LEADERSHIP WORKING GUIDE | 20-MINUTE INITIAL ASSESSMENT

How exposed are your operations?

OT, ICS & IoT cybersecurity risk and readiness self-assessment

Could a cyberattack disrupt the equipment your business depends on?

Manufacturing equipment. Refrigeration. Warehouse automation. Medical devices. Building controls. Connected machinery.

These systems support production, revenue, safety, and everyday business operations. Many are connected to other systems, networks, or external service providers, creating cybersecurity risks that traditional IT security may overlook.

This assessment helps you evaluate how well your organization understands, protects, monitors, and prepares to recover its critical operational technology.

> **Who this is for**
>
> Business, operations, IT, and cybersecurity leaders. Allow approximately 20 minutes for the initial discussion; verifying answers or assessing additional locations may take more time.

Step 1: Decide what you are assessing

You can assess your entire organization, one facility, a department, an assembly line, or a critical business process. For a large organization, start with one operational area and repeat this assessment for others. Only select the entire organization if you can support your answers across all relevant locations and systems.

Organization / facility:

Assessment scope:

Examples: Distribution center, manufacturing line 3, hospital laboratory, refrigerated warehouse, or entire organization.

Completed by / date:

STEP 1 | CONTINUED

Look beyond the obvious equipment

Consider the equipment that performs the work and everything it depends on.

Examples include controllers, sensors, monitoring systems, network connections, supporting software, building infrastructure, and equipment managed by outside vendors.

Some systems may be connected without your IT team knowing about them. Others may be physically isolated but still critical to operations.

What critical equipment or processes are included in this assessment?

What other systems, services, or vendors do those operations depend on?

What would happen if these operations stopped or were manipulated?

How to complete this assessment

Bring together someone who understands business operations and someone familiar with your technology, facilities, or equipment.

For each statement on the following pages, select the answer that best reflects your verified current state.

2	Yes, verified	We have current evidence supporting our answer.
1	Partially verified	We can demonstrate some coverage, but gaps remain.
0	No	We know this capability or protection is missing.
?	Unknown	We do not have enough evidence to answer.

What counts as verification?

Verification applies to everything in this assessment: equipment inventories, system dependencies, vendor access, security protections, monitoring, and recovery capabilities.

Evidence might include technical discovery results, physical inspections, network maps, recent vendor assessments, system configurations, or documented testing.

> **Do not substitute confidence for evidence**
>
> An old spreadsheet, outdated diagram, or someone's assurance that everything is covered may not accurately represent today's environment. Good visibility is maintained over time. You should know what exists today and recognize when equipment, connections, or critical settings change. If you cannot verify an answer, mark it unknown.

Evidence sources used for this assessment

Record how you checked your answers and anything you could not confirm. You can use this section later to support the scores and assign follow-up work.

Recent discovery results, records, tests, or inspections reviewed:

Assets, connections, suppliers, or protections still needing verification:

STEP 2 | QUESTIONS 1–3

A. Asset visibility and business impact

Evaluate only the systems and operations defined in Step 1. Select 2 / 1 / 0 / ? for each statement based on current evidence, not assumption.

1. We know what operational equipment we have and when something changes.

Our inventory has been verified through discovery or inspection, is kept current, and helps us identify new equipment or changes to existing systems and connections.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

2. We understand which systems are critical and what they depend on.

We know how equipment supports the business, what other systems, data, and suppliers it relies on, and what would happen if those dependencies failed.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

3. Someone is accountable for every critical operational system.

We know who owns each system, approves changes, manages suppliers, and is responsible for addressing its cybersecurity risks.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

STEP 2 | QUESTIONS 4–6

B. Access, supplier risk, and vulnerabilities

Check your ability to show how critical equipment is reached, how supplier risks are managed, and whether weaknesses are being reduced.

4. We know how someone could reach or gain control of our critical equipment.

We have verified connections and potential access paths through business networks, remote systems, vendors, and physical access, with protections limiting unnecessary access.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

5. We evaluate the risks that suppliers and their products introduce into our business.

We review critical suppliers' security practices, product weaknesses, access, and ability to maintain services. We understand how their compromise or failure could affect our operations.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

6. We identify vulnerabilities and take appropriate action to reduce their risk.

We know which equipment has security weaknesses, whether attackers could exploit them, and what protections are in place. When patching is not possible, we use other safeguards to reduce exposure.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

STEP 2 | QUESTIONS 7–9

C. Monitoring, response, and safeguards

Consider what your teams can detect and whether the right people and protective mechanisms are ready to act.

7. We can detect suspicious activity or dangerous changes to critical equipment.

Monitoring can identify unauthorized access, unexpected configuration changes, abnormal equipment behavior, and changes that could disrupt operations.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

8. We have the right people and a documented process to respond.

Our security team or provider, operations personnel, and equipment vendors know their responsibilities. Alerts reach people qualified to investigate, make decisions, and take action, including outside business hours.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

9. Critical equipment has appropriate safeguards against unsafe operation.

Independent alarms, safety controls, or other protective measures can detect or limit dangerous conditions even when primary equipment controls are compromised. These safeguards are tested.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

STEP 2 | QUESTIONS 10–12

D. Incident response and recovery

The key test is whether your organization can restore safe, functioning operations, beyond merely having a written plan or successful backup.

10. We have documented procedures for operational cybersecurity incidents.

Our teams know how to safely isolate affected equipment, coordinate decisions, contain the incident, and begin restoring operations.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

11. We have the resources needed to restore critical operations.

We maintain necessary backups, equipment configurations, software, recovery instructions, and alternative operating procedures. We understand what is required to bring equipment and dependent processes back online.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

12. We have tested that our response and recovery procedures actually work.

Our teams have practiced realistic incidents and validated recovery through appropriate restoration tests or controlled exercises. A successful backup notification or discussion-only exercise is not sufficient proof of operational recovery.

☐ 2 Verified ☐ 1 Partially ☐ 0 No ☐ ? Unknown

Evidence, gap, or follow-up needed:

STEP 3 | SCORE

Calculate your readiness score

Add the 2, 1, and 0 answers in each category. Count unknown answers as zero, but record them separately.

Asset visibility and business impact (1–3)	____ / 6
Access, supplier risk, and vulnerabilities (4–6)	____ / 6
Monitoring, response, and safeguards (7–9)	____ / 6
Incident response and recovery (10–12)	____ / 6
TOTAL PREPAREDNESS SCORE	**____ / 24**
UNKNOWN ANSWERS	**____ / 12**

What your score does and does not mean

This score reflects what you can demonstrate about cybersecurity preparedness in the operational area you selected. It does not calculate the likelihood of an attack, certify safety, or guarantee that systems are secure.

> **Use your score to challenge assumptions**
>
> Read the descriptions on the next pages. If the description of your scoring range does not reflect what you actually do, revisit your answers. Every unknown answer involving important equipment needs investigation.

How to use the next pages

- Compare your score to the corresponding maturity description.
- Review the warning signs that require attention regardless of score.
- Estimate business impact, record significant findings, and assign action owners.

STEP 3 | INTERPRETATION

What your score suggests

19–24 | Stronger demonstrated readiness

Your score suggests you have established OT cybersecurity practices. At this level, we would expect:

- A continuously maintained inventory of operational assets and their dependencies.
- Documented access routes and potential attack paths to critical equipment.
- Ongoing supplier risk reviews and vulnerability management, including compensating controls.
- OT-aware monitoring, documented response responsibilities, and tested recovery capabilities.

Your next steps: Validate that these capabilities work across the environment. Conduct realistic incident and recovery exercises, review attack paths as systems change, and build cybersecurity into modernization, expansion, and equipment procurement plans.

13–18 | Partial readiness

You have some protections in place, but important capabilities may be incomplete. At this level, you may have:

- An equipment inventory that is not continuously verified or updated.
- Basic network protections without a complete understanding of attack paths.
- Supplier reviews, monitoring, or incident procedures that do not cover all critical equipment.
- Backups and response plans without sufficient recovery testing.

Your next steps: Identify assumptions that need validation. Prioritize gaps affecting critical operations, strengthen supplier oversight, and test whether existing safeguards and recovery procedures work.

If the description of your score does not match reality, revisit your answers before using the score to make decisions.

STEP 3 | INTERPRETATION

Understand significant readiness gaps

7–12 | Material preparedness gaps

Your organization has significant gaps in demonstrated readiness. You may be relying on:

- Outdated equipment lists or incomplete knowledge of dependencies.
- Networks and vendor connections without fully understood exposure.
- Informal cybersecurity responsibilities and limited operational monitoring.
- Recovery plans that have never been adequately tested.

Your next steps: Establish verified asset visibility, identify critical access routes and vulnerabilities, assign response responsibilities, and address dangerous exposures. Consider an independent assessment to establish a reliable baseline.

0–6 | Limited demonstrated readiness

You cannot currently demonstrate many of the capabilities needed to protect your operations. Critical equipment, network connections, supplier dependencies, and recovery procedures may be poorly understood or unverified.

Your next steps: Identify the operations whose failure could cause serious business or safety consequences. Verify the equipment and connections involved, investigate immediate exposures, and establish a practical protection plan. If critical operations are involved, seek qualified outside assistance rather than relying on assumptions.

> **Low confidence is a finding**
>
> Do not inflate answers simply because no incident has occurred. For every material gap or unknown, record what needs to be checked, who owns it, and when it will be reviewed.

STEP 3 | WARNING SIGNS

Risks that require attention at any score

Any of the following should trigger further investigation:

- You cannot identify the equipment connected to your operational environment or recognize when it changes.
- You cannot map how someone could reach critical systems through business networks, vendors, remote connections, or physical access.
- Critical systems have exploitable weaknesses without effective patches or compensating controls.
- Shared administrator accounts, inadequate authentication, or uncontrolled supplier access could allow unauthorized changes.
- You cannot demonstrate how harmful changes would be detected, who would respond, or whether critical safeguards work.
- You cannot demonstrate that critical systems and operations can actually be recovered.
- You answered “Unknown” to questions involving important operational systems.

> **An unknown answer needs investigation**
>
> You cannot protect or prioritize something you do not understand.

Confidence is not evidence

When people work in the same environment every day, they get used to how things operate. Old equipment, insecure configurations, excessive permissions, temporary workarounds, and undocumented connections can become accepted simply because they have always been there.

Nothing bad has happened, so nobody questions them.

An independent cybersecurity professional examines that same environment without those assumptions. They can identify vulnerabilities, unexpected connections, and attack paths your internal team has learned to overlook.

If a single compromised system could stop production, destroy valuable inventory, or endanger people, an independent assessment is worth serious consideration.

Need an independent view? viLogics can help validate your environment and identify exposures.

One final question

> **If someone compromised your most critical equipment tonight...**
>
> Would your team know what happened, how to contain it, and how to restore safe operations?

STEP 4 | BUSINESS IMPACT

Calculate what disruption could cost

You may have identified several gaps or dozens. Document every significant finding; do not stop at an arbitrary number. You cannot fix everything simultaneously, but you need to understand what you are accepting when risk remains unresolved.

A Business Impact Analysis (BIA) helps estimate the consequences of losing a critical process or system.

1. How long could operations be disrupted?

Estimate the effects of a 1-hour, 8-hour, 24-hour, or multi-day outage. Identify how long the business can tolerate disruption before consequences become unacceptable.

Critical process and disruption scenario:

Estimated outage duration / maximum tolerable disruption:

---

2. What would the interruption cost?

> **Practical estimated loss formula**
>
> Lost business contribution + damaged inventory or equipment + recovery expenses + contractual or regulatory costs

Calculate lost business contribution using profit lost from sales or production that cannot be recovered. Add spoiled inventory, equipment damage, overtime, emergency contractors, penalties, and other relevant expenses. Avoid counting the same loss twice.

Illustrative example: An 8-hour production outage

Lost contribution: $5,000/hour × 8 hours	$40,000
Damaged inventory	$20,000
Recovery labor and expenses	$8,000
TOTAL ESTIMATED LOSS	**$68,000**

Illustrative scenario only, not a prediction of cyberattack losses.

STEP 4 | BUSINESS IMPACT

Estimate consequences and set priorities

3. What consequences cannot easily be measured in dollars?

Consider employee or patient injury, environmental damage, regulatory exposure, lawsuits, client trust, and reputational harm. Some consequences cannot responsibly be reduced to a financial estimate.

> **Safety can outrank a dollar estimate**
>
> A credible risk of serious injury, loss of life, or major environmental harm deserves priority even when its financial impact is uncertain.

Your own disruption estimate

Lost business contribution (unrecoverable margin):

Inventory / equipment damage:

Recovery expenses and incremental costs:

Contractual / regulatory expenses:

Estimated total (avoid double counting):

Safety, legal, environmental, or reputation consequences:

STEP 4 | PRIORITIES

Decide what needs attention first

Prioritize every significant finding by considering:

- Business and safety impact: How severe would the consequences be?
- Exposure: Can someone reach or exploit the weakness, and what protections exist?
- Time sensitivity: How quickly could harm occur, and how long would recovery take?
- Uncertainty: What needs verification before you can make an informed decision?

Address urgent safety concerns and readily exploitable, high-consequence weaknesses first. Investigate unknowns that prevent you from understanding critical exposure.

Methodology references: Ready.gov Business Impact Analysis and NIST SP 800-34 Contingency Planning.

Turn your findings into documented actions

For every significant finding, document the risk, action required, accountable owner, target date, and what evidence will prove the issue has been addressed.

Example of a completed action

Risk or gap	An equipment vendor uses a shared administrator account without MFA to access a critical manufacturing system.
Action to reduce risk	Replace shared access with individual vendor accounts, require MFA through a secure access gateway, and restrict access to approved equipment.
Owner / target date	IT Director / agreed deadline
Proof of success	Access configuration is validated and tested. Unauthorized access attempts are blocked, while approved maintenance access still works.

STEP 4 | ACTION WORKSHEET

Your findings and action plan

Use this worksheet for each significant finding. Duplicate it or continue in your risk register until every significant gap has a documented owner and follow-up. The worksheets are examples, not a limit on the number of issues to address.

FINDING / ACTION 1

Risk or gap (what is the situation?)

Potential business and safety impact

Action required to reduce the risk

Owner and target completion date

Proof that the action works (what will be demonstrated?)

STEP 4 | ACTION WORKSHEET

Additional finding and action

Continue until every significant risk has a documented action, owner, due date, and proof of success.

FINDING / ACTION 2

Risk or gap (what is the situation?)

Potential business and safety impact

Action required to reduce the risk

Owner and target completion date

Proof that the action works (what will be demonstrated?)

STEP 4 | ACTION WORKSHEET

Additional finding and action

Duplicate this page in Word or continue in your organization's risk register if more space is needed.

FINDING / ACTION 3

Risk or gap (what is the situation?)

Potential business and safety impact

Action required to reduce the risk

Owner and target completion date

Proof that the action works (what will be demonstrated?)

STEP 4 | NEXT STEPS

Where should you start?

Do not know what equipment you have?

Verify the operational asset inventory, network connections, and business dependencies.

Ask for: OT/ICS/IoT Asset Discovery and Business Impact Assessment.

Uncertain about suppliers or third-party exposure?

Review supplier security practices, product vulnerabilities, contractual obligations, operational dependencies, and remote access.

Ask for: Third-Party Risk and Supply Chain Security Assessment.

Have vulnerabilities that cannot be patched?

Identify how attackers could reach affected equipment and implement effective compensating controls.

Ask for: OT Exposure and Attack Path Assessment with a Remediation Plan.

Unsure whether monitoring and recovery would work?

Validate alerting, response responsibilities, equipment restoration, and operational continuity through realistic exercises.

Ask for: OT Security Monitoring, Incident Response and Recovery Readiness Assessment.

TAKE THE NEXT STEP

Found risks you cannot confidently address?

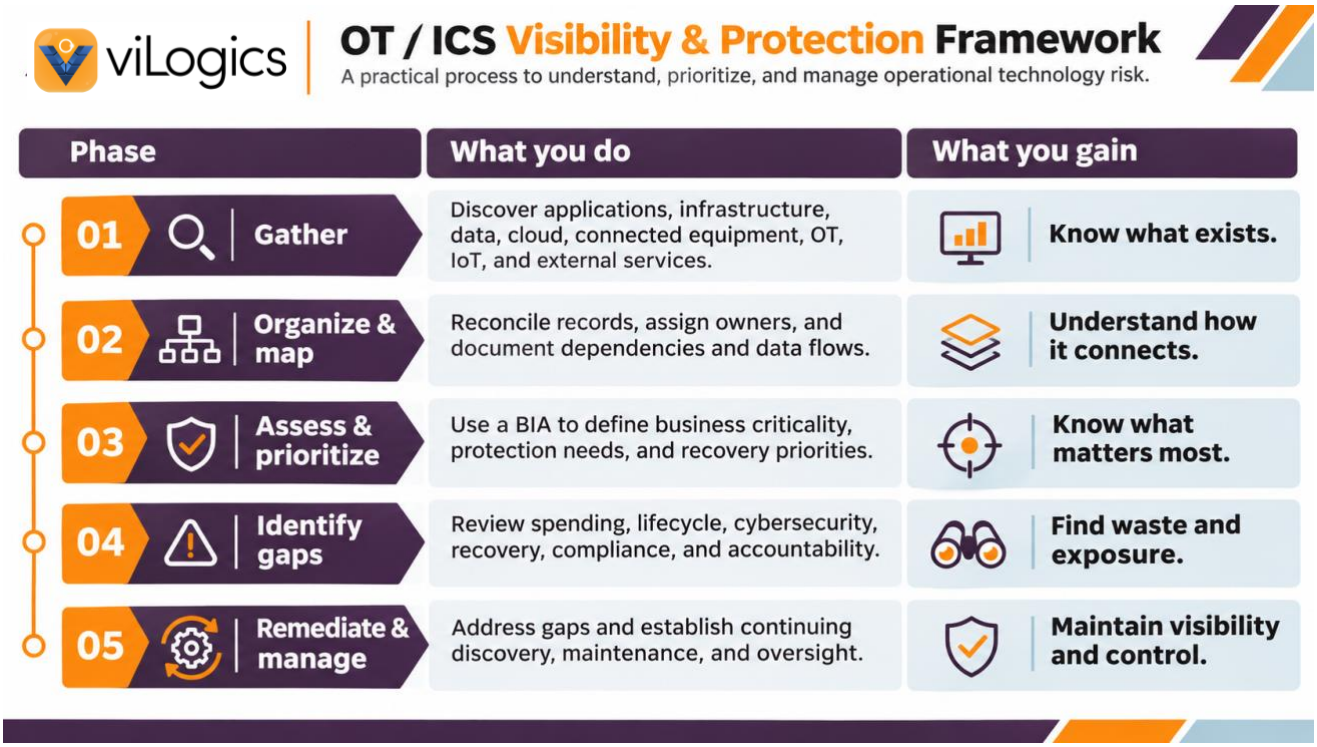
If this assessment exposed gaps, unknown assets, weak protections, or untested recovery capabilities, you need a plan supported by evidence.

viLogics helps organizations discover IT, OT, ICS, and IoT assets, identify critical business dependencies, evaluate vulnerabilities and attack paths, and develop practical protection plans.

Our Asset Visibility & Discovery engagements provide an independent understanding of your environment and the risks most likely to affect your operations. We can help prioritize improvements, strengthen cybersecurity protections, and build an ongoing program that fits your business.

Our Managed OT/IoT Security Services continually monitor these environments and protect them with context not just vulnerability scores.

Secure your OT business now, **Start the conversation** with our OT cybersecurity advisory team.



Important note

This self-assessment is a leadership planning tool, not a formal cybersecurity audit, safety certification, or complete risk assessment. Financial examples are illustrative and should be validated against your organization's actual operating data.