Technology and Territory

IT/OT Systems Review

What you run, how it connects, and where the risks are

Prepared for: [Client organization] · Prepared by: Onake Systems Inc.

Representative excerpts from a full engagement report.

Inside this sample

- Systems and asset inventory
- Where IT and OT meet
- Risk and single points of failure
- Decision-making framework
- Prioritized roadmap

SECTION 1

How to read this report

This review documents the technology your organization runs today, maps where your information systems and the operational systems that run physical infrastructure meet, and identifies where the risks and single points of failure sit. It is written to be used: the inventory and mapping tables become the working record your team maintains after the engagement, and the risk findings drive a prioritized plan of action.

The review separates two things that are usually tangled together: information technology (email, records, networks, cloud services) and operational technology (the SCADA, controllers and sensors that run water, power and building systems). Where these two worlds connect without anyone owning the seam is where most avoidable risk lives.

- Findings are stated against evidence, not impression.
- Every risk is rated by likelihood and by consequence if it occurs.
- Where information was unavailable, the report says so rather than estimating.

Scope of this sample

This document contains representative excerpts. A full engagement report runs approximately 40 to 60 pages, depending on the number of systems reviewed.

SECTION 2

Systems and asset inventory

Every system the organization runs, what it does, where it lives, and who is responsible for it. Most organizations have never assembled this in one place, and the exercise routinely surfaces systems no one is clearly accountable for and services that quietly renew.

System	Type	Location	Owner	Status
Financial / ERP	IT	Cloud (US)	Finance	Supported
Water treatment SCADA	OT	On-site	Public works	Aging
Email / files	IT	Cloud (CA)	Admin	Supported
Building controls	OT	On-site	Unassigned	Unknown
Member records	IT	On-site server	Admin	At risk
Backup power / genset	OT	On-site	Public works	Supported

In the example above, two findings come from the inventory alone: building controls have no assigned owner, and the member-records server is a single on-site machine flagged at risk. Neither is a technology problem first; both are accountability problems that technology then inherits.

SECTION 3

Where IT and OT meet

The seam between information and operational technology is where convenience and risk trade off directly. Connecting a control system to the office network or the internet makes it easier to monitor, and also easier to reach. This section maps every one of those connections and states what protects it.

Connection	Purpose	Exposure	Segmented	Risk
SCADA to office LAN	Remote monitoring	Internal	No	High
SCADA to internet	Vendor support	Public	No	Critical
Building controls to LAN	Scheduling	Internal	Partial	Medium
Genset to SCADA	Status alerts	Internal	Yes	Low
Cameras to internet	Remote view	Public	No	Medium

The critical finding here is common and dangerous: the water-treatment SCADA is reachable from the internet for vendor support, with no network segmentation between it and the public. National cyber authorities have confirmed real intrusions into exactly this configuration at small Canadian water systems. This is the first thing to close.

SECTION 4

Risk and single points of failure

A single point of failure is any component whose loss stops something important, with no fallback. This section lists them by consequence, not by cost, because the cheapest thing to fix is often the one that would hurt the most.

Component	If it fails	Fallback	Likelihood	Priority
Member-records server	Records lost	None	Medium	Critical
Water SCADA link	Blind operation	Manual	Medium	Critical
Single internet line	All sites offline	None	High	High
One IT contractor	No support	None	Medium	High
On-site backups only	Fire / theft loss	None	Low	High

Two of these stand out. The member-records server has no backup off the premises, so a fire or theft loses the records outright. And a single internet line takes every site offline at once. Both are inexpensive to address relative to the consequence of leaving them.

SECTION 5

Decision-making framework

This section is written in plain language for council and administration. Technology fails communities most often not through bad systems but through decisions made with no framework: who decides what is bought, who owns each system, and how spending is reviewed. The tools below are the ones the toolkit provides for your team to run itself.

- Name an owner for every system in the inventory. An unowned system is an unmanaged risk.
- Route technology spending above a set threshold through a standing review, even a two-person one.
- Keep a written decision log, so a change of staff does not erase why a system was chosen.
- Separate the decision to buy from the vendor selling it: define the need first, in writing.

How to use this section

The framework is deliberately lightweight. The goal is a decision that can be explained and defended later, not a heavy process that no one follows.

SECTION 6

Roadmap

Findings are ordered by consequence. The items that address an exposed critical system or an unrecoverable data loss come first, regardless of cost, and the larger planning work is identified separately so it can be scheduled rather than rushed.

Priority	Action	Horizon	Indicative cost
1	Remove water SCADA from direct internet exposure	0-1 months	$3k-8k
2	Off-site backup for member records	0-2 months	$2k-6k
3	Assign an owner to every system	0-3 months	administrative
4	Second internet path for critical sites	3-9 months	$10k-25k
5	Full IT/OT segmentation design	6-12 months	$15k-40k

- Costs are indicative ranges for planning only and are not quotations.
- Items 1 and 2 address exposures that could cause real harm and should proceed regardless of funding outcomes.
- Items 4 and 5 are the design work that a funding application or a larger engagement would build on.