30-point OT security readiness checklist

For operators of industrial sites. Priorities, practical guidance for each point, and a realistic order for the first 18 months.

THE 30 POINTS BY AREA	Fix first	Fix this year	Build over time
1 Know what you run	3	1, 2, 4, 5	
2 Remote access	6, 7, 8	9, 10	
3 Network separation	11, 12	14, 15	13
4 Accounts, passwords and devices	16, 20	17, 19	18
5 Backups and recovery	21, 22, 23	24	25
6 Incident readiness		26, 27, 29	28, 30

BEFORE YOU START

How to use this checklist

1

Who

Your operations lead, or the person who knows the control systems best, plus whoever looks after IT for the site. Allow one hour.

2

How

Read each point and answer Yes, Partly or No. "We think so" is Partly. Write down the evidence for each Yes: a document, a screen, a log. A Yes without evidence is a Partly.

3

Then

Count your Yes answers. Fix the Priority 1 gaps first, then Priority 2, then Priority 3. The plan near the end shows a realistic order.

The three priorities

PRIORITY 1 — **11** points

Fix first

NEXT 30 TO 90 DAYS

A direct way in for an attacker, or the thing that decides whether you get the plant back after an incident.

3 6 7 8 11 12 16 20 21 22 23

PRIORITY 2 — **14** points

Fix this year

3 TO 9 MONTHS

The basics that make Priority 1 last, and that an auditor will ask about.

1 2 4 5 9 10 14 15 17 19 24 26 27 29

PRIORITY 3 — **5** points

Build over time

9 TO 18 MONTHS

Maturity steps. They matter, but only after Priority 1 and 2 are in place.

13 18 25 28 30

> **About the effort figures.** Effort is a rough guide for one mid-sized site with 50 to 300 control devices. It is internal staff time, not calendar time, and it does not include buying equipment.

What is in this document

01	**Scorecard**	one page to print and fill in
02	**Where the points apply**	the network zones in one drawing
03	**The 30 points**	what good looks like, how to do it, who, effort
04	**A realistic order**	from the first 30 days to month 18
05	**Your result**	what your score means and what to do next

PRINT THIS PAGE

Scorecard

Tick one box for each point. The colour shows the priority.

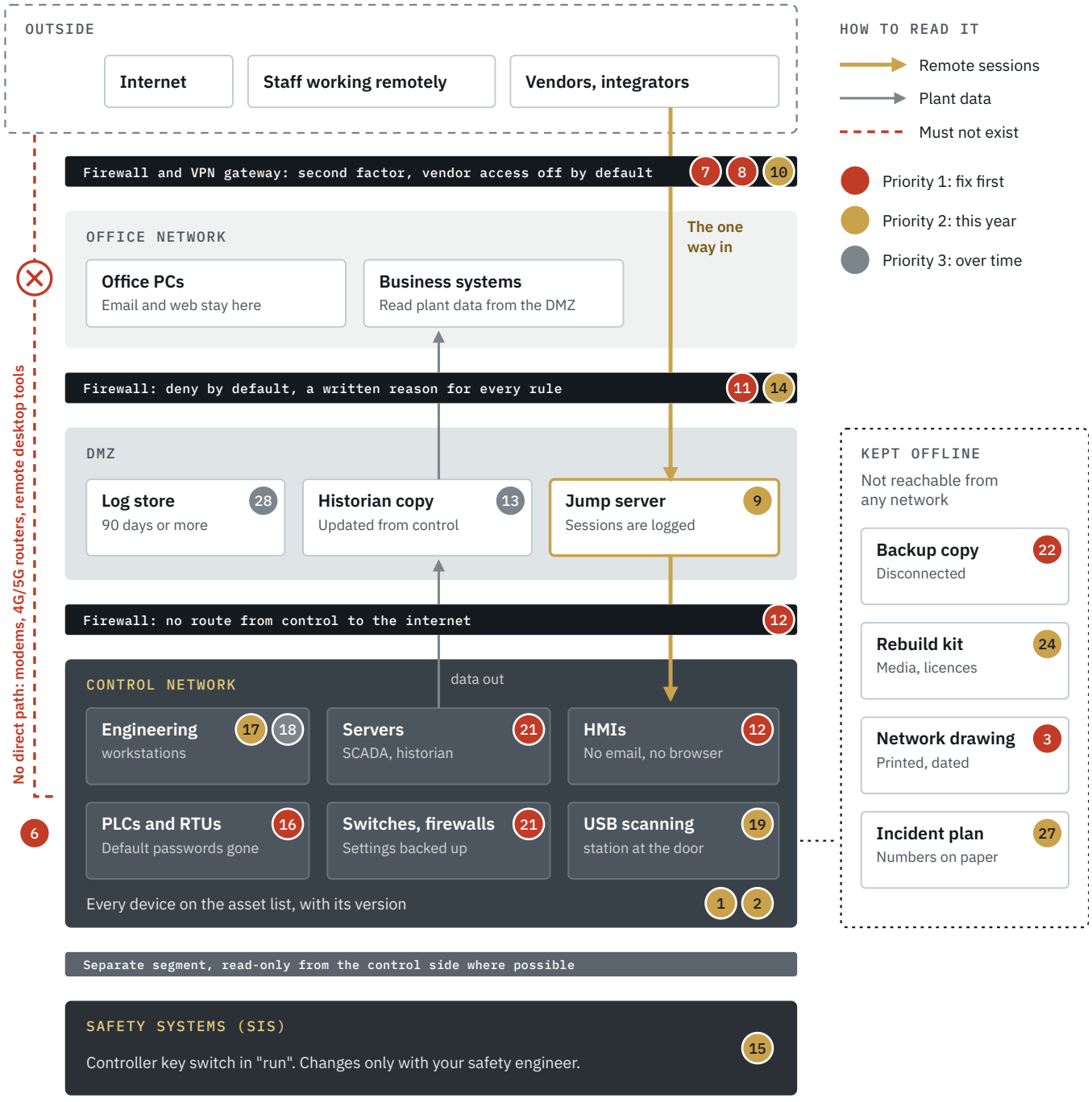
	POINT	PRIORITY	YES	PARTLY	NO	EVIDENCE OR NOTE
1	**Know what you run**					
1	Asset list	P2	☐	☐	☐	
2	Versions on the list	P2	☐	☐	☐	
3	Network drawing	P1	☐	☐	☐	
4	Critical systems	P2	☐	☐	☐	
5	Vendor advisories	P2	☐	☐	☐	
2	**Remote access**					
6	Every way in	P1	☐	☐	☐	
7	Second factor for remote access	P1	☐	☐	☐	
8	Vendor access off by default	P1	☐	☐	☐	
9	One controlled entry point	P2	☐	☐	☐	
10	Review remote accounts every three months	P2	☐	☐	☐	
3	**Network separation**					
11	Firewall between office and control	P1	☐	☐	☐	
12	No internet, email or browsing on control systems	P1	☐	☐	☐	
13	Data leaves through a DMZ	P3	☐	☐	☐	
14	Yearly firewall rule review	P2	☐	☐	☐	
15	Safety systems separate	P2	☐	☐	☐	
4	**Accounts, passwords and devices**					
16	Default passwords changed	P1	☐	☐	☐	
17	Personal accounts	P2	☐	☐	☐	
18	Few administrators	P3	☐	☐	☐	
19	USB sticks and visiting laptops checked	P2	☐	☐	☐	
20	Leavers lose access on their last day	P1	☐	☐	☐	
5	**Backups and recovery**					
21	Backups of what the business needs	P1	☐	☐	☐	
22	One copy offline	P1	☐	☐	☐	
23	Tested restore	P1	☐	☐	☐	
24	Rebuild kit available offline	P2	☐	☐	☐	
25	Manual operation practised	P3	☐	☐	☐	
6	**Incident readiness**					
26	Operators know the signs and who to call	P2	☐	☐	☐	
27	Short incident plan, numbers on paper	P2	☐	☐	☐	
28	Logs kept for 90 days	P3	☐	☐	☐	
29	Who reports, and the 24-hour early warning	P2	☐	☐	☐	
30	Yearly exercise	P3	☐	☐	☐	

Yes answers _____ **of 30** **of which Priority 1** _____ **of 11** DATE _____

SECTIONS 2 AND 3 IN ONE DRAWING

Where the points apply

One controlled way in, a firewall between every zone, and nothing that reaches the control network directly. The numbers are the checklist points.



Not on the drawing, because they are about people and practice: 4 Critical systems · 5 Vendor advisories · 20 Leavers lose access on their last day · 23 Tested restore · 25 Manual operation practised · 26 Operators know the signs and who to call · 29 Who reports, and the 24-hour early warning · 30 Yearly exercise

1 Know what you run

SECTION 1 OF 6 / POINTS 1 TO 5

1 2 3 4 5

1 Asset list

PRIORITY 2 | FIX THIS YEAR

You have a list of every PLC, RTU, HMI, engineering workstation and server in the control network, with where it is and who is responsible for it.

☐ YES ☐ PARTLY ☐ NO

WHY

You cannot protect, patch or restore equipment you do not know you have. Every other point in this checklist depends on this list.

GOOD LOOKS LIKE

One spreadsheet or tool, owned by one person. Each device has: name, type, vendor and model, location (site, cabinet), network address, the process it serves, and the responsible person.

HOW TO DO IT

- Start from what exists: the integrator's documentation, the PLC project files, the switch MAC tables, the SCADA tag database.
- Walk the site with the list, cabinet by cabinet. Paper records are always out of date; the walk finds what they miss.
- Start with passive network discovery (listening to traffic through a mirror port). Be careful with active scans on a live control network: some older PLCs and RTUs stop or reboot when scanned. For newer devices, active scanning with tools built for OT is an option; recent research shows it is less dangerous than previously thought.
- An automated tool is preferable, but a spreadsheet that is updated every six months beats an expensive tool that nobody uses or updates.

WHO

Operations or automation engineer, with the integrator if needed.

EFFORT

3 to 10 days for the first version; then a few hours per change.

COMMON MISTAKE

Building the list once for an audit and never updating it. Add "update the asset list" to the procedure for every change. Review the full list at least once a year.

2 Versions on the list

PRIORITY 2 | FIX THIS YEAR

The list shows firmware and software versions, and someone checked it against the site in the last 12 months.

☐ YES ☐ PARTLY ☐ NO

WHY

When a vendor publishes a flaw, the versions tell you in minutes whether it affects you, instead of in weeks.

GOOD LOOKS LIKE

A firmware/software version column for each device, a "last verified" date, and a yearly check.

HOW TO DO IT

- Read versions from the engineering software (most PLC tools show firmware when online) during planned maintenance.
- Record operating system and patch level for HMIs, servers and engineering workstations.
- Note the vendor's support status: devices without security updates need extra protection in the network instead (points 11 and 14).

WHO

Automation engineer.

EFFORT

1 to 3 days on top of point 1.

COMMON MISTAKE

Recording the version once at installation and never updating it.

3 Network drawing

PRIORITY 1 | FIX FIRST

You have a current drawing of the control network that shows every connection to the office network, the internet and outside companies.

☐ YES ☐ PARTLY ☐ NO

WHY

Attackers usually reach the OT assets through a connection that nobody remembered. You need this drawing to do points 6 and 11.

GOOD LOOKS LIKE

One drawing that shows the zones (office, DMZ, control, safety), every link between them, and every way out: firewalls, VPNs, modems, 4G/5G routers, vendor links, wireless. Dated and owned by one person.

HOW TO DO IT

- Draw the zones first, then the links between them. Detail inside a zone can come later.
- Confirm each link physically: follow the cables, check the firewall and router settings, look for 4G/5G routers in cabinets.
- Mark each external link with its owner and its purpose. A link with no owner and no purpose is a candidate for removal.
- Store a printed copy offline. You will need it during an incident.

WHO

Automation engineer with IT network staff.

EFFORT

2 to 5 days.

COMMON MISTAKE

A drawing of how the network was designed, without the data flows and the owners of the external connections.

4 Critical systems

PRIORITY 2 | FIX THIS YEAR

You know which systems the process cannot run without for more than a few hours.

☐ YES ☐ PARTLY ☐ NO

WHY

Those systems get the strongest protection, the best backups, and you restore them first.

GOOD LOOKS LIKE

A short list (often 5 to 15 systems) that shows, for each one, how long the process can run without it and what happens when it stops.

HOW TO DO IT

- Hold a two-hour workshop with operations, maintenance and the plant manager. Ask: "if this system stops now, what happens in one hour, one day, one week?"
- Mark the critical systems on the asset list and on the drawing.
- Use the result to order the restore plan (point 23) and the protection work.

WHO

Plant manager and operations lead.

EFFORT

1 to 2 days including the workshop.

COMMON MISTAKE

Marking everything as critical. If everything is critical, nothing is.

5 Vendor advisories

PRIORITY 2 | FIX THIS YEAR

A named person receives the security advisories from your equipment vendors and decides what to do with each one.

☐ YES ☐ PARTLY ☐ NO

WHY

An advisory that nobody reads is a known flaw that stays open and a potential doorway for attackers.

GOOD LOOKS LIKE

A named person, a subscription to each vendor's security notices and to a public advisory feed for industrial systems. Also a short log for each advisory: does it affect us (yes/no, from the asset list), decision, date.

HOW TO DO IT

- Subscribe to the security notification service of each main vendor.
- Check each advisory against the asset list (point 2).
- Decide one of four actions: patch at the next planned outage window, add a network control instead, accept the risk with a reason, or not relevant. Record the decision.
- In OT, patching is rarely immediate. A documented decision with a compensating control is often the correct answer.

WHO

Automation engineer or the person responsible for OT security.

EFFORT

1 day to set up; then 1 to 2 hours per month.

COMMON MISTAKE

Ignoring advisories, or patching straight away without testing. Test with the vendor or on a spare system, and patch during planned maintenance.

2 Remote access

SECTION 2 OF 6 / POINTS 6 TO 10

6 7 8 9 10

6 Every way in

PRIORITY 1 | FIX FIRST

You can list every way into the control network from outside: VPNs, remote desktop tools, vendor modems and 4G/5G routers.

☐ YES ☐ PARTLY ☐ NO

WHY

A forgotten modem or remote desktop tool is one of the most common ways in.

GOOD LOOKS LIKE

A complete list of remote access paths, each with an owner, a user group, a purpose and an approval.

HOW TO DO IT

- Use the drawing (point 3) and ask every vendor and integrator how they connect today.
- Search the HMIs, servers and engineering workstations for installed remote desktop tools.
- Physically check cabinets and control rooms for modems and 4G/5G routers.
- Remove every path you cannot justify. Move the rest to the one controlled entry point (point 9).

WHO

Automation engineer with IT security.

EFFORT

2 to 5 days.

COMMON MISTAKE

Trusting the paperwork. The paths that hurt you are the ones nobody wrote down.

7 Second factor for remote access

PRIORITY 1 | FIX FIRST

Every remote connection into the control network needs a second factor, such as a code on a phone or a hardware key.

☐ YES ☐ PARTLY ☐ NO

WHY

With a second factor, a stolen password alone is not enough. Stolen or guessed passwords are behind a large share of security incidents.

GOOD LOOKS LIKE

Multi-factor authentication on every VPN and remote access account, including vendors, with no exceptions for "service" accounts.

HOW TO DO IT

- Turn it on at the entry point (VPN or remote access gateway), so it covers everyone who comes in that way.
- Give vendors their own personal accounts with a second factor. No shared vendor logins.
- Prefer an app or hardware key over SMS codes.
- Plan for the night shift: a working process if a phone is lost, so nobody switches the second factor off "temporarily".

WHO

IT security, with operations for the rollout.

EFFORT

2 to 5 days, often with existing VPN licences.

COMMON MISTAKE

One shared "vendor" account with the second factor on one person's phone.

8 Vendor access off by default

PRIORITY 1 | FIX FIRST

Vendor and integrator access is off by default. You switch it on for a specific job and switch it off when the job is done.

☐ YES ☐ PARTLY ☐ NO

WHY

Access that is always on is access that an attacker can also use at 3 a.m.

GOOD LOOKS LIKE

Vendor accounts disabled by default. A short request process: who, which system, why, for how long. Access opened by your staff and closed when the job is done or at the end of the day.

HOW TO DO IT

- Disable all vendor accounts now. Enable them on request with a valid business reason.
- Use a simple request form or ticket. The control room approves.
- Where the tools allow it, set access to expire automatically.
- For critical systems, record or monitor the activity.

WHO

Operations lead (approves), IT or automation (opens and closes).

EFFORT

1 to 2 days to set up.

COMMON MISTAKE

An emergency exception that becomes permanent.

9 One controlled entry point

PRIORITY 2 | FIX THIS YEAR

Remote sessions go through one controlled point, such as a jump server (bastion host), where they are logged. Nobody connects straight to a PLC or HMI from outside.

☐ YES ☐ PARTLY ☐ NO

WHY

One entry point is one place to watch, and with logging enabled you can see who did what.

GOOD LOOKS LIKE

A jump server or remote access gateway in the DMZ. Users connect to it, then to the target. Sessions are logged and, for vendors, ideally recorded.

HOW TO DO IT

- Place the jump server in the DMZ (point 13), not in the control network.
- Install the engineering tools that vendors need on the jump server, so they do not need to bring their own laptop.
- Allow traffic from the jump server only to the systems each user needs.
- Keep its logs where an attacker cannot easily delete them (point 28).

WHO

IT security with automation engineering.

EFFORT

5 to 15 days, plus hardware or licences.

COMMON MISTAKE

A jump server with a direct path around it that is "only for emergencies".

10 Review remote accounts every three months

PRIORITY 2 | FIX THIS YEAR

At least every three months, someone reviews the remote access accounts and removes the ones that are no longer needed.

☐ YES ☐ PARTLY ☐ NO

WHY

Old accounts of former staff and finished projects are easy targets.

GOOD LOOKS LIKE

A dated review record every quarter: list of accounts, keep or remove, and who decided.

HOW TO DO IT

- Export the account list from the VPN or gateway.
- Send it to the operations lead to confirm each account.
- Disable what nobody confirms. If someone needs it, they will ask.
- Keep the record. It is the evidence an auditor asks for.

WHO

IT security with the operations lead.

EFFORT

2 to 4 hours per quarter.

COMMON MISTAKE

Reviewing without removing anything.

3 Network separation

SECTION 3 OF 6 / POINTS 11 TO 15

11 12 13 14 15

11 Firewall between office and control

PRIORITY 1 | FIX FIRST

A firewall separates the control network from the office network, and each firewall rule has a written reason.

☐ YES ☐ PARTLY ☐ NO

WHY

If ransomware hits the office, the firewall decides whether it reaches the plant.

GOOD LOOKS LIKE

A dedicated firewall (not only a router or a VLAN) between office and control. Default rule: deny. Each allowed rule has a source, a destination, a port, a reason and an owner.

HOW TO DO IT

- If there is no firewall, this is the first purchase.
- Before you tighten the rules, watch the traffic for two to four weeks to learn what the process really needs.
- Introduce the deny rule in steps, during planned maintenance, with a rollback plan.
- Write the reason next to each rule in the firewall itself.

WHO

IT network with automation engineering.

EFFORT

5 to 15 days, plus hardware if needed.

COMMON MISTAKE

A VLAN without filtering, called "segmentation".

12 No internet, email or browsing on control systems

PRIORITY 1 | FIX FIRST

No control system can reach the internet directly, and nobody reads email or browses the web on an HMI or engineering workstation.

☐ YES ☐ PARTLY ☐ NO

WHY

Email and web browsing are how most malware arrives.

GOOD LOOKS LIKE

The firewall blocks outbound internet from the control network. HMIs and engineering workstations have no email client and no browser use. Updates arrive through a controlled path.

HOW TO DO IT

- Block outbound internet at the firewall and check the logs for what breaks. Usually it is a licence check or an update service; give those a narrow, documented path.
- Give operators and engineers a separate office PC for email and web.
- Bring updates in through the DMZ or a checked USB process (point 19).

WHO

IT network with operations.

EFFORT

2 to 5 days.

COMMON MISTAKE

"just for this one licence server" rules that open far more than needed.

13 Data leaves through a DMZ

PRIORITY 3 | BUILD OVER TIME

Data that the business needs, such as historian data and reports, leaves the control network through a separate zone (a DMZ), not through a direct connection.

☐ YES ☐ PARTLY ☐ NO

WHY

The office then never needs a direct path into the control network, so an attacker has no direct connection to abuse.

GOOD LOOKS LIKE

A DMZ between office and control. The control side pushes data to a historian copy or file server in the DMZ. The office reads from the DMZ. No direct office-to-control connection.

HOW TO DO IT

- Design this with point 11; it is often one project.
- Start with the historian: a copy in the DMZ, updated from the control side.
- Move the jump server (point 9) and update services into the DMZ.
- For very critical sites, consider a one-way data diode for the data that only needs to leave.

WHO

IT network, automation engineering, the historian owner.

EFFORT

10 to 30 days, plus hardware. Often a planned project.

COMMON MISTAKE

A DMZ that the office can still bypass.

14 Yearly firewall rule review

PRIORITY 2 | FIX THIS YEAR

Someone reviewed the firewall rules in the last 12 months and removed the rules that allow all traffic.

☐ YES ☐ PARTLY ☐ NO

WHY

Temporary rules for one job tend to stay for years.

GOOD LOOKS LIKE

A yearly review record. No "any to any" rules. Every rule has a reason and an owner, and temporary rules have an end date.

HOW TO DO IT

- Export the rules and the hit counts. Rules with no hits in 90 days are candidates for removal.
- Ask the owner of each rule whether it is still needed.
- Remove in steps, during planned maintenance, with a rollback plan.

WHO

IT network with automation engineering.

EFFORT

1 to 3 days per year.

COMMON MISTAKE

Being afraid to remove anything, so nothing changes.

15 Safety systems separate

PRIORITY 2 | FIX THIS YEAR

Safety systems (SIS) are on their own network segment, or physically separate from the control system.

☐ YES ☐ PARTLY ☐ NO

WHY

An attack on the control system must not be able to switch off the protection.

GOOD LOOKS LIKE

The SIS is in its own zone, with only the connections the safety case needs, ideally read-only from the control side. The engineering key switch on the SIS controller is in "run", not "program".

HOW TO DO IT

- Check the drawing for every link to the SIS. Remove what is not needed for safety.
- Keep the SIS controller in run mode; switch to program only under a permit.
- Agree changes with your safety engineer and follow your functional safety process (IEC 61511). Never change an SIS link without them.

WHO

Safety engineer and automation engineer.

EFFORT

2 to 10 days, depending on the design.

COMMON MISTAKE

An engineering workstation that can reach both the control system and the SIS, left logged in.

4 Accounts, passwords and devices

SECTION 4 OF 6 / POINTS 16 TO 20

16 17 18 19 20

16 Default passwords changed

PRIORITY 1 | FIX FIRST

The default passwords on PLCs, HMIs, switches and firewalls are changed.

☐ YES ☐ PARTLY ☐ NO

WHY

Default passwords are published in the vendors' own manuals.

GOOD LOOKS LIKE

No default password anywhere on the control network. New passwords are kept in a password vault or a sealed record, not on a note on the cabinet.

HOW TO DO IT

- Use the asset list (point 1) and go device by device.
- Where a device cannot change its password, protect it in the network (points 11 and 14) and record the exception.
- Change passwords during planned maintenance; some devices need a restart or a project download.
- Store the new passwords in a password vault with access for the people who need them, and a sealed copy for emergencies.

WHO

Automation engineer.

EFFORT

2 to 5 days.

COMMON MISTAKE

The same new password on every device.

17 Personal accounts

PRIORITY 2 | FIX THIS YEAR

Every person has their own account. Shared accounts are used only where the system allows nothing else, and their passwords change when someone leaves.

☐ YES ☐ PARTLY ☐ NO

WHY

With personal accounts you know who made a change, and you can remove one person's access.

GOOD LOOKS LIKE

Personal accounts on engineering workstations, servers, jump server and VPN. Shared operator logins on HMIs are acceptable where the HMI needs them, with a list of who knows the password.

HOW TO DO IT

- Start where it is easiest: VPN, jump server, servers, engineering workstations.
- For HMIs, keep the shared operator login if a personal login would slow down the operators; protect the engineering functions behind personal accounts.
- Keep a list of every shared account and who knows its password.

WHO

IT with automation engineering.

EFFORT

3 to 10 days.

COMMON MISTAKE

Making the operators' work harder. Security that slows the control room is switched off within a month.

18 Few administrators

PRIORITY 3 | BUILD OVER TIME

Only the people who need it have administrator rights on engineering workstations and servers.

☐ YES ☐ PARTLY ☐ NO

WHY

Fewer administrators means fewer accounts that an attacker can use to change the process.

GOOD LOOKS LIKE

A short list of administrators, reviewed with point 10. Day-to-day work under a normal account.

HOW TO DO IT

- List who has administrator rights now.
- Remove rights from day-to-day accounts. Give the people who need them a separate administrator account.
- Test that the engineering software runs without administrator rights before you remove them; some older tools need exceptions.

WHO

IT with automation engineering.

EFFORT

1 to 3 days.

COMMON MISTAKE

Removing rights without testing the engineering tools.

19 USB sticks and visiting laptops checked

PRIORITY 2 | FIX THIS YEAR

USB sticks and laptops brought onto site are checked before they connect to a control system, for example at a scanning station.

☐ YES ☐ PARTLY ☐ NO

WHY

Networks that are separated from the internet are still infected through USB sticks and visiting laptops.

GOOD LOOKS LIKE

A scanning station at the entrance to the control room. A rule that every USB stick is scanned before use. Vendor laptops either scanned or not connected; vendors work through the jump server instead.

HOW TO DO IT

- Set up a scanning station (a dedicated PC with up-to-date malware scanning, ideally with more than one scan engine).
- Give staff company USB sticks that stay on site.
- Block USB storage on HMIs and engineering workstations where the process allows it.
- Brief vendors before their visit. The rule is easier to keep when they expect it.

WHO

Operations lead with IT security.

EFFORT

2 to 5 days.

COMMON MISTAKE

A scanning station that nobody uses because it is in the wrong place.

20 Leavers lose access on their last day

PRIORITY 1 | FIX FIRST

Staff and contractors who leave lose all access, including remote access, on their last working day.

☐ YES ☐ PARTLY ☐ NO

WHY

The access of people who left is rarely watched by anyone.

GOOD LOOKS LIKE

A leaver checklist that includes control system accounts, VPN, jump server, shared passwords they knew, and physical keys or cards.

HOW TO DO IT

- Add the control system accounts to the HR leaver process.
- Change the shared passwords that the leaver knew (point 17).
- For contractors, the project manager confirms the end date, and accounts expire on that date.

WHO

HR, IT and the operations lead.

EFFORT

1 day to set up.

COMMON MISTAKE

The HR process covers office IT only, not the plant.

5 Backups and recovery

SECTION 5 OF 6 / POINTS 21 TO 25

21 22 23 24 25

21 Backups of what the business needs

PRIORITY 1 | FIX FIRST

You have current backups of PLC programs, HMI projects, switch and firewall settings, and engineering workstation images.

☐ YES ☐ PARTLY ☐ NO

WHY

Without the PLC programs and HMI projects, a rebuild takes weeks instead of days.

GOOD LOOKS LIKE

A backup for every critical system (point 4), taken after every change and at least every quarter, with the date, the version and the person who made it.

HOW TO DO IT

- Start with the critical systems.
- Take the PLC program from the running controller, not from the integrator's laptop; they are often different.
- Back up network device settings and firewall rules too.
- Make "take a backup" the last step of every change.

WHO

Automation engineer.

EFFORT

3 to 10 days for the first full set.

COMMON MISTAKE

The only copy of the PLC program is on the integrator's laptop.

22 One copy offline

PRIORITY 1 | FIX FIRST

At least one copy of these backups is kept offline or off the control network.

☐ YES ☐ PARTLY ☐ NO

WHY

Ransomware encrypts every backup that it can reach.

GOOD LOOKS LIKE

Three copies, on two kinds of media, one offline or offsite. The offline copy is updated after each change and at least every quarter.

HOW TO DO IT

- Copy the backups to an external disk or protected storage that is disconnected after each update.
- Keep one copy at another site, or in a fire safe.
- Protect the offline copy with encryption and record who has the key.

WHO

Automation engineer with IT.

EFFORT

1 to 2 days to set up.

COMMON MISTAKE

A backup disk that stays connected "for convenience".

23 Tested restore

PRIORITY 1 | FIX FIRST

In the last 12 months, someone restored a system from a backup and saw it work. ☐ YES ☐ PARTLY ☐ NO

WHY

A backup is only proven when a restore from it has worked.

GOOD LOOKS LIKE

A yearly restore test for each critical system, with a short record: what was restored, how long it took, and what was missing.

HOW TO DO IT

- Restore to a spare controller or a test PC, not to the live system.
- Time the restore. The time tells you whether point 25 is realistic.
- Write down everything that was missing (licences, drivers, passwords) and fix it.
- Start with one critical system; add one per quarter.

WHO

Automation engineer.

EFFORT

1 to 2 days per system.

COMMON MISTAKE

Checking that the backup file exists, not that it restores.

24 Rebuild kit available offline

PRIORITY 2 | FIX THIS YEAR

The installation media, licences and project files to rebuild an engineering workstation are stored where you can find them without the network. ☐ YES ☐ PARTLY ☐ NO

WHY

During an incident, the network and the file server may be the first things you lose.

GOOD LOOKS LIKE

A "rebuild kit" per critical system: installation media, licence keys or dongles, project files, a short rebuild instruction, all kept offline.

HOW TO DO IT

- Build the kit during the first restore test (point 23); the test shows what you need.
- Ask vendors how licences are restored without internet access.
- Keep one kit on site and one at another location.

WHO

Automation engineer.

EFFORT

1 to 3 days.

COMMON MISTAKE

A licence that can only be activated online.

25 Manual operation practised

PRIORITY 3 | BUILD OVER TIME

You know how long you can run the process by hand or keep it in a safe state, and the operators have practised it. ☐ YES ☐ PARTLY ☐ NO

WHY

This time is what you have to restore the control systems.

GOOD LOOKS LIKE

A written procedure for manual or reduced operation, and for a safe stop. Operators practise it once a year. The time it holds is known and compared to the restore times from point 23.

HOW TO DO IT

- Write the procedure with the most experienced operators.
- Practise during a planned period of low demand.
- Compare: if manual operation lasts 8 hours and the restore takes 3 days, you need a better plan.

WHO

Operations lead and plant manager.

EFFORT

2 to 5 days plus the exercise.

COMMON MISTAKE

Assuming the old manual skills are still there.

6 Incident readiness

SECTION 6 OF 6 / POINTS 26 TO 30

26 27 28 29 30

26 Operators know the signs and who to call

PRIORITY 2 | FIX THIS YEAR

Operators know what looks wrong, such as an HMI that moves by itself, unknown logins or changed set points, and who to call at any hour.

☐ YES ☐ PARTLY ☐ NO

WHY

The operator on shift is usually the first person to see an attack.

GOOD LOOKS LIKE

A one-page card in the control room: the signs, the first three actions, and the phone numbers. A short briefing for every shift once a year.

HOW TO DO IT

- Write the card with the operators, in their words.
- First actions: do not switch anything off unless safety requires it, write down what you see and when, call the number.
- Brief every shift once a year, together with the safety briefing. Fifteen minutes is enough.

WHO

Operations lead.

EFFORT

1 to 2 days.

COMMON MISTAKE

A cyber procedure that only IT understands.

27 Short incident plan, numbers on paper

PRIORITY 2 | FIX THIS YEAR

There is a short written incident plan for the control environment, with the phone numbers also on paper.

☐ YES ☐ PARTLY ☐ NO

WHY

In an incident, the systems that hold the plan and the numbers may be down.

GOOD LOOKS LIKE

A plan of a few pages: who decides, who to call (internal, vendors, authority, insurer), when to isolate the control network from the office, how to keep the process safe. Printed, in the control room.

HOW TO DO IT

- Keep it short. A plan nobody reads does not help.
- Agree in advance who may decide to disconnect the plant from the office network, so nobody waits for permission.
- Include your main vendors' emergency numbers and your insurer.
- Review it after every exercise (point 30).

WHO

OT security owner with operations and management.

EFFORT

3 to 5 days.

COMMON MISTAKE

A copy of the IT incident plan with "OT" added.

28 Logs kept for 90 days

PRIORITY 3 | BUILD OVER TIME

Logs from firewalls, remote access and key servers are kept for at least 90 days, where an attacker cannot easily delete them.

☐ YES ☐ PARTLY ☐ NO

WHY

Attackers are often inside for weeks before anyone notices, and the logs show how they came in.

GOOD LOOKS LIKE

Logs from the firewalls, VPN, jump server and Windows servers sent to one central log store, kept 90 days or more, with someone looking at the important alerts.

HOW TO DO IT

- Start with the logs that matter most: firewall, VPN, jump server.
- Send them to a central store outside the control network.
- Check the clocks: all systems on the same time, or the logs cannot be compared.
- Later, consider an OT network monitoring tool. Do it after P1 and P2, not before.

WHO

IT security.

EFFORT

3 to 10 days.

COMMON MISTAKE

Buying a monitoring tool before the basics are in place, and nobody looks at its alerts.

29 Who reports, and the 24-hour early warning

PRIORITY 2 | FIX THIS YEAR

You know who reports a serious incident to the authority, and that NIS2 asks for an early warning within 24 hours.

☐ YES ☐ PARTLY ☐ NO

WHY

24 hours passes quickly when you are busy saving the operations.

GOOD LOOKS LIKE

A named person and a deputy. The contact details of your national CSIRT or competent authority in the incident plan. A short template ready. Under NIS2: an early warning within 24 hours, an incident notification within 72 hours, and a final report within one month.

HOW TO DO IT

- Find out which authority applies to your sector, and how it accepts reports.
- Prepare a template for the early warning; it can be short.
- Agree in advance who may send it, so it does not wait for the board.
- Practise it in the exercise (point 30).

WHO

OT security owner, management, legal.

EFFORT

1 to 2 days.

COMMON MISTAKE

Thinking the 24 hours start after the investigation. They start when you become aware of a significant incident.

30 Yearly exercise

PRIORITY 3 | BUILD OVER TIME

In the last 12 months, operations and management ran an exercise on a cyber incident at the plant, even if only a two-hour discussion at a table.

☐ YES ☐ PARTLY ☐ NO

WHY

An exercise shows the gaps in the plan before a real incident does.

GOOD LOOKS LIKE

A yearly tabletop exercise with operations, IT, management and, if possible, a key vendor. A short list of lessons, with owners and dates.

HOW TO DO IT

- Use a realistic scenario: ransomware in the office spreading toward operations, or a vendor account used at night.
- Two to three hours is enough. Have someone outside the team run it.
- Include the decision to isolate, the safe state, and the 24-hour report.
- Write down the lessons, give each an owner and a date, and check them at the next exercise.

WHO

OT security owner with management.

EFFORT

2 to 3 days to prepare, plus the exercise.

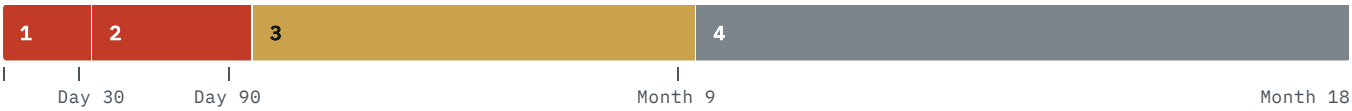
COMMON MISTAKE

A scenario so easy that nobody learns anything.

THE PLAN

A realistic order

From the first 30 days to month 18. The first two phases are short on purpose: they close the direct ways in and prove that you can recover.



1 DAYS 1 TO 30 — See and close the doors

PRIORITY 1

- 3 Network drawing
- 8 Vendor access off by default
- 16 Default passwords (start with critical systems)
- 6 Every way in
- 20 Leavers process

2 DAYS 30 TO 90 — Lock the doors and secure the way back

PRIORITY 1

- 7 Second factor
- 12 No internet on control systems
- 22 Offline copy
- 11 Firewall office/control
- 21 Backups
- 23 First restore test

3 MONTHS 3 TO 9 — Make it last and make it provable

PRIORITY 2

- 1 Asset list
- 5 Advisories
- 14 Firewall review
- 19 USB process
- 27 Incident plan
- 2 Versions
- 9 Jump server
- 15 Safety separation
- 24 Rebuild kit
- 29 Reporting
- 4 Critical systems
- 10 Account reviews
- 17 Personal accounts
- 26 Operator card

4 MONTHS 9 TO 18 — Build maturity

PRIORITY 3

- 13 DMZ
- 25 Manual operation practised
- 30 Yearly exercise
- 18 Few administrators
- 28 Central logs

Note. Points 1 and 3 support each other. A rough drawing first (Priority 1) lets you close the doors quickly; the full asset list (Priority 2) then makes everything else easier to keep.

AFTER THE HOUR

Your result

	Yes answers		Priority 1 Yes answers
	of 30		of 11

0 to 12

Exposed

Some direct ways in are probably open, and recovery is not proven. Start the Priority 1 points this month.

13 to 22

Basics in place

The main doors are closed. Work through Priority 2 so the basics last and you can show the evidence.

23 to 30

Well prepared

Keep the reviews and the exercise running, and have someone from outside test what you believe.

> **One rule above the score.** A No on any Priority 1 point comes first, whatever your total.

Your three first actions

Start with the Priority 1 points you answered No.

1 _____

2 _____

3 _____

Next steps

The NIS2 readiness check

Free, about five minutes. It covers the management side, such as board approval, risk assessment, suppliers and reporting, and emails you a personal report.

kimk-t.com/nis2-readiness

A 30-minute call

Go through your answers with Ivan Dragnev. No sales deck.

kimk-t.com/book

KIMK

OFFICE@KIMK-T.COM / KIMK-T.COM