IEC 62443

Implementation Plan

A practical, stage-by-stage guide for asset owners — aligned to the ISASecure ACSSA conformity assessment framework

---

Prepared by DeNexus

OT Cyber Risk Quantification & Underwriting Intelligence

Why This Plan Exists

IEC 62443 is the only internationally recognized cybersecurity standard built specifically for Industrial Automation and Control Systems (IACS). It is widely referenced, broadly endorsed, and — outside a small number of sector- and country-specific mandates — completely voluntary. That voluntary status is part of why so many asset owners struggle to start: there is no regulator pushing a deadline, no enforcement authority asking for evidence, and no obvious place to begin inside a standard that runs to dozens of parts across six document groups.

This document exists to fix that. It is a practical, stage-by-stage roadmap for an asset owner implementing IEC 62443 across an operational facility or a fleet of facilities. It maps the journey from initial scoping through ongoing operations, and ends at preparation for the ISASecure Automation and Control System Security Assurance (ACSSA) conformity assessment — the only formal third-party certification program currently available for asset owner IACS security posture.

It is written for the OT cybersecurity professional who has to actually build the program: define the work, secure the budget, sequence the activities, deliver the work products, and demonstrate progress to leadership and external stakeholders. Where the standard tells you what to do, this plan tells you how to organize the doing.

How This Plan Is Organized

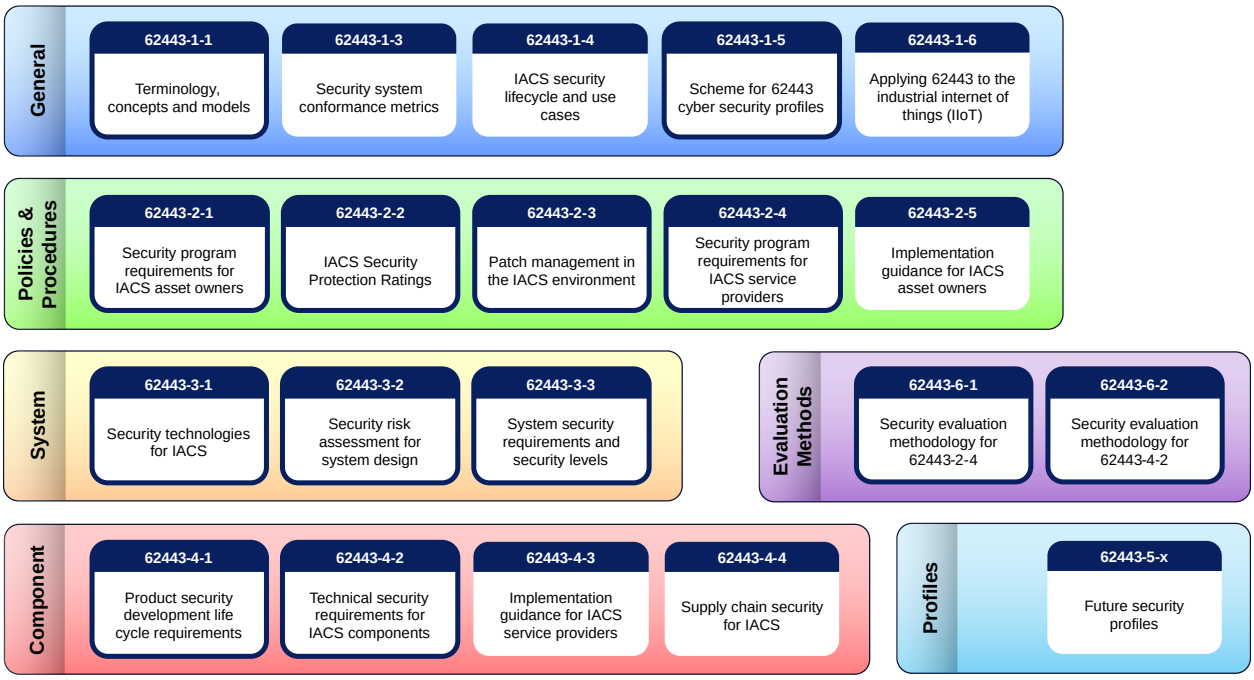
Implementation is organized into seven project stages. Each stage maps to specific parts of the IEC 62443 series and produces work products that build toward the next stage.

Stage	Focus	What It Maps To
Stage 0	Scope & Prepare	Defines what's in, what's out, and who owns it
Stage 1	Establish the Security Program	Parts 2-1 and 2-3 — governance and the cybersecurity program
Stage 2	Third-party Service Providers	Part 2-4 — supply chain and contractor security
Stage 3	Assess Risk & Design Zones/Conduits	Part 3-2 — the engineering risk assessment
Stage 4	Implement Technical Controls	Part 3-3 — security level capabilities
Stage 5	Operate & Maintain	Run the program; sustain control effectiveness
Stage 6	Prepare for ACSSA Conformity Assessment	Get evidence-ready for third-party validation (*if you claim adoption of 62443, why not validate it is correct?*)

Stages are sequenced, but in practice they overlap. Establishing the security program (Stage 1) takes months and continues into Stage 2 and 3 work. Implementing controls (Stage 4) ramps up during Stage 3 risk assessment as soon as the highest-priority zones are identified. The sequence is a planning structure, not a strict gate.

A Note on Voluntary Adoption

IEC 62443 is not mandatory anywhere in the world as a standalone legal requirement. Several regulatory regimes (e.g., NIS2 in the EU and its national transpositions, NIST CSF in the US, the NCSC Cyber Assessment Framework in the UK, and sector-specific frameworks such as NERC CIP) reference 62443 as a recognized methodology, an informative reference, or a benchmark of good practice. None of them substitute compliance with 62443 for compliance with the regulation itself. Asset owners must still meet their direct regulatory obligations; 62443 provides the engineering methodology that makes meeting them manageable, structured, and defensible.



The practical implication: don't implement 62443 to satisfy a regulator. Implement it because it gives you a structured, repeatable, internationally recognized way to reduce real risk in your environment — and then demonstrate to your infrastructure funds investor, parent company, executives, regulator, or insurer that your 62443-aligned program meets their specific obligations.

STAGE 0 Scope & Prepare

Purpose

Stage 0 is the work that happens before a security program exists. The output is clarity: which systems are in scope, which 62443 roles your organization occupies, who is accountable for the program, and what executive sponsorship looks like. Skipping Stage 0 is the most common reason 62443 implementations stall — teams begin work without agreement on what the work covers and getting leadership support.

Key Activities

Identify the Facilities / Locations in Scope

Few ICS/OT owners/operators have a single location, they have several. The first step is confirming if 62443 adoption will be applied to all sites right away, or if it will be introduced at a single site first (like a proof of concept / proof of value) before rolling out across the organization.

Define the System Under Consideration (SuC)

Within a facility are the various ICS/OT control & automation systems. If you aggregated them altogether, this is the scope where 62443 program is applied. This scope of systems, is the ‘system under consideration’ (SuC).

The SuC is the set of IACS assets, networks, communications, and supporting infrastructure that the 62443 program will cover. Part 3-2 will partition the SuC into zones and conduits later, but Stage 0 sets the outer boundary. The SuC definition typically starts at a single facility or production line and expands as the program matures.

For each candidate SuC, document:

- Physical scope — sites, buildings, production lines
- Logical scope — control systems, safety systems, supporting networks, engineering workstations, historians, MES integrations
- Ingress and egress points — every external network connection, vendor remote access path, and removable media route
- Equipment Under Control (EUC) — the physical process the IACS operates
- Service providers in scope — integrators, maintenance contractors, vendor support staff who interact with the SuC

62443 Roles: This Plan is for Asset Owners

Most industrial operators are Asset Owners. Some organizations also act as Integration Service Providers (when they self-integrate) or Maintenance Service Providers (when they have internal maintenance organizations that serve other parts of the business). Role assignment matters because the applicable parts of the standard differ by role. **This implementation plan focuses on the Asset Owner role**; if your organization plays multiple roles, you will need parallel programs aligned to Parts 2-4, 3-3, 4-1, or 4-2 as applicable.

Assign Program Accountability

Part 2-1 will formalize roles and responsibilities, but Stage 0 needs an executive sponsor and a program owner before any program-defining work begins. The program owner is typically the head of OT cybersecurity, a CISO with OT scope, VP of facility production operations, or a designated IACS security manager. The executive sponsor is typically the COO, the head of operations, or in some organizations the CFO — the latter often most effective because budget authority and risk ownership sit there.

Establish the Business Case

The 62443 program will consume real budget over multiple years. Stage 0 produces the initial business case — the answer to "why are we doing this, and why now?" The case typically blends regulatory pressure, insurance requirements, parent company requirements, customer mandates, board-level cyber risk concern, and known incidents in your sector.

The IEC 62443 standard itself doesn't prescribe a financial methodology for prioritization, which is a gap most asset owners eventually fill by adding quantified risk analysis on top of the standard's process — more on that in the closing section of this plan.

Work Products

- Documented System Under Consideration (boundary, asset list, network topology)
- Role determination memo (Asset Owner, and any additional 62443 roles)
- Executive sponsorship confirmation and named program owner
- Initial business case and multi-year budget estimate
- Project charter for the 62443 program

Stage 0 typically takes

1 to 3 months for a single facility, longer for multi-site or fleet-wide programs. The pace is set by executive alignment, not technical complexity.

STAGE 1 Establish the Security Program

Primary references: IEC 62443-2-1:2024 (Security program requirements for IACS asset owners) and IEC TR 62443-2-3 (Patch management in the IACS environment)

Purpose

Part 2-1 is the foundational standard for asset owners. It defines what a Security Program (SP) for an IACS must contain — policies, procedures, governance structures, personnel responsibilities, and the supporting capabilities that make security an organizational discipline rather than a project. The 2024 edition substantially modernized the standard from the 2010 original, recognizing legacy systems, compensating measures, and the practical reality that IACS lifespans exceed twenty years. It also better aligns with the 27000 framework, making it easier to add 62443 to an existing 27000 program.

Stage 1 also covers Part 2-3 — patch management for the IACS environment. Patch management is established alongside the broader security program because Part 2-1 requires patch management as a capability, but Part 2-3 provides the operational detail that Part 2-1 doesn't include. The two are designed to be implemented together.

Key Activities

Build the Security Program Structure (Part 2-1)

Part 2-1:2024 organizes the Security Program around required capabilities. At minimum, the SP must define and operationalize:

- Security governance — who owns the program, how decisions are escalated, how policies are approved and reviewed
- Roles and responsibilities — what each role (operations, IT, OT cyber, engineering, executive) is accountable for and how they interact
- Risk management — how cyber risk is identified, evaluated, prioritized, and tracked over time
- Asset management — the inventory of IACS assets, kept current under change control
- Personnel security — clearance, training, awareness, and lifecycle (joiners, movers, leavers)
- Physical security — protection of IACS hardware, control rooms, and field equipment
- Network and system security policies — segmentation, remote access, removable media, wireless
- Identity and access management — accounts, privileges, authentication standards

- Incident response and recovery — detection, escalation, containment, recovery, post-incident review
- Business continuity and disaster recovery — operational continuity under cyber-induced disruption
- Compliance and audit — internal audit of the SP itself, plus mapping to external obligations

Define Risk Management Methodology

Part 2-1 requires the asset owner to define how cyber risk will be managed. It does not prescribe a specific methodology — that decision is left to the organization, which must select one consistent with its overall enterprise risk approach. Part 3-2 will later require a specific risk assessment for system design (covered in Stage 3), but Part 2-1 is broader: it covers ongoing operational risk management for the entire program.

Most asset owners adopt a qualitative or semi-quantitative risk matrix at this stage, because that is what the standard's examples illustrate and what most organizational risk frameworks already use. The standard does not yet recognize financial quantification of cyber risk as a methodology, even though many mature organizations are beginning to layer financial models on top of their qualitative process.

DeNexus provides Cyber Risk Quantification (CRQ) for ICS/OT environments. We return to this point in the closing section.

Establish Patch Management (Part 2-3)

Patching IACS systems is operationally distinct from patching IT systems. Production environments cannot accept reboots on demand. Some legacy assets cannot be patched at all because the vendor no longer exists. Field equipment may sit in environments where physical access is dangerous or expensive. Part 2-3 acknowledges all of this and provides a framework that an IT-style patch policy will not provide.

The patch management program defined in Stage 1 needs to cover:

- Patch source identification — which vendors, which advisories, which channels
- Patch impact assessment — risk of applying the patch versus risk of not applying it, with explicit acceptance of "defer" as a valid outcome
- Test environments — where patches are validated before they touch production
- Deployment windows — planned outages, staged rollout, contingency rollback procedures
- Compensating measures — for assets that cannot be patched (network isolation, additional monitoring, access restriction)
- Documentation and audit trail — every patch decision and its rationale recorded

A pragmatic patch reality

Most industrial facilities will not be able to patch every system on a routine cadence. The Part 2-3 program is what allows you to defend that — to demonstrate that patching decisions are deliberate, risk-informed, and supported by compensating controls — rather than appearing as gaps in an audit.

Document Policies and Procedures

The Security Program is only as real as the documentation that supports it. Every capability above produces at least one policy document and typically several procedural documents. Templates can accelerate this — ISA, ISAGCA, and several large industrial operators have published reference templates — but every template needs adaptation to your specific environment, asset inventory, and operational reality.

Operationalize Personnel Security and Awareness

Training is a continuous program element, not a one-time event. Part 2-1 requires that personnel with IACS responsibilities receive role-appropriate training, that contractor personnel meet the same standards, and that awareness is refreshed regularly. ISA itself offers the IC32/IC33/IC34/IC37 training tracks aligned to 62443 roles; many asset owners also build internal awareness curricula tailored to their specific equipment and processes.

Work Products

- Documented Security Program (SP) covering all required capabilities
- Risk management policy and procedure
- Patch management program (Part 2-3 aligned)
- Asset inventory with change control process
- Personnel security and training program
- Incident response plan with OT-specific procedures
- Internal audit plan for the SP itself

Stage 1 typically takes

6 to 12 months for first establishment. Sustaining the SP is then an ongoing operational discipline — see Stage 5.

STAGE 2 Govern Service Providers

Primary reference: ISA/IEC 62443-2-4 (Security program requirements for IACS service providers)

Purpose

Most asset owners depend on third parties to design, integrate, configure, commission, and maintain their IACS — vendor field engineers, system integrators, specialized maintenance contractors, and OEM remote support. Those service providers have privileged access to your environment, and their security practices directly affect your security posture. Part 2-4 specifies what the service provider's security program must contain. Stage 2 is where the asset owner makes Part 2-4 a real procurement and operational requirement.

Supply chain security failures are a documented and significant source of OT cyber incidents. Stage 2 is the asset owner's mechanism for addressing that risk before incidents happen — through contracts, assessments, ongoing monitoring, and clearly assigned accountability.

Key Activities

Inventory Service Providers

Every party with logical or physical access to the IACS environment is a service provider for Part 2-4 purposes — whether their relationship is a single field visit per year or a permanent on-site presence. Build the inventory with:

- Service provider organization name and primary contact
- Type of service provided — integration, maintenance, remote support, specialty engineering
- Access required — physical, logical, remote, persistent or session-based
- Systems and zones touched
- Contract status and renewal date

Assess Service Providers Against Part 2-4

Part 2-4 defines security program requirements that service providers must meet across categories including personnel security, training, secure development practices for any custom code or configurations, account management, configuration management, malware protection, vulnerability handling, and incident response. The asset owner needs to assess each service provider against these requirements proportionate to the access they hold.

For high-access service providers (those with persistent remote access, privileged accounts, or safety-system reach), expect to conduct formal assessment with documentation, interviews, and

evidence review. For lower-access providers (occasional on-site visits with supervised access), questionnaire-based assessment may be sufficient. Some service providers will hold ISASecure 2-4 certification for specific services; that certification provides partial evidence and reduces the asset owner's assessment burden for those services.

Build Part 2-4 Requirements Into Procurement

New service provider contracts and renewals must include Part 2-4-aligned requirements in the contract language and procurement specifications. Typical contract additions include:

- Required security program elements the provider must maintain
- Personnel training and background check requirements
- Account management — provisioning, deprovisioning, separation of duties.
- Human resources – notifying asset owner when personnel having privileged ICS/OT access depart the third-party organization, as it may trigger password changes.
- Asset owner right to audit
- Incident notification timelines and escalation paths
- Subcontractor flow-down — same requirements apply to the provider's subcontractors
- Evidence requirements — what documentation the provider must produce on request

Operationalize Ongoing Oversight

Service provider security is not a one-time procurement exercise. Stage 2 also defines the ongoing oversight mechanism: how often providers are re-assessed, how access reviews are conducted, how off-boarding works when a contract ends, and how incidents involving providers are escalated and tracked.

Work Products

- Service provider inventory with access and scope mapping
- Part 2-4 assessment for each service provider, proportionate to access
- Updated procurement standards including Part 2-4 requirements
- Contract amendments for in-flight relationships
- Service provider oversight program — assessment cadence, access reviews, incident escalation

Stage 2 typically takes

3 to 6 months to complete initial assessment and procurement updates. Ongoing oversight then runs continuously through Stage 5.

STAGE 3 Assess Risk & Design Zones / Conduits

Primary reference: ISA/IEC 62443-3-2 (Security risk assessment for system design)

Purpose

Part 3-2 is the engineering risk assessment for the actual control system and its architecture in a facility. Where Part 2-1 sets the organizational risk management approach, Part 3-2 is the specific methodology for partitioning the IACS into security zones and conduits, assessing the cybersecurity risk to each, and assigning Target Security Levels (SL-T) that drive the control selection in Stage 4.

The output of Stage 3 is the Cybersecurity Requirements Specification (CRS) — the single authoritative document that drives all subsequent design and procurement decisions. Most asset owners describe the CRS as the most important artifact produced during the entire 62443 implementation.

The Part 3-2 Process: Zone, Conduit, Risk

Part 3-2 organizes the risk assessment into a series of Zone, Conduit, and Risk requirements, abbreviated ZCR. The process flows as follows:

ZCR 1 — Identify the System Under Consideration

Begin from the Stage 0 scope definition, but at higher fidelity. ZCR 1 requires a current and accurate inventory of every asset in scope, a network architecture diagram showing how those assets communicate, an enumeration of every external connection, and identification of all supporting services (engineering workstations, historians, MES, ERP integrations). Stage 3 cannot proceed without an accurate SuC inventory — gaps here propagate into every subsequent decision.

This inventory, including vulnerabilities and network architecture, can be used as telemetry inputs to DeNexus DeRISK CRQ platform. This telemetry provides more accurate modelling of the vulnerabilities that could be used in a cyber-attack, and produces better financial impact values.

ZCR 2 — Perform Initial Cybersecurity Risk Assessment

An initial high-level assessment of the SuC as a whole, against the consequence categories the organization cares about: safety, environmental release, production loss, equipment damage, regulatory consequence, reputational consequence. The initial assessment produces a first read on whether the risk exceeds tolerable thresholds.

ZCR 3 — Partition the SuC Into Zones and Conduits

A zone is a grouping of logical or physical assets sharing common security requirements. A conduit is a logical grouping of communications that connects zones. Partitioning is the central design exercise of Part 3-2.

Typical zone partitioning criteria include:

- Criticality of the function the assets perform (safety, control, supervisory, business)
- Required security level — assets needing higher security grouped together
- Operational function — segregating control from environmental monitoring from safety
- Physical or logical location
- Responsible organization — assets maintained by different teams or providers

Part 3-2 explicitly recommends partitioning business assets from control assets, safety assets from control assets, temporarily connected devices into their own zones, and wireless assets into their own zones. Each zone gets a documented description, asset list, and identified conduits to and from other zones.

Where zones and network architecture get confused is when the impact of one system is high (e.g., safety) and the other is low (e.g., environmental monitoring) but share the same network. If their security requirements are different, they should be in isolated zones. Period. Cyber assets that share the same trust level and security requirements could be together, but the designer may choose to separate them (e.g., control room 1 and 2) because they don't need to communicate or to reduce lateral movement & cyber attack impact.

ZCR 4 — Determine If Initial Risk Exceeds Tolerable Risk

If the initial assessment from ZCR 2 already shows risk within tolerance for every zone, the process can move forward with a documented basis. If any zone exceeds tolerable risk, a more detailed assessment is required for that zone (ZCR 5).

This process can be supplemented with cyber risk quantification to express risk in dollar values. Following the 62443-3-2 process, risk is shown as the product of a risk matrix. It is a color-code, severity label, or numeric 0-5 value. These simple ranks don't get budgets approved, financial risk does. Augment the risk assessment with a CRQ baseline and the financial 'return on mitigation' if the project is implemented.

ZCR 5 — Perform Detailed Cybersecurity Risk Assessment

For each zone where initial risk exceeded tolerance, conduct a detailed assessment. Part 3-2 supports several methodologies; the most common in practice is a threat-vulnerability-consequence analysis using a likelihood-impact risk matrix, often calibrated against the organization's enterprise risk matrix. The output is a residual cybersecurity risk score for each zone and a Target Security Level (SL-T) — a Part 3-3 concept that describes the strength of controls required for the zone.

Part 3-2's risk matrix methodology has known limitations. It produces qualitative or semi-quantitative outputs that are difficult to translate into financial terms or to compare across zones with very different consequence profiles. Many asset owners now supplement Part 3-2 with quantified risk modeling that expresses zone-level risk in dollar terms — Annual Expected Loss, Value at Risk — to support prioritization and budget allocation decisions that the standard's matrix approach doesn't directly enable. This is discussed further in the closing section.

ZCR 6 — Document the Cybersecurity Requirements Specification

The CRS is the primary output of Part 3-2. It contains:

- Description of the SuC
- Zone and conduit diagrams
- Threat environment for each zone
- Risk assessment results
- Target Security Level (SL-T) for each zone and conduit
- Required countermeasures derived from the risk assessment
- Security requirements derived from organizational policies and applicable regulations
- Assumptions and constraints

ZCR 7 — Obtain Asset Owner Approval

Before the CRS becomes the design basis for Stage 4 implementation, it must be formally approved by the asset owner. This is not a rubber-stamp activity — approval means the asset owner accepts the residual risk and commits to funding the controls required to reach SL-T for each zone.

Using cyber risk quantification, the baseline financial loss value of the existing environment is compared against the loss reduction of the moving forward with a higher SL-T. This financial justification is more effective than moving risk from “red to orange”.

Work Products

- Updated SuC inventory and network architecture diagrams
- Initial cybersecurity risk assessment
- Zone and conduit partitioning with documented criteria
- Cyber risk quantification baseline (optional)
- Detailed risk assessment for zones exceeding initial tolerance
- Cybersecurity Requirements Specification (CRS) with SL-T per zone
- What-if analysis using CRQ the financial loss reduction of improved security level (optional)
- Approved CRS signed off by the asset owner

Stage 3 typically takes

4 to 8 months for a single facility, often longer for legacy or complex multi-process environments. The risk assessment is the project's longest single technical exercise; budget time accordingly.

STAGE 4 Implement Technical Controls

Primary reference: ISA/IEC 62443-3-3 (System security requirements and security levels)

Purpose

Part 3-3 defines the technical security requirements an IACS must meet to achieve each Security Level. Where Stage 3 determined what Target Security Level each zone needs, Stage 4 is the engineering work of selecting, procuring, configuring, and validating the controls to meet that target.

Part 3-3 is organized around seven Foundational Requirements (FRs). Every requirement in the standard is derived from one of these seven. The FRs are the structure that makes the standard navigable; without them, an asset owner faces an undifferentiated list of dozens of technical requirements.

The Seven Foundational Requirements

FR	Name	What It Addresses
FR 1	Identification and Authentication Control	How users, devices, and systems prove who they are
FR 2	Use Control	What authenticated identities are permitted to do
FR 3	System Integrity	Protection of the system from unauthorized modification
FR 4	Data Confidentiality	Protection of information from unauthorized disclosure
FR 5	Restricted Data Flow	Controls on data movement between zones and conduits
FR 6	Timely Response to Events	Detection of and response to security events
FR 7	Resource Availability	Ensuring system availability against degradation or denial

Key Activities

Map FRs to Zones and Determine Required Strength

Each zone has an SL-T from Stage 3. Part 3-3 specifies requirements at four security levels (SL1 through SL4), where higher levels address increasingly capable adversaries. For each FR, the requirements are stronger at higher SLs. Stage 4 begins by mapping every FR to every

zone at the zone's SL-T, producing a control specification matrix that drives procurement and implementation.

Conduct a Gap Analysis Against Current State

For each control specified by the matrix, assess whether the existing IACS already meets the requirement, partially meets it, or fails to meet it. The gap analysis becomes the basis for the remediation plan.

Plan Remediation Sequencing

Remediation in operational facilities cannot happen all at once. Production schedules, maintenance windows, equipment lifecycles, capital cycles, vendor support, and operational risk all constrain when changes can be implemented. Sequencing typically prioritizes:

1) Safety-related gaps and zones with severe consequence exposure
2) Gaps where compensating measures cannot adequately bridge the residual risk
3) Controls that enable later controls — for example, network segmentation before zone-specific access controls
4) Controls aligned with planned equipment refreshes or expansion projects, where the marginal cost is lowest

This is also where financial prioritization is most directly useful. Most asset owners will face more gaps than budget can close in a single planning cycle. Without a way to compare "how much risk does this dollar of remediation reduce against another dollar spent elsewhere," the prioritization conversation tends to defer to noisy proxies like CVSS severity scores or general impressions of criticality. Quantified risk methods expressed in dollar terms are explicitly designed to answer that question — addressed in the closing section.

Select Capable Products

Where new equipment is required, select products that meet the zone's SL-T. Products with ISASecure System Security Assurance (SSA) certification have been independently validated against Part 3-3 at specific security levels. Products with ISASecure Component Security Assurance (CSA) certification meet the corresponding Part 4-2 component requirements. Using certified products simplifies the asset owner's evidence burden and reduces the integration cost of demonstrating SL conformance.

Implement With Validation

Each control is implemented, tested, and validated. Validation means producing evidence that the control operates as intended, not just that it is present. Validation evidence becomes part of the audit trail that will be reviewed during ACSSA preparation in Stage 6.

Apply Compensating Measures Where Direct Controls Are Infeasible

Legacy systems frequently cannot natively meet a Part 3-3 requirement — a 20-year-old PLC may have no native authentication capability, for example. Part 2-1 anticipates this: compensating measures (additional network isolation, monitoring, physical security, procedural controls) are valid responses, provided they are documented, deliberate, and supported by a risk assessment showing residual risk is within tolerance.

Work Products

- FR-to-zone control specification matrix
- Gap analysis against current state
- Multi-year remediation plan with sequencing rationale
- Using cyber risk quantification, you can forecast the financial risk reduction as major milestones in the remediation plan are implemented. When you achieve the goal, you can use the financial benefit to retain your OT cyber budget from attempts to reduce or cancel it.
- Procurement specifications for new equipment
- Implementation records and validation evidence per control
- Documented compensating measures with supporting risk assessments

Stage 4 typically takes

2 to 4 years for a mid-complexity facility to bring all zones to their respective SL-T. Many controls are implemented incrementally; the timeline reflects sustained engineering work, not project duration to a single closeout.

STAGE 5 Operate & Maintain

Primary references: All parts touched in Stages 1–4, applied operationally — particularly Parts 2-1 (ongoing program), 2-3 (patching execution), 2-4 (service provider oversight), and 3-3 (sustained control effectiveness)

Purpose

Stage 5 is not the end of the project — it is the rest of the program's life. Once controls are implemented and the Security Program is operating, the work shifts from establishment to sustainment. Most cyber security failures in industrial environments are not failures of design or implementation; they are failures of ongoing operation: a patch deferred too long, an account left enabled past a contractor's departure, a monitoring rule that stopped firing months ago, an asset added without being added to the inventory.

Key Activities

Execute the Patch Management Program

The patch management program established in Stage 1 against Part 2-3 now runs operationally. The discipline includes ongoing monitoring of vendor advisories, regular risk-informed decisions about which patches to apply, scheduled deployment windows aligned with planned outages, and documented rationale for any deferred patches. Compensating measures applied to unpatchable systems are reviewed periodically to confirm they remain effective.

Maintain the Asset Inventory Under Change Control

Any change to the IACS — added asset, removed asset, configuration change, network change — flows through change management. Some organizations have integrated DCS/SCADA/ICS/OT work into their work permit office, because changes to OT require similar safety evaluation and this is a good juncture to ensure it follows change control. The asset inventory becomes the operational source of truth and must remain current. Stale inventories are the most common single weakness identified during audits and conformity assessments.

Operate Continuous Monitoring

Monitoring deployed in Stage 4 must remain operational: alerts being received, baselines updated, rules tuned, false positives investigated. Monitoring that stops being watched is monitoring that has been removed.

Conduct Periodic Access Reviews

User accounts, service accounts, vendor access, and privileged access all require periodic review. Reviews typically run quarterly for privileged access and at least annually for all access.

Every account that is unused should be evaluated for disablement; every access that exceeds the role's needs is reduced.

Run Incident Response Exercises

An incident response plan is only useful to the extent it has been exercised. Annual tabletop exercises and periodic technical exercises validate that the plan reflects reality and that personnel can execute it under pressure. Exercise outputs feed back into program improvement.

Oversee Service Providers

Stage 2 sets up service provider governance. Stage 5 operates it: periodic reassessment, access reviews, incident escalation handling, contract renewals with current Part 2-4 requirements, and onboarding/offboarding workflows.

Continuously Improve the Program

Part 2-1 expects the Security Program to evolve. Annual reviews of the program against changing threat conditions, regulatory environment, technology landscape, and the organization's own risk appetite produce program updates. Lessons learned from incidents, exercises, and near-misses feed into program enhancements.

Work Products

- Patch decision records (every applied or deferred patch documented)
- Asset inventory updates under change control
- Monitoring outputs, alert investigation records, and rule tuning history
- Access review records
- Incident response exercise reports and after-action improvements
- Annual program review and improvement plan
- Service provider reassessment records and contract renewals

Stage 5 runs

Continuously, for the operational life of the IACS. Sustained operation is what separates organizations that pass an ACSSA evaluation from those that achieve a certificate and then drift.

STAGE 6 Prepare for ACSSA Conformity Assessment

Primary reference: ISASecure ACSSA program documentation (ACSSA-100, -101, -200, -300, -303, -304, -305, -311)

Purpose

ACSSA — Automation and Control System Security Assurance — is the ISASecure conformity assessment program for asset owner IACS security posture. It is currently the only third-party certification program that attests to an asset owner's conformity with 62443 standards across the organizational, design, and technical dimensions. ACSSA was introduced in early 2026 and represents a significant new external validation option for industrial operators.

ACSSA evaluates against four parts of the standard: Part 2-1 (security program), Part 2-4 (service provider requirements), Part 3-2 (risk assessment), and Part 3-3 (system security requirements and security levels). These are the four parts that this implementation plan has been building toward. Stage 6 is preparation for the evaluation itself.

Inspection vs. Certification

ACSSA offers two scheme variants. The technical evaluation process and conformity criteria are identical between them; the difference is in the resulting attestation:

ACSSA Inspection

Performed by an accredited Inspection Body. Produces a pass/fail letter referencing a formal inspection report. Used typically for internal purposes — to gauge current security posture, to confirm readiness before pursuing certification, or to extend internal audit work. No public listing; results are confidential to the asset owner unless they choose to share.

ACSSA Certification

Performed by an accredited Certification Body. Produces a certificate and a certification report. Valid for three years, with annual surveillance reviews to maintain certification. Asset owners with certified IACS may display the ISASecure symbol in association with that IACS. Used typically as part of a long-term public commitment to security program maturity, in response to insurer or customer requirements, or to provide external stakeholders with formal, comparable evidence of cyber security maturity.

Key Activities

Implement Stages 1-4

This is a quick reminder that proceeding with an ACSSA inspection is a waste of time unless the facility has made significant progress or only needs validation they have implemented the necessary parts from 62443.

Select Scope and Engage a Body

The asset owner determines the scope of the IACS for evaluation. Scope typically aligns to the SuC defined in Stage 0 and refined in Stage 3, but can be narrower (a single zone, a single facility within a fleet) or broader as appropriate. An Inspection Body or Certification Body is selected from the ISASecure-accredited list. The Body confirms eligibility against ACSSA-300 requirements before any formal evaluation begins.

Assemble Required Evidence

Stages 1–5 have already produced the evidence — Stage 6 is the work of organizing it for evaluation. Required submissions typically include:

- System asset inventory under change control
- Risk assessment per Part 3-2
- Cybersecurity Requirements Specification
- Security Program documentation per Part 2-1
- Service provider assessments and contracts per Part 2-4
- Implementation and validation evidence for Part 3-3 controls
- Operational records showing sustained execution — patches, access reviews, monitoring, incident exercises

Conduct Pre-Evaluation Gap Analysis

Most Certification Bodies offer a pre-evaluation gap analysis as part of the certification engagement. This identifies areas of nonconformity early, allowing remediation before the formal evaluation. For asset owners pursuing certification rather than inspection, the gap analysis materially reduces the risk of evaluation findings that delay certification.

Execute the Evaluation

The Inspection Body or Certification Body executes the evaluation per the agreed plan. Evaluation typically includes documentation review, personnel interviews, walk-downs of the physical IACS environment, and review of operational records demonstrating sustained execution.

Address Nonconformities and Receive Attestation

Identified nonconformities are addressed against documented remediation plans. Upon successful evaluation, the asset owner receives either the inspection report (Inspection scheme) or the certificate and certification report (Certification scheme).

Maintain Certification (If Certified)

ACSSA certification is valid for three years. Annual surveillance reviews and a recertification process at year three are required to maintain certification beyond the initial period. Surveillance is generally less intensive than initial certification but follows the same criteria.

Work Products

- Defined ACSSA evaluation scope
- Selected and engaged Inspection Body or Certification Body
- Organized evidence package mapped to ACSSA-300 requirements
- Pre-evaluation gap analysis and remediation plan (for certification path)
- Formal evaluation report or certification certificate
- Surveillance plan for years 2 and 3 (for certification path)

Stage 6 typically takes

6 to 12 months from engagement to attestation, depending on scope, evidence readiness, and any nonconformities identified during evaluation.

Funding the Program: Why Quantified Risk Matters

Every stage in this plan has hinted at the same gap. The IEC 62443 series tells you what to do — establish a Security Program, assess risk per Part 3-2, implement controls per Part 3-3, govern service providers per Part 2-4. What it does not tell you is how much money any of this should cost, how much risk reduction each dollar spent will produce, or how to make the case to the executives and boards who control the budget.

This is not a flaw in the standard. 62443 is intentionally agnostic on financial methodology. Part 2-1 requires risk-based prioritization but lets the asset owner choose the methodology. Part 3-2 supports several risk assessment approaches but its illustrative examples use qualitative likelihood-impact matrices, not financial quantification. The standard's choice to remain methodology-neutral is a deliberate strength — it lets the framework adapt to organizations with widely different risk cultures, regulatory environments, and analytic capabilities.

But 62443 leaves a practical problem unsolved. Industrial operators are competing for capital against every other business priority — production expansion, equipment modernization, safety investment, operational efficiency, regulatory compliance, sustainability. Boards and CFOs allocate budget by comparing expected returns. A 62443 program described in qualitative maturity terms — "this raises our security posture from medium to high" — is hard to defend against a capital project described in dollar terms — "this will reduce production cost by $4M per year." The 62443 program loses that comparison even when, in actual risk-adjusted terms, it would win it.

Cyber Risk Quantification: The Financial Language

Cyber Risk Quantification (CRQ) is the discipline of translating cyber risk into financial terms — typically Annual Expected Loss (AEL), Value at Risk (VaR), and probability distributions of loss across scenarios. CRQ does not replace the 62443 process; it sits on top of it, taking the same risk assessment inputs the standard already requires and translating them into the financial language executives use to make capital decisions.

For a 62443 implementation, CRQ provides three concrete benefits:

- **Stage prioritization.** Which zone should be remediated first? Without financial quantification, prioritization falls back on qualitative judgments — "production zone is critical," "safety system is critical," "everything is critical." With CRQ, the answer is concrete: the zone with the highest expected loss reduction per dollar of remediation goes first.
- **Budget justification.** The annual security investment decision becomes defensible in the same terms as every other capital decision the organization makes. "This $2M of 62443 remediation reduces expected annual loss by $5M" is a conversation that the CFO and the board can have on familiar ground.

- **Program scope decisions.** Where in the standard's range of possible implementations should this organization aim? CRQ provides the analytic basis for deciding — and for defending — the chosen scope, target maturity levels, and remediation depth.

DeRISK, the DeNexus OT cyber risk quantification platform, is built to provide exactly this layer of financial analysis on top of an asset owner's 62443 program. DeRISK takes the same inputs the Part 3-2 risk assessment uses — asset inventory, control posture, threat environment, consequence model — and produces facility-level financial outputs. The platform's risk quantification is designed to be consistent with how the standard structures risk while expressing the result in the language of capital allocation.

ACSSA and the Cyber Insurance Market

There is a second financial dimension worth highlighting before closing this plan. The cyber insurance industry — particularly insurers and reinsurers writing OT cyber coverage for industrial operators — is closely watching ACSSA adoption. ACSSA evaluation reports represent something the insurance market has been seeking for years: a standardized, third-party-validated, data-driven artifact that describes an industrial operator's cyber security posture against an internationally recognized engineering standard.

For underwriters, an ACSSA report is materially better than a self-attestation questionnaire — better than even most consulting assessments — because the methodology is standardized across accredited Inspection and Certification Bodies, the report format follows a defined specification, and the outputs are directly comparable across insureds. As ACSSA adoption grows, asset owners that hold ACSSA inspection or certification are likely to find tangible benefits in their cyber insurance program: broader coverage availability, more competitive premiums, and reduced friction during underwriting and renewal.

This is the practical answer to "why pursue ACSSA at all?" beyond internal program rigor. The conformity assessment produces an externally credible artifact that has direct economic value in the insurance market — and the budget required to reach ACSSA-ready posture can be defended in part on that basis, alongside the risk reduction the program itself produces.

Closing: The Financial Case Is the Strongest Case

Implementations of IEC 62443 succeed when leadership stays engaged across multiple budget cycles. They succeed when each year's investment can be defended on its own terms, not as a single up-front capital ask the organization may not be able to sustain. They succeed when the program produces evidence the insurance market and external stakeholders can recognize and reward.

All three of those depend on speaking the language of finance throughout the program, not only at funding moments. The standard provides the engineering structure. Quantified risk provides the financial language. ACSSA provides the third-party validation. Together they form a

defensible, fundable, sustained program — not a single project with a beginning, middle, and end.

Learn more

Visit denexus.io/derisk-platform to see how DeRISK extends 62443 with financial quantification.

Read the companion article on IEC 62443 at www.denexus.io/learn/iec-62443 for the conceptual overview.

Connect with the DeNexus team for a discussion of how quantified risk can support your specific 62443 program.