01 / MANAGEMENT SUMMARY

Executive evidence pack

Demonstration packaging cell

A worked example of observation, review and accountable action. All assets, evidence extracts and actions are synthetic, authored for this website sample. This is not a customer report or a live platform export.

DECISION REQUIRED

Confirm ownership and approval of the illustrated maintenance path before the next maintenance window.

Demo engineering lead to obtain the access register and approval record. Current state: review required; no approval recorded.

Scope and confidence

Scope item	Review basis / limitation
Demonstration scope	One packaging cell and its illustrated maintenance access path.
Illustrative inventory	20 fictional assets across five protocol groups. Not measured plant coverage.
Worked record	PLC-DEMO-01; Modbus TCP. Only the displayed synthetic extract is supplied.
Coverage boundary	Example switch mirror feed only. Other segments and intermittent traffic are not represented.
Freshness / authority	No live collection date. Plant owner and authorised engineering reviewer must decide any real action.

Three questions for handover

Order*	Review question	Owner role
1	Is the maintenance path approved for the intended scope?	Engineering lead
2	Does confirmed device / firmware information match any vulnerability lead?	Asset owner
3	Which communications fall outside the collection scope?	OT support

*Suggested discussion order, not a risk rating. Actions A-01 to A-03 appear on page 3.

Preparation support only: no compliance certification, security-level determination, safety assurance or production authorisation. OTCogniShield remains in pre-launch validation.

02 / WORKED ENGINEERING EXAMPLE

From observation to decision

Finding F-01 / Maintenance access approval

The following excerpts demonstrate evidence structure. They were written for this document; the referenced inventory, diagram and capture files are not attached.

Evidence ID / type	Included synthetic extract
E-01 / inventory	PLC-DEMO-01 | 192.0.2.20 | PLC | Modbus TCP Identity and firmware: not verified.
E-02 / flow observation	192.0.2.10 -> 192.0.2.20 | TCP/502 Maintenance workstation -> PLC; request type not established.
E-03 / scope note	Illustrated switch mirror feed for the packaging cell. No visibility asserted for other segments.
E-04 / review record	Access owner approval: not supplied in this synthetic example.

Human review and next action

Review step	Recorded interpretation
Observed / represented	E-02 illustrates a communication path. It does not establish approved access or a malicious session.
Uncertainty	Owner, permitted destination, maintenance window and session controls remain unconfirmed. Protocol alone does not establish read-only behaviour.
Potential consequence	Unapproved maintenance access could affect production. No plant-specific likelihood, consequence or risk score has been established.
Action A-01	Engineering lead to confirm access ownership, permitted scope and approval before the next maintenance window.
Closure evidence	Reference the reviewed access register and approval decision; retain reviewer, date and any conditions.
Approval state	Pending in this fictional example. No live approval, isolation or configuration change has occurred.

Sense: record scope and observation. **Analyse:** test assumptions and operational context. **Advise:** propose an owned action for authorised review.

All real actions remain subject to OT change control. This sample does not execute PLC writes, network isolation or a deterministic plant safe state.

03 / ACTIONS AND REVIEW RECORD

Make the handover accountable

Draft action register

ID / owner role	Action / closure evidence	Target / status
A-01 Engineering lead	Confirm maintenance access approval (F-01). Close with access register and recorded approval decision.	Before next window Pending
A-02 Asset owner	Confirm device / firmware before evaluating a vulnerability lead. Close with identity source and applicability review.	Agree at review Pending
A-03 OT support	Confirm collection scope and blind spots. Close with reviewed scope diagram and coverage limitations.	Agree at review Pending

SANS ICS themes / evidence prompts

Original review prompts informed by the SANS Five ICS Cybersecurity Critical Controls. These are preparation themes, not a scored assessment or SANS endorsement.

Review area	Evidence to prepare
ICS Incident Response Plan	Contacts, exercised response plan and approved recovery procedures.
Defensible Architecture	Reviewed zone diagram, permitted flows and exception decisions.
ICS Network Visibility & Monitoring	Collection scope, asset context, observations and blind spots.
Secure Remote Access	Approved users, entry points, destinations and session-control records.
Risk-Based Vulnerability Management	Confirmed applicability, exposure, impact and treatment decision.

Review and approval checklist

[ ] Scope and evidence limitations checked. [ ] Facts separated from assumptions.
[ ] Owners and target dates agreed. [ ] Supporting references retained.

Review field	Completion state in this sample
Reviewer / review date	Not assigned / not recorded.
Owner decision / next review	Pending / to be agreed by responsible owner.

Version: v1.2 | 25 October 2026. Added worked evidence chain, decision box and action register. All content remains synthetic.

Source: SANS Institute, Robert M. Lee and Tim Conway (2022), The Five ICS Cybersecurity Critical Controls. Source publication. Framework applicability and technical effectiveness require separate review.