Clustra Security Review Checklist

Sample controls and evidence artifact

Preview material for enterprise evaluation. Not a legal document or customer deployment proof.

Review Surface

- Data boundary: prompts, responses, traces, logs, and model artifacts.
- Identity: users, applications, agents, approved models, and policy owners.
- Network: gateway path, private frontends, runtime isolation, restricted environments.
- Retention: customer-owned evidence stores and retention policy mapping.

Clustra Security Review Checklist

Sample controls and evidence artifact

Preview material for enterprise evaluation. Not a legal document or customer deployment proof.

Control Questions

- Who can publish or retire approved model names?
- Which applications can access each model through the gateway?
- Where are traces and audit events retained?
- How are secrets handled and rotated?
- What evidence is required before production approval?

Clustra Security Review Checklist

Sample controls and evidence artifact

Preview material for enterprise evaluation. Not a legal document or customer deployment proof.

Expected Outputs

- Control owner map.
- Open security questions and risk register.
- Evidence required for production hardening.
- Recommended policy updates and follow-up owners.