



ENGAGEMENT REPORT — SYSTEMS AND RISK

IT/OT Systems Review

What you run, how it connects, and where the risks are — traced to the seam where information and operational technology meet.

SAMPLE EXCERPT

- | | | | |
|------------------------------|--------------------------------|--------------------------------|--------------------------------------|
| 01 How to read this report | 02 Systems and asset inventory | 03 Where IT and OT meet | 04 Risk and single points of failure |
| 05 Decision-making framework | 06 Roadmap | — Three figures, listed inside | |

PREPARED FOR

[Client organization]
Community and council

PREPARED BY

Onakeio Systems Inc.
Kanesatake, Québec

DOCUMENT

Representative excerpts
Full report runs 40–60 pp.

LANGUAGES

EN / FR
info@onakeio.ca

This document reproduces representative sections of a full IT/OT Systems Review. The tables and figures use illustrative data from a composite community; the structure, method and standard of evidence are those of a real engagement.

01	How to read this report	What the review covers, and the standard of evidence it holds itself to.
02	Systems and asset inventory	Every system the organization runs, where it lives, and who is responsible for it.
03	Where IT and OT meet	Every connection between the two worlds, and what protects it.
04	Risk and single points of failure	Listed by consequence, because the cheapest fix is often the one that matters most.
05	Decision-making framework	How technology decisions get made, and who is accountable for them.
06	Roadmap	Ordered by consequence, with the planning work scheduled rather than rushed.

Figures

Fig. 3.1	Where information and operational technology meet
Fig. 4.1	Single points of failure by likelihood and consequence
Fig. 6.1	Twelve-month sequence, ordered by consequence

How the full report differs

A complete review runs approximately 40 to 60 pages, and adds the per-item technical annexes, the supporting correspondence, and the working spreadsheets your team keeps and maintains afterwards.

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, meaning the SCADA systems, 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.

The standard of evidence

- 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.
- Every risk is traced to a named component, not to a general condition.

WHAT THIS REPORT IS NOT

It is not a procurement document and not a quotation. Costs are planning ranges. It does not name a preferred provider, and Onakeio takes no commission, referral fee or reseller margin from any vendor named in it.

Scope of this sample

This document contains representative excerpts. A full engagement report runs approximately 40 to 60 pages.

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

FINDING 2.1

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.

What the inventory is used for afterwards

- **Accountability.** A system with a named owner gets patched, budgeted and renewed. An unowned system is discovered when it fails.
- **Budgeting.** Aging and unsupported systems can be scheduled for replacement rather than replaced in an emergency at a premium.
- **Continuity.** When staff or contractors change, the record of what runs the community does not leave with them.

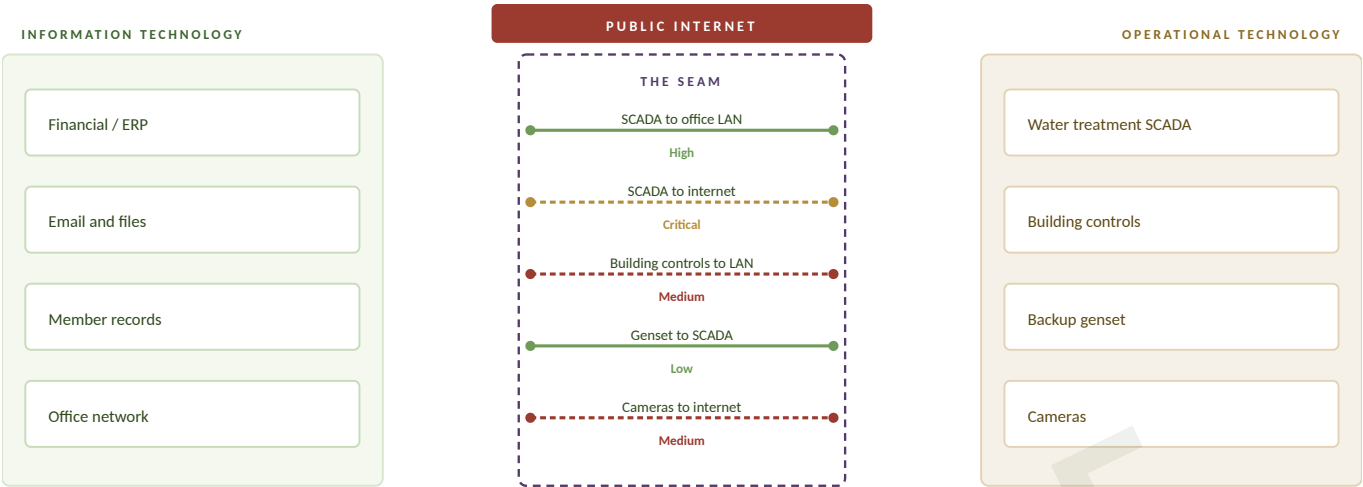
SECTION 3 Where IT and OT meet

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	Yes	HIGH
SCADA to internet	Vendor support	Public	Partial	CRITICAL
Building controls to LAN	Scheduling	Internal	No	MEDIUM
Genset to SCADA	Status alerts	Internal	Yes	LOW
Cameras to internet	Remote view	Public	No	MEDIUM

FIGURE 3.1



Each crossing is a decision someone made. Where no one owns the crossing, no one reviews it.

The unsegmented path from the public internet to water treatment is the finding that outranks every other in this review.

The seam, drawn. Each line is a connection someone made for a reason. Solid lines are segmented; dashed lines are not. The path from the public internet to water treatment is the one that outranks every other finding in this review.

FINDING 3.1

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, and it is inexpensive to close.

Why this is the seam and not simply a firewall question

Segmentation is a technical control, but the reason it is missing is almost never technical. It is missing because the office network and the plant are owned by different people, and the connection between them is owned by neither.

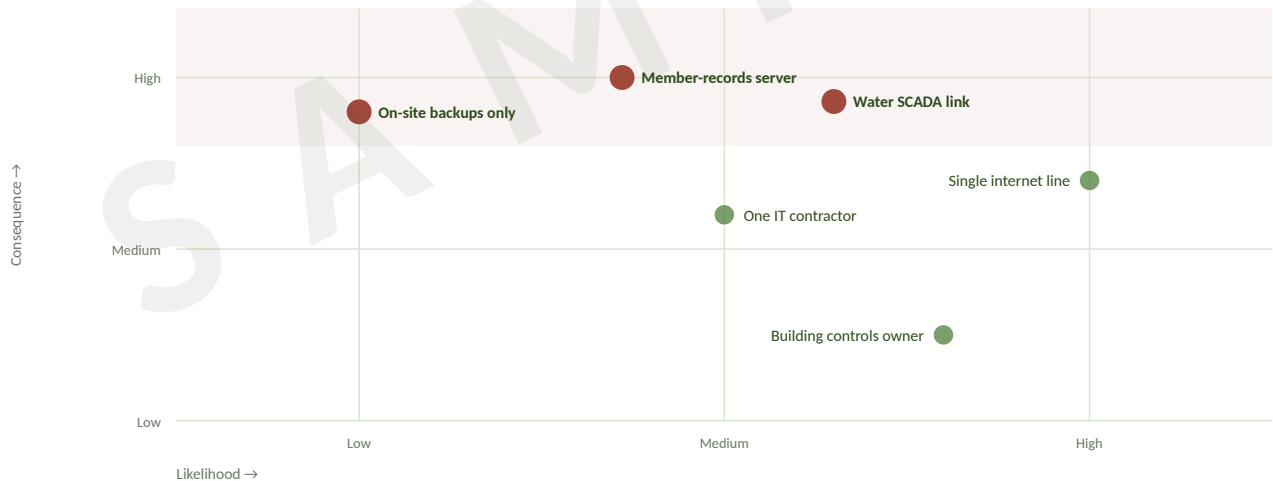
SECTION 4 Risk and single points of failure

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

FIGURE 4.1



Everything in the upper band stops something important and has no fallback. Cost is not what orders this chart.

Placed by likelihood against consequence. The shaded band is where a failure stops something important and nothing catches it. Cost does not appear on this chart, and deliberately so.

FINDING 4.1

Two of these stand out. The member-records server has no backup off the premises, so a fire or a 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

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. This section is written in plain language for council and administration, and 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.

Why a framework rather than a policy

A policy describes what should happen. A framework describes who decides, and that is the part that is usually missing. Every finding in Section 2 that concerned ownership rather than technology would have been caught by the first bullet above.

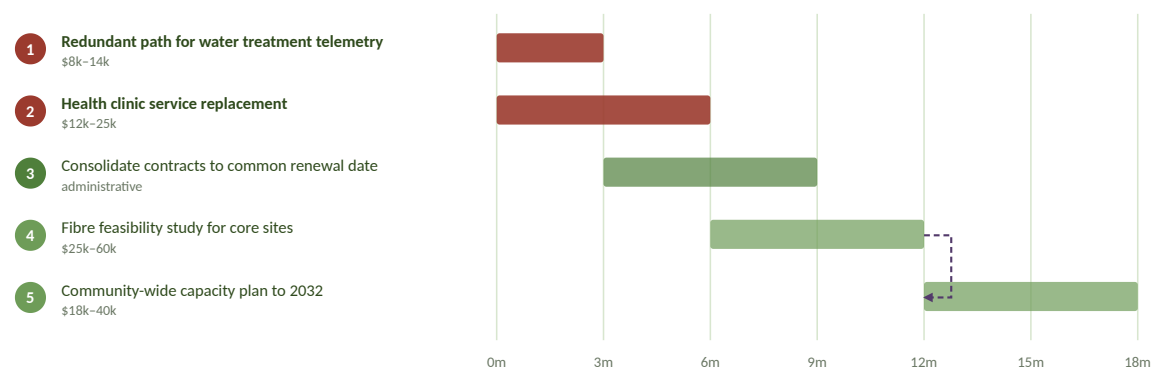
SECTION 6 Roadmap

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

FIGURE 6.1



Items 1 and 2 answer documented failures against critical requirements and proceed regardless of funding. Items 4 and 5 are the documentation most federal and provincial programs ask for at application.

Twelve-month sequence. The first two items close active exposure and are measured in weeks, not quarters. The dotted line marks the dependency: segmentation design assumes the second path exists.

- 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.

What happens after this report

The inventory, connection map and risk register are delivered as editable working documents. Your team maintains them, and the decision framework in Section 5 is designed to be run without us.

About this sample

Onakeio Systems Inc. is a 100% Indigenous-owned IT and operational technology practice based in Kanesatake, Québec, working with First Nations, government and critical infrastructure operators across Canada, in English and French. To discuss an engagement for your community, write to info@onakeio.ca.