RAVENFORGE OT

OT assurance approach and framework

Purpose

A repeatable OT assurance method connecting operational context to evidence, decisions and improvement. A control checklist supports practitioner judgement; it does not replace it.

1. Scope and operational context

Agree sites, systems, vital processes, stakeholders, operational constraints and evidence boundaries. Record exclusions and dependencies before assessment. The customer retains production change authority.

2. Architecture and applicability

Review documented assets, zones, conduits, access paths and dependencies. Mark each control applicable, not applicable with rationale, or unknown. Missing evidence is not a pass.

3. Evidence and control assessment

Use original control prompts and expected evidence. Record reference, date, reviewer, implementation status, effectiveness observations and limitations. Sample depth is agreed in the statement of work.

4. Operational scenarios

Identify plausible causes, affected assets, operational consequences and existing safeguards. Rate impact and likelihood using customer-approved definitions. Preserve rationale; ordinal scores are prioritisation aids, not financial loss estimates.

5. Findings and treatment

Link each finding to evidence and affected controls/scenarios. Record treatment options, dependencies, proposed owner, due date and acceptance authority. Safety/availability-critical concerns receive explicit review rather than disappearing into averages.

6. Roadmap and executive report

Sequence actions according to operational consequence, feasibility, dependencies and maintenance windows. Report unknowns and evidence quality alongside progress. Include scope, critical decisions, actions and investment assumptions.

7. Reassessment

Review implementation evidence and effectiveness before changing a control or risk conclusion. A completed action or project percentage does not automatically reduce risk. Track the reviewer, date and remaining uncertainty.

Framework references

IEC 62443, NIST CSF 2.0 and NIST SP 800-82 can inform agreed assessment criteria. This pack is an original working method, not the text of those standards or a formal conformity/certification instrument. A versioned crosswalk and permitted source access are required for a standards-specific engagement.

Responsible use

Do not perform intrusive tests or make production changes without separate scope, authorisation and operational safeguards. Store customer evidence in an approved system. Use Microsoft Copilot only with approved information and human verification; no customer data is sent to AI by these tools.