (e.g. Group A, “local partner,” etc.) must be included;
- The basis for the discount (policy, volume, regulatory order, etc.) must be stated.

5. Right of audit request (only if safety permits):

Any stakeholder may submit a **Shadow Audit request** to determine whether they or others were improperly classified or denied access to fair pricing. TCORF recommends **aggregated pricing audits** over individual ones for safety and privacy reasons.

27. Tariff Stability Safeguard [AUDIT EFFECT]

Extension ID: D32-R27-EXT

Calibrated Tariff Surcharges (part of “Diplomatic API”) for Stable, Evidence-Based Trade Friction Shadow Audit Notice (How to Read This Document)

This document is a **Shadow Audit checklist**. It is written as a **QA-style verification tool** to assess whether tariff surcharges are applied in a **rule-based, stable, auditable** way that preserves trade viability and avoids arbitrary political churn.

Preamble (Calibrated Tariff “Diplomatic API” Rationale)

Rather than pursuing trade termination, total bans, or purely political sanctions—which often create excessive domestic friction and unfairly punish companies for issues beyond their control—this protocol uses **calibrated tariff surcharges** as a controlled, measurable tool.

Built on **historical humility**, it recognizes that different systems are easy to judge, yet most nations have experienced “dark” periods in their history. Instead of moral absolutes, this Right expresses ethical and security frictions as **standardized tariff tiers with defined ranges**, providing a fast, market-based method that keeps trade alive while incentivizing higher global standards.

For Shadow Audit purposes, the key test is whether tariff actions are **tier-based, capped, evidence-referenced, stable, and transparently governed**, rather than arbitrary or purely reactive.

Purpose (Pass Condition)

Owners are meaningfully informed and protected if tariff measures are:

1. traceable to standardized triggers,
2. capped and scoped to prevent escalation abuse,
3. stable for a minimum period once imposed, and
4. not altered abruptly without notice and published impact analysis.

PASS condition:

If tariff decisions and modifications are predictable, documented, and constrained by defined floors and notice requirements, this Right functions as a low-friction remedy instead of a political shock tool.

Scope

This checklist applies to:

- import tariff surcharges applied to specific jurisdictions and/or sectors
- tariff modifications (increases, reductions, removals)
- emergency or politically sensitive tariff actions

Definitions

Calibrated Tariff Surcharge

A tariff surcharge is a **measured price friction**, not a full trade termination mechanism. It should be designed to keep trade functioning while signaling quantified risk or ethical friction.

Tier System (Standardized Trigger Logic)

Tariffs are categorized into tiers to prevent arbitrary or inconsistent escalation. Each tier has defined ranges and should be evidence-referenced.

Multilateral Exception Rule (Integrated Economic Regions)

If the counterparty is a member of the same integrated economic region (e.g., **EU, USMCA/NAFTA**), tariff escalation should be treated as a last step. The Organization should first prioritize the region’s existing dispute resolution mechanisms to minimize friction and prevent duplicate enforcement systems.

Shadow Audit Checklist — Tariff Stability & Integrity (R27)

1) Central Tariff Registry Exists (Public, Searchable, Historical)

Test: Can Owners access a complete list of active and historical tariff surcharges?

PASS indicators

- A single official registry exists (central, searchable)
- Each tariff lists: counterparty jurisdiction, scope (sector or general), tier, effective date, end/review date
- Historic records are preserved (no deletion of prior tariff states)

FAIL indicators

- Information exists only in speeches or press releases
- Missing effective dates, missing scope, missing archives

2) Clear Objective (Trade Continuity + Calibrated Friction)

Test: Is the tariff framed as calibrated friction, not a disguised ban?

PASS indicators

- Written purpose states: “maintain trade while applying measurable friction”
- Scope is defined and targeted where possible
- Essential goods minimization/exemption logic is addressed where relevant

FAIL indicators

- Tariff functions as an indefinite punishment tool without scope discipline
- Blanket tariffs applied without targeting logic

3) Tier Classification is Standardized and Evidence-Referenced

Test: Are tariffs justified through standardized tiers rather than ad-hoc politics?

PASS indicators

- Each tariff references a tier classification
- Tier rationale is documented and repeatable
- Evidence basis exists (events/actions/thresholds and sources)

FAIL indicators

- No tier classification
- Inconsistent tiering across comparable cases
- Rationale is purely rhetorical

4) Caps are Respected (Anti-Escalation Guardrails)

Test: Do tariff surcharges remain within defined tier caps?

Tier caps

- Tier 1 (Human Rights & Civil Liberties): 1%–max 2%
- Tier 2 (Geopolitical / Legal / Environmental): 1%–max 10%
- Tier 3 (Security / Industrial Distortion): 1%–max 50%
- Tier 4 (Existential Aggression): 1%–max 100%

PASS indicators

- Surcharges do not exceed caps
- Any adjustments remain within the tier range and are justified

FAIL indicators

- Caps exceeded
- “Equivalent tariff” mechanisms used to bypass caps

5) Minimum Duration Floor is Honored (Stability Over Churn)

Test: Once applied, is the tariff kept stable long enough to be meaningful?

PASS indicators

- Once imposed, the tariff remains in place for ≥ 365 days
- Early reductions/removals are logged as exceptions with explicit justification

FAIL indicators

- Tariff is imposed then rapidly reduced/removed for political theater
- Short-term churn creates volatility rather than stable policy

6) Notice Period is Respected (Predictability Requirement)

Test: Are modifications announced with enough lead time to avoid market shock?

PASS indicators

- Any modification (increase or reduction) is announced ≥ 90 days in advance

- Announcement includes: parameters, effective date, and impact analysis

FAIL indicators

- Sudden changes without lead time
- “Immediate effect” modifications without documented emergency justification

7) Domestic Impact Analysis Exists (Costs Are Visible)

Test: Does the Organization publish expected domestic impacts?

PASS indicators

- Analysis includes likely consumer cost impact and business input impact
- Sector design explains how domestic harm is minimized while preserving signal strength
- Analysis is archived with the decision record

FAIL indicators

- No domestic impact analysis
- Impacts are ignored or hand-waved

8) Decision Record is Auditable (Authority + Rule Basis)

Test: Can Owners trace the tariff decision to an accountable process?

PASS indicators

- Decision authority is defined (office/role)
- Date, tier basis, scope, and rationale are recorded
- Modification decisions are logged consistently over time

FAIL indicators

- No clear accountable authorizer
- Decisions occur without traceable records

9) Owner Request / Objection Channel Exists (Non-Binding Signal)

Test: Can Owners file tariff requests or objections in a trackable way?

PASS indicators

- Owners can submit a request for tariff action or a non-binding objection to premature reduction
- Requests receive a receipt/ID and are preserved
- The Organization acknowledges requests through standard intake procedures

FAIL indicators

- No intake mechanism, or requests are ignored/dropped
- Missing receipts / no tracking / deletion without logging

Category 9: State Structure & Security

35. The Right to Surveillance Warnings [AUDIT EFFECT]

Extension ID: D32-R35-EXT

Shadow Audit Notice

This extension defines a **QA-style disclosure benchmark** for surveillance/manipulation risk in goods and services. It is not a ban, not a political demand, and not a legal claim — it is a **consumer safety warning standard** for modern digital hazards.

Definitions

Surveillance Warning (SW):

A short, visible notice provided at purchase/activation that explains surveillance/manipulation behavior and Owner control options.

Point-of-Purchase / Point-of-Activation:

Package label (physical), invoice/receipt, checkout screen, confirmation email, or first-run setup screen.

Surveillance / Manipulation (audit meaning):

Any capture, inference, transmission, or profiling of audio/video/location/biometrics/behavioral patterns, and/or product behavior that limits Owner agency (coercive UX, forced accounts, remote disablement, enforced policy restrictions).

Preamble

Modern digital products can observe, record, profile, or steer users from the first second of use — often silently.

Most Owners cannot realistically evaluate this risk from technical specs or buried terms.

This right exists to:

- raise visibility of surveillance risk,
- make products comparable at purchase time,
- and create a market incentive for more secure, Owner-controlled designs.
-

Why a Surveillance Warning belongs next to chemical/fire hazard warnings

In consumer protection, when a product presents a serious risk, the risk is disclosed **visibly at the moment of purchase/use**, not hidden in long text. This is normal for hazards such as:

- toxic or corrosive chemicals
- flammable liquids
- electrical shock/fire risks
- choking hazards
- allergens and food contamination
- high-powered lasers / radiation labels
- heavy machinery / tool injury warnings

The reason is simple: **an uninformed user cannot consent to a hazard they cannot see.**

This right treats **unknown or unauthorized surveillance/manipulation** as a modern hazard category because it can cause severe real-world harm, including:

- stalking and personal safety threats
- coercion / blackmail / intimidation
- identity theft and financial harm
- discrimination and social targeting
- irreversible long-term behavioral profiling (“permanent record” risk)

So the **Surveillance Warning (SW)** is anchored to the same principle as hazardous product warnings:

If a product can cause serious harm through its normal operation, the user should receive a visible warning and plain-language explanation at purchase/activation.

This is why the warning should appear on the **package or invoice/checkout/first-run** — not only inside lengthy legal terms.

Pass Condition (10-second rule)

Pass Condition is met when a typical Owner can understand surveillance/manipulation risk within 10 seconds, at or before purchase/activation, using a visible disclosure notice written in plain language that includes:

1. **Behavior Disclosure** (what it does by default / immediately)
2. **Remote Power Disclosure** (remote access/admin/shutdown: Yes/No/Unknown)
3. **Owner Control Disclosure**
 - **Physical OFF possible?** (Yes/No/Partial/Unknown)
 - **One software switch OFF possible?** (Yes/No/Partial/Unknown)
4. **Disclosure Status** (verified/certified vs self-attested vs unknown)
5. **Where to find details** (short reference; not buried terms)

Non-compliance indicator: disclosure exists only in long terms-of-service, a policy page, or post-purchase documentation.

Shadow Audit Checklist

1) Visible Surveillance Warning exists *before or at* purchase/activation

- PASS: shown on package / invoice / checkout / confirmation / first-run
- PARTIAL: only visible after purchase (settings/help pages)
- FAIL: only buried in legal terms or not present

2) Behavior Disclosure is stated as “DOES / DEFAULTS,” not “MAY / CAN”

This is your key correction: the harm is what it **does immediately**, not what it *could* do.

- PASS if the warning states, in plain language, what happens:
 - **on first launch**
 - **by default**
 - **continuously / in background**
 - **without explicit user approval**
- PARTIAL if it's vague (“may collect data”)
- FAIL if it only describes potential capability (“can”) without default behavior

3) Data/Observation Types are listed plainly (minimum set)

The SW should disclose whether the product **records/collects**:

- Audio (microphone)
 - Video (camera)
 - Location
 - Biometrics
 - Behavioral profiling / usage telemetry
 - Content access (files/messages/contacts)
 - Network activity (where relevant)
- PASS: explicit list (Yes/No per category, or clear statement)
 - PARTIAL: incomplete list
 - FAIL: no meaningful specifics

4) Remote Power Disclosure (Yes/No/Unknown)

The SW should answer whether a non-Owner can:

- access data remotely
- administer/control the device
- push forced updates/settings
- disable features or the product remotely (“remote shutdown”)

PASS: Yes/No/Unknown is shown clearly

PARTIAL: implied but unclear

FAIL: not disclosed

5) Owner Control Disclosure — Physical OFF

Does the Owner have a **hardware-enforceable OFF** option (not just a software toggle)?

Examples: camera shutter, mic hardware cut, sensor disconnect, modem kill switch.

PASS: “Yes” + what it disables

PARTIAL: physical control exists but incomplete (some sensors only)

FAIL: no physical OFF / not disclosed

6) Owner Control Disclosure — One Software Switch OFF

Can surveillance/telemetry be disabled **easily** (one clear switch) without navigating complex menus?

PASS: single switch exists + scope stated

PARTIAL: requires multiple permissions scattered across apps

FAIL: no clear software OFF path / dark-patterned controls

7) Multi-Software Requirement (preinstalled apps/services)

Devices (like smartphone/laptop/car) can include many preinstalled systems.

PASS if the SW includes disclosure for:

- the **device/OS layer** AND
- **each preinstalled surveillance-relevant component** (assistant, analytics, cloud sync, OEM apps, “safety/security” services)

PARTIAL if only OS-level statement exists

FAIL if disclosures are missing per component

8) Disclosure Status (Verified / Self-attested / Unknown)

PASS: the SW states verification status clearly

PARTIAL: suggests verification (“secure”) but no status

FAIL: marketing-only language

9) Persistent Proof (invoice/confirmation reference)

PASS: the disclosure is referenced in a retrievable artifact (invoice/receipt/confirmation)

PARTIAL: only visible once

FAIL: no record

38. Voter Approval for Border Changes [AUDIT EFFECT]

Extension ID: D32-R38-EXT

Shadow Audit Notice (How to use this extension)

This extension is a **Shadow Audit checklist** for verifying whether any **Annexation** or **Separation** meets the **minimum authorization threshold** required by Owners.

R38 treats border changes as “contract-level rewrites.”

If the authorization protocol is not satisfied, the border change is **invalid** and any Owner can consider it that way.

This checklist is written to produce **binary outcomes** (PASS / FAIL) using auditable evidence.

Preamble (Anchoring)

Border changes are not routine policy decisions. They permanently alter:

- **who votes** (voter dilution / imported electorate effects)
- **who is protected and who is exposed** (security risk, conflict inheritance)
- **who pays** (debt, taxes, welfare/pension obligations)
- **what laws govern Owners** (jurisdictional replacement)
- **what wars or sanctions Owners inherit**

In practice, **unauthorized annexation or separation** is comparable to an **unauthorized constitution rewrite**. It can transform the Owner’s future without consent.

This is why R38 demands **maximum consent clarity** and **high-quality voting integrity**, not elite-level dealmaking, administrative shortcuts, or emergency manipulation.

Purpose (Pass Condition)

R38 PASS occurs only if ALL conditions below are satisfied:

1. **365-day public disclosure lead-time** (resets if terms change)
2. **Valid vote authorization** under the **Double-Lock Standard**
3. **High-quality vote integrity** (must meet the Voting Integrity right and its audit checklist)
4. **No administrative “equivalents”** that bypass Owner consent
5. **Post-authorization execution is faithful** (no silent implementation changes)

FAIL on any condition triggers

Scope

R38 applies to any territorial change, including:

- **Annexation** (absorption, merger, integration of jurisdictions)
- **Separation** (secession, decoupling, partition)
- Any administrative action that **functionally changes borders**, even if labeled “temporary,” “special zone,” “integration agreement,” “autonomy framework,” or similar.

Definitions

Annexation: A two-party event where two jurisdictions merge or one absorbs another.

Separation: A one-party event where a territory exits the primary Organization.

Owner Mandate: A valid authorization vote meeting the Double-Lock Standard.

365-Day Rule: Full terms must be publicly disclosed for ≥ 365 days before the authorization vote.

Reset Rule: Any material change to terms restarts the disclosure clock.

Double-Lock Standard: A mandate is valid only if BOTH conditions are met:

- **Lock A (Electorate Lock):** YES votes are **>50% of the total eligible electorate**, AND
- **Lock B (Supermajority Lock):** YES votes are **$\geq 2/3$ of ballots cast**

Voting Integrity Gate: Any R38 vote must meet the **High-Quality Voting** requirements and pass the relevant Shadow Audit checklist for election integrity.

Evidence Package (Collect before scoring)

Gather these items for the case file:

- Official proposal text + all versions + dates
- Official announcement date and the scheduled vote date
- Plain-language summary of terms (tax/debt, security, citizenship, voter eligibility impacts, governance changes)
- Eligible electorate definition and counts (baseline + final)
- Voter roll publication/audit artifacts
- Vote results: total ballots cast, YES/NO totals, turnout, invalid ballots
- Implementation timeline: treaties, executive orders, administrative actions
- Proof of any term changes after announcement
- Proof of intimidation, censorship, emergency measures, or coercion (if present)

Scoring Framework

For each checkpoint mark: **PASS / PARTIAL / FAIL**, and attach evidence.

R38 is **FAIL** if any core item fails.

A) Lead-Time & Transparency Controls (365-Day Protocol)

A1 — Full public disclosure occurred ≥365 days before the vote

PASS if: complete terms are published and accessible ≥365 days before the vote date.

FAIL if: vote occurs sooner, key terms appear late, or disclosure is incomplete.

A2 — Reset Rule enforced (term changes restarted the clock)

PASS if: material changes trigger a public revision record AND the 365-day timeline restarts.

FAIL if: major changes are relabeled “minor” to avoid restarting.

A3 — Owner-Readable Summary exists (contract-impact clarity)

PASS if: a plain-language summary exists covering at minimum:

- tax/debt impact
- security/war exposure
- citizenship and voter eligibility changes
- governance and legal-system changes
- timeline and irreversible steps

FAIL if: only long technical texts exist and ordinary Owners cannot understand consequences.

B) Vote Type Rules (Annexation vs Separation)

B1 — Annexation requires two-party authorization

PASS if: both jurisdictions hold valid votes for the entire eligible electorate, and both pass Double-Lock.

FAIL if: only one side votes, only partial regions vote, or any side fails Double-Lock.

B2 — Separation requires the separating territory's vote only

PASS if: the separating territory holds the authorization vote for its eligible electorate.

FAIL if: separation occurs without a valid territory vote.

Clarification:

Only eligible Owners **resident in the separating territory** vote on separation. The primary Organization does not “vote to approve” separation.

C) Voting Integrity Gate (High-Quality Voting Required)

A border-change vote is **invalid by default** unless it meets the **High-Quality Voting** standard.

C1 — Election integrity checklist passed

PASS if the vote meets the high-quality voting criteria (verifiable rolls, auditable count, anti-fraud controls, transparent procedures, meaningful observer access, enforceable dispute resolution).

FAIL if the vote cannot be audited, rolls are unstable/unverifiable, counting lacks integrity, or the process is coercive.

C2 — Electorate definition stability during the mandate period

PASS if eligibility rules and electorate definition remain stable during the disclosure period and are publicly auditable.

FAIL if eligibility is altered late, expanded strategically, or “mass registration” occurs without verification.

D) Anti-Bypass Controls (No “Silent Annexation”)

E1 — No de facto border change before authorization

PASS if no irreversible integration begins prior to mandate.

FAIL if implementation starts before vote (administrative absorption, security control shifts, legal system changes, forced citizenship changes).

E2 — No “temporary framework” used to bypass mandate

PASS if temporary measures do not create irreversible outcomes and remain strictly reversible until mandate.

FAIL if temporary arrangements become permanent without authorization.

E) Coercion & Emergency Manipulation Safeguards

F1 — Mandate environment is free from intimidation and vote-distorting emergency powers

PASS if Owners can freely decide without coercion, censorship, or retaliation.

FAIL if emergency decrees, intimidation, censorship, or retaliation distort the decision environment.

F) Expedited Separation Safety Valve (180-Day Protocol)

Some events impose extreme burdens on Owners and justify a faster exit option.

F1 — Expedited separation is allowed only under extreme trigger conditions

PASS if a verified extreme condition exists, such as:

- unauthorized annexation / structural border change without mandate
- extreme non-compliance that functionally voids the Owner-contract
- **unprovoked aggression / offensive war (“war of choice”)** initiated by the Organization, creating severe Owner burdens (sanctions risk, conscription, economic collapse, legal/moral liability)

FAIL if expedited separation is used as a shortcut without extreme trigger evidence.

F2 — Expedited disclosure period satisfied (≥180 days)

PASS if full terms are disclosed for ≥180 days and the Reset Rule is honored.

FAIL if rushed below 180 days or terms change without reset.

39. Fair Pay to Prevent Corruption [AUDIT EFFECT]

Extension ID: D32-R39-EXT

To attract capable leadership and reduce the economic incentive for systemic corruption, Owners may advocate for standardized, transparent compensation ranges for high-stakes Agents. If the disclosure and benchmark criteria in the Shadow Audit below are satisfied, Owners can reasonably conclude that **structural underpayment is unlikely to be the primary corruption driver**—while recognizing that corruption may still occur through other mechanisms. This extension anchors compensation to **local median net income** and **organizational scale**, so pay is neither arbitrarily low nor politically improvised.

As a positive historical example: A cornerstone of **Singapore's** economic success—institutionalized in the 1960s and maintained to this day—is the policy of providing competitive, market-aligned salaries for civil servants to attract top-tier talent while enforcing a zero-tolerance policy toward corruption.

Operational Note on Binding Authority: A formal request by an individual Owner for the disclosure of salary ranges is an exercise of transparency and does not constitute a binding mandate for the Organization to adjust current compensation levels. The Organization maintains final operational discretion over the timing and implementation of salary adjustments, using these requests as a metric of stakeholder awareness and strategic pressure for market alignment.

Shadow Audit Benchmarks

A. The Standardized Compensation Formula

The compensation range for any high-level position is determined by the intersection of the local economic baseline, the complexity of the role, and the jurisdictional scale. This objective approach makes public service more attractive to high-skilled professionals who may have previously avoided politics due to non-competitive compensation.

The Calculation:

Salary Range=[Local Median Net Salary]×[Position Factor]×[Population Factor]

B. Multiplier Tiers: Position-Weighted Factors

The following factors define the baseline multiplier for specific levels of organizational responsibility:

- **Tier 1: National Executive Leadership (8x min to 20x max)**
 - President, Head of Government, Cabinet Ministers (Ministry Heads).
 - Heads of Police, Military, Intelligence, and Internal Revenue Services (IRS).
 - Members of the Supreme Court and the Head of the Electoral Commission.
- **Tier 2: Legislative & High-Level Deputy Roles (4x min to 10x max)**
 - Members of Parliament, Congress, or Senate.
 - Top three (3) deputy or assistant director roles within the primary agencies (Police, Military, Intelligence, IRS).
- **Tier 3: Municipal Executive Leadership (3x min to 5x max)**
 - Heads of Municipal Councils (for populations exceeding 5,000).
- **Tier 4: Local Governance Representatives (2x min to 3x max)**
 - Members of Municipal Councils (for populations exceeding 5,000).

C. Multiplier Tiers: Jurisdictional Scale Factors

The complexity of management increases with the population size of the jurisdiction, represented by the following multipliers:

Population Size	Scale Factor
Above 100 Million	5x
Above 10 Million	4x
Above 1 Million	3x
Above 0.1 Million (100k)	2x
Below 0.1 Million (100k)	1x

D. Illustrative Operational Examples

- **National Executive:** The President of a country with a population of **70 million**.
 - *Scale Factor:* 4x (for population >10M).
 - *Position Factor:* 8x–20x.
 - **Result:** The salary **should** be between **32x and 80x** of the **Median Net Salary** of the country.
- **Local Representative:** A city council member in a municipality of **11 million**.
 - *Scale Factor:* 4x (for population >10M).
 - *Position Factor:* 2x–3x.
 - **Result:** The salary **should** be between **8x and 12x** of the **Local Median Net Salary**.