ASTRA Ready

ASTRA LIBRARY

Certification Guide - ASTRA Cybersecurity Sales Specialist

Version 0.2 -

hello@astraready.com - www.astraready.com

ASTRA Cybersecurity Sales Specialist - Certification Guide

Launch-ready draft v0.1
Credential: ASTRA Cybersecurity Sales Specialist
Linked learning: ASTRA Cybersecurity Sales Specialist programme

This guide follows the same candidate-facing information architecture as the existing ASTRA Ready certification guides; curriculum facts come from the approved ASTRA Cybersecurity Sales Specialist programme objectives, blueprint and lessons, while examination operations follow standing ASTRA Ready policy.

1. About this credential

The ASTRA Cybersecurity Sales Specialist credential is designed for people whose commercial work involves cybersecurity products or services. It assesses whether a candidate can make evidence-led sales decisions about buyer authority, business consequence, product scope, deployed coverage, proof, licensing, managed-service responsibility and deal execution.

What the credential attests. A holder has passed an ASTRA Ready examination of commercial judgement for selling cybersecurity products and services at this level. The credential does not certify security engineering, penetration testing, security operations, legal advice, job performance or accreditation by another organisation.

The linked ASTRA Cybersecurity Sales Specialist programme is recommended preparation rather than an examination prerequisite. Entry to the assessment is open, subject to ASTRA Ready's candidate eligibility and examination policies.

The programme and examination are intentionally different from product training. Candidates are expected to decide what the supplied evidence supports, not to recall a vendor portfolio, configure a security tool or perform an attack or defence task.

2. The exam at a glance

Item | ASTRA Cybersecurity Sales Specialist specification

Credential | ASTRA Cybersecurity Sales Specialist
Linked programme | ASTRA Cybersecurity Sales Specialist programme
Scored questions | 40
Customer cases | 7
Staged cases | 1, containing 5 scored questions
Examination time | 100 minutes
Question formats | Single choice, exact set, row mapping, ordering and numeric
Performance-based questions | 5, included inside the 40 scored questions
Delivery | Online on the candidate's own supported computer
Supervision | AI-assisted checks with human review of flags
Marking | One point per scored question; no negative marking; no partial credit
Passing standard | Approved for each examination paper through standard setting rather than a fixed percentage
Result | Pass or Not yet passed, with the overall score, normally released within 3 working days
Credential validity | 3 years from issue
Retakes | A Not yet passed result requires a 14-day wait; no more than 3 sittings in a rolling 12-month period

Managing the 100 minutes

Forty scored questions across seven evidence-led cases gives an average of 2.5 minutes per question, but the evidence should be read before that arithmetic is used as a pacing rule. Spend enough time at the start

of each case to identify the customer decision, the records supplied and the boundaries those records create.

The staged case behaves differently from an ordinary case. Once a candidate advances to its next stage, earlier answers are locked, because later evidence may alter the commercially responsible next action.

Answer every scored question before the timer expires. Unanswered items receive no credit, and there is no penalty for choosing an incorrect response.

3. What the exam covers

The blueprint contains six domains and forty scored questions. The first four domains contribute seven questions each, while the final two contribute six each.

Domain | What is assessed | Questions | Weight

S1 | The security buyer and decision rights | 7 | 17.5%
S2 | Threat to business consequence, including India's incident-reporting and data-protection duties | 7 | 17.5%
S3 | What security product categories actually do; capability versus deployed coverage | 7 | 17.5%
S4 | Proof: POCs, assurance reports, questionnaires, frameworks and proof boundaries | 7 | 17.5%
S5 | Security commercials: licensing meters, managed services and honest risk-reduction claims | 6 | 15.0%
S6 | Deal execution: POC design, channel roles, handover and renewal | 6 | 15.0%

Regulatory currency for S2

India-related assessment content is controlled by the dated ASTRA Cybersecurity Sales Specialist Regulatory Reference Note rather than by memory. The note is calibrated to 3 October 2026 and states: "qualifying cyber incidents are to be reported within six hours; entities may provide information available at the time and supplement it later." That statement is used only with a supplied official extract and a stated seller/service boundary; candidates are not asked to give legal advice.

The same source control treats India's data-protection framework as phased. Examination material must provide the commencement facts needed for the decision and must not turn a future-dated provision into a current customer duty.

4. How the exam works

Every case starts with a commercial cybersecurity situation and a controlled evidence pack. The evidence may include meeting notes, decision-right records, incident summaries, service schedules, coverage tables, price rules, POC results, assurance extracts, questionnaires, framework mappings or channel agreements.

Candidates answer from what the case establishes. A plausible security statement does not become correct merely because it sounds familiar, and a well-known industry practice is not a substitute for the record supplied in the question.

The five response formats

Format | What the candidate does

Single choice | Select the one response best supported by the case
Exact set | Choose exactly the stated number of supported options
Row mapping | Assign one answer to every row, such as a decision right or evidence owner
Ordering | Place all listed commercial or evidence steps in the required sequence
Numeric | Calculate a result using the formula, denominator or commercial rule given in the case

The five performance-based questions are structured commercial evidence tasks, not technical labs. They cover a buyer-rights matrix, an India incident-support sequence, an effective-coverage calculation, a claim-to-proof matrix and a staged POC decision gate.

The staged case releases information in parts. The candidate is judged on the evidence that was available at each stage, and the design does not require guessing a fact intentionally withheld for a later stage.

5. Scoring and results

Each of the forty scored questions contributes one point. Exact-set, row-mapping and ordering items require the complete correct response for the point; the scoring model does not award partial credit.

The pass standard is not a percentage selected for convenience before the paper is reviewed. ASTRA Ready uses a documented standard-setting process for each examination paper and approves the standard before results are issued.

Candidates receive an overall score together with Pass or Not yet passed. A short release window allows supervision flags and examination irregularities to be reviewed by a person before a result becomes final.

Domain feedback may be published only when ASTRA Ready has enough evidence to treat that breakdown as reliable. A result never certifies that the candidate can perform technical cybersecurity operations in a live environment.

6. Before exam day

Use a supported desktop or laptop with a working webcam, a stable connection and a current supported browser. Complete the system check before beginning the sitting rather than discovering a device or permission issue after the examination clock is ready to start.

Choose a quiet private room where the screen and webcam can remain available for the full sitting. A government-issued photo ID must match the name on the candidate account.

The examination is closed book. External websites, personal notes, AI tools, another person and a second device are not permitted during the sitting; no calculator is permitted, and the arithmetic in numeric questions is designed to be done by hand.

Candidates who require an accommodation should request it before booking or starting the examination. The Candidate Handbook explains the available adjustment process and the evidence ASTRA Ready may request.

7. On exam day

The candidate completes identity checks, provides the required supervision consent, shares the full screen and performs the short room and camera checks shown by the examination interface. The monitoring system looks for events that may need review; it does not independently decide that a candidate has failed.

If the system raises a concern, a trained person reviews the relevant record before any misconduct decision is made. Candidates can provide an explanation and can use the published appeal route if they dispute the outcome.

During the sitting, stay inside the examination environment and do not copy, photograph, record or share question content. Saved responses are submitted when the candidate submits the examination or when the allowed time ends.

8. Sample questions

These five examples demonstrate the response formats only. They were written for this guide, use a fresh fictional organisation and are not adapted from the ASTRA Cybersecurity Sales Specialist programme lessons, any practice set, mock, simulation or examination paper.

Sample case - Vostapani Textiles

Vostapani Textiles is evaluating a managed security service for corporate endpoints used by operations teams in India and Singapore. The deal record assigns business sponsorship to the Chief Operating Officer, security acceptance to the Security Director, technical validation to the Infrastructure Lead, commercial negotiation to the Procurement Director and contract signature to the Chief Financial Officer. The approved

endpoint inventory is 1,360 devices. Eighty devices are documented retirement exclusions, leaving 1,280 devices in the intended protection population. The quote includes 1,250 endpoint entitlements; 1,220 agents are deployed and 1,184 are actively reporting. For this sample, effective deployed coverage means actively reporting devices divided by the intended protection population. A six-day lab POC used 93 seeded qualifying events. The signed success criterion required at least 84 events to create the defined alert within nine minutes; 87 met that criterion. Production traffic, overnight managed-service performance and production response actions were not tested. An independent assurance report covers the supplier-hosted service for its stated reporting period. Vostapani tenant-role configuration is outside that report. The pilot decision sequence is fixed: confirm the written POC criteria; run the lab POC; verify the result against the signed criterion; obtain the Infrastructure Lead's technical validation for the proposed deployment boundary; then open final commercial negotiation.

Question 1 - Single choice

Which customer statement is supported by the current POC evidence?

- A. The service has demonstrated production-wide security effectiveness for Vostapani's endpoint estate.
- B. The lab POC met its signed alert-timing criterion for the seeded events and tested conditions.
- C. The six-day result proves the managed service will meet the same timing during overnight operations.
- D. The independent assurance report confirms Vostapani's tenant roles are configured for the proposed deployment.

Question 2 - Exact set

Which TWO statements accurately describe the current endpoint coverage record?

- A. The intended protection population is 1,280 devices after the approved retirement exclusions.
- B. All 1,250 licensed devices are evidenced as actively reporting at the review point.
- C. The quoted entitlement exceeds the intended protection population by thirty devices.
- D. The reporting population is smaller than both the deployed population and the quoted entitlement.
- E. The 1,220 deployed agents establish managed-service response coverage for every deployed endpoint.

Question 3 - Row mapping

Map each decision to the owner named in the case.

Use these owner options for every row:

- A. Security Director - security control acceptance owner
- B. Infrastructure Lead - deployment boundary validation owner
- C. Procurement Director - commercial negotiation process owner
- D. Chief Financial Officer - contract signature authority

Rows:

- Accept the security design for this purchase
- Validate the proposed deployment boundary
- Run the final commercial negotiation
- Sign the contract

Question 4 - Ordering

Place the five pilot-to-commercial steps in the order required by the case.

- A. Verify the POC result against the signed criterion.
- B. Open final commercial negotiation.

- C. Confirm the written POC criteria.
- D. Obtain technical validation for the proposed deployment boundary.
- E. Run the lab POC.

Question 5 - Numeric

What is the effective deployed coverage percentage? Use the stated formula and give one decimal place.

Sample answers and explanations

Question 1 - B. The signed criterion was met in the lab POC: 87 of 93 seeded qualifying events produced the defined alert within nine minutes, against a threshold of at least 84. Option A generalises the laboratory evidence to production effectiveness; option C extends a six-day daytime test to overnight service performance; option D uses supplier assurance to answer a customer-tenant configuration question outside the report.

Question 2 - A and D. The approved exclusions reduce the intended population from 1,360 to 1,280, and the 1,184 reporting count is below both the 1,220 deployed count and the 1,250 entitlement. Option B substitutes licences for reporting evidence; option C reverses the quantity relationship because 1,250 is thirty below 1,280; option E turns deployment into proof of managed-service response coverage.

Question 3. Security design acceptance -> Security Director; deployment-boundary validation -> Infrastructure Lead; final commercial negotiation -> Procurement Director; contract signature -> Chief Financial Officer. The case assigns each right separately, so participation by one stakeholder does not transfer another stakeholder's authority.

Question 4 - C, E, A, D, B. The written criterion must exist before the POC runs; the POC produces the result; the result is checked against that criterion; technical validation follows for the proposed deployment boundary; only then does final commercial negotiation open.

Question 5 - 92.5%. 1,184 ÷ 1,280 × 100 = 92.5%. The denominator is the intended protection population after the eighty approved exclusions, not the licence quantity or deployment count.

9. How to prepare, retakes and appeals

Start with the six modules of the ASTRA Cybersecurity Sales Specialist programme and connect each lesson to the published objective it teaches. The useful preparation question is not "can I repeat the definition?" but "can I make the decision when the case contains a tempting claim, a missing owner or a scope mismatch?"

Use the programme's worked evidence, unscored checks and field checks to practise the habits the examination expects: trace authority, separate observed consequences from inference, distinguish capability from deployed coverage, match claims to proof, reconcile commercials and keep POC-to-production boundaries visible.

When additional disclosed practice or rehearsal material is made available for the ASTRA Cybersecurity Sales Specialist programme, use it to learn the examination mechanics rather than to memorise wording. Confidential examination content is never part of the learning material.

After a Not yet passed result, the normal ASTRA Ready retake wait is 14 days, and a candidate may sit no more than three times in a rolling twelve-month period. A later sitting uses a different examination paper where an approved alternate is available.

A credential remains valid for three years. Renewal requires passing the ASTRA Cybersecurity Sales Specialist examination that is current at the time of renewal; completing continuing professional development does not substitute for that examination under the current policy.

A candidate may ask for a result review within 14 days, challenge a potentially faulty item within 7 days and appeal a misconduct decision within 14 days. The Candidate Handbook and Appeals and complaints policy

control the process and should be read before the sitting.

10. Exam objectives

The following 36 objectives are the final v1.0.1 ASTRA Cybersecurity Sales Specialist objectives. Every scored examination question maps to one of these published objectives, and the example concepts indicate the kinds of evidence or decisions that can appear without creating an exhaustive syllabus.

S1 - The security buyer and decision rights

CS-01-S1 - Given a scenario, map the security buying group to the decision rights for business sponsorship, security acceptance, technical validation, commercial approval and signature.

Example concepts: economic buyer, security approver, technical evaluator, procurement, contract signatory.

CS-01-S2 - Given a scenario, distinguish a stakeholder's influence from the authority to accept security risk, approve architecture, release budget or commit the organisation.

Example concepts: influence, risk acceptance, architecture approval, budget authority, commitment authority.

CS-01-S3 - Given a scenario, reconcile conflicting success criteria from security, IT, operations, privacy or legal, procurement and the business sponsor before advancing the deal.

Example concepts: CISO priority, operations constraint, privacy concern, procurement gate, business outcome.

CS-01-S4 - Given a scenario, infer the next decision gate and the missing decision-maker evidence from meeting notes, an organisation chart and an approval matrix.

Example concepts: decision gate, missing stakeholder, approval matrix, meeting evidence.

CS-01-S5 - Given a scenario, diagnose a single-threaded security deal from the supplied contact history and choose the next stakeholder access request needed to test the buying path.

Example concepts: single-threading, champion, risk owner, evaluator, procurement access, stakeholder gap.

CS-01-S6 - Given a scenario, build a security deal decision map that separates recommender, evaluator, approver, signer, operator and risk owner, including unresolved authority.

Example concepts: recommender, evaluator, approver, signer, operator, risk owner.

S2 - Threat to business consequence, including India's incident-reporting and data-protection duties

CS-02-S1 - Given a scenario, classify which stated business consequences are supported by the supplied incident evidence and which remain assumptions or seller inference.

Example concepts: outage, data exposure, transaction disruption, recovery effort, evidenced consequence, assumption.

CS-02-S2 - Given a scenario, prioritise security sales discovery using the supplied business-service criticality, consequence tolerance and dependency evidence without inferring technical likelihood.

Example concepts: critical service, consequence tolerance, business dependency, discovery priority, technical likelihood.

CS-02-S3 - Given a scenario, judge whether a seller claim about supporting CERT-In incident reporting is supported by the product or service scope, without transferring the customer's reporting responsibility to the seller.

_Example concepts: CERT-In direction, six-hour reporting, service scope, reporting workflow, customer

responsibility._

CS-02-S4 - Given a scenario, use the supplied commencement notice and rule extract to distinguish India data-protection provisions already in force from future-dated duties and bound the sales message accordingly.

Example concepts: commencement date, phased enforcement, DPDP Act, DPDP Rules, current duty, future duty.

CS-02-S5 - Given a scenario, distinguish incident questions the seller can answer from approved vendor or service evidence from questions that require the customer's security, legal or regulatory owner.

Example concepts: vendor evidence, service evidence, incident fact, legal interpretation, regulatory owner, seller boundary.

CS-02-S6 - Given a scenario, write an evidence-bounded risk-reduction proposition linking the buyer's threat concern, business consequence, control objective, seller scope and residual exposure.

Example concepts: threat concern, business consequence, control objective, seller scope, residual exposure.

S3 - What security product categories actually do; capability versus deployed coverage

CS-03-S1 - Given a scenario, classify a security offer by the primary job its supplied capabilities perform rather than by the vendor's category label.

Example concepts: identity, endpoint, network, cloud, data, email, detection and response, exposure management.

CS-03-S2 - Given a scenario, distinguish a product capability shown in documentation from the portion of the customer environment where that capability is actually deployed and active.

Example concepts: documented capability, licensed population, deployed population, active telemetry, coverage exception.

CS-03-S3 - Given a scenario, calculate effective deployed coverage from the supplied eligible population, exclusions, licensed quantity, deployment status and reporting status.

Example concepts: eligible assets, exclusions, licences, onboarded assets, reporting assets, coverage percentage.

CS-03-S4 - Given a scenario, evaluate an alleged replacement or consolidation claim by separating overlapping features from the distinct security jobs, dependencies and uncovered use cases.

Example concepts: feature overlap, security job, dependency, consolidation, replacement claim, uncovered use case.

CS-03-S5 - Given a scenario, identify the operating dependencies required for a security capability to deliver its stated outcome and mark any dependency not evidenced in the deal record.

Example concepts: telemetry, policy, integration, identity source, analyst coverage, tuning, unproven dependency.

CS-03-S6 - Given a scenario, recommend a bounded security category fit using the buyer's concern, environment, operating model and observed coverage gaps, while naming what the category does not address.

Example concepts: category fit, environment, operating model, coverage gap, exclusion, adjacent control.

S4 - Proof: POCs, assurance reports, questionnaires, frameworks and proof boundaries

CS-04-S1 - Given a scenario, select the proof instrument that best answers the buyer's stated question and

identify the claim that instrument cannot establish.

Example concepts: POC, assurance report, questionnaire, framework mapping, certification, reference, claim boundary.

CS-04-S2 - Given a scenario, interpret a security POC result within its tested data, environment, duration and success criteria without generalising it to production-wide effectiveness.

Example concepts: POC scope, test data, test environment, duration, success criterion, production generalisation.

CS-04-S3 - Given a scenario, reconcile a buyer claim across a POC result, assurance report and questionnaire response and identify any conflict, gap or scope mismatch.

Example concepts: POC evidence, assurance scope, questionnaire answer, conflict, evidence gap, scope mismatch.

CS-04-S4 - Given a scenario, distinguish a supplier assertion, completed questionnaire response, independently tested evidence and customer-specific verification when judging proof strength.

Example concepts: assertion, questionnaire, independent test, customer verification, evidence strength.

CS-04-S5 - Given a scenario, interpret a security framework mapping as a statement of relationship or coverage and distinguish it from certification, implementation and legal compliance.

Example concepts: framework mapping, control relationship, certification, implementation, compliance claim.

CS-04-S6 - Given a scenario, assemble a proof plan that maps each disputed sales claim to the best available evidence, evidence owner, limitation and next verification step.

Example concepts: disputed claim, evidence source, evidence owner, limitation, verification step.

S5 - Security commercials: licensing meters, managed services and honest risk-reduction claims

CS-05-S1 - Given a scenario, identify the security licensing meter and the customer environment variable that will change billable quantity or leave part of the intended population uncovered.

Example concepts: user, endpoint, workload, asset, bandwidth, data ingest, event volume, coverage exposure.

CS-05-S2 - Given a scenario, reconcile the customer's security inventory to quoted entitlements and identify any assets, users, workloads or data volumes that fall outside the proposed commercial coverage.

Example concepts: inventory, entitlement, protected quantity, uncovered quantity, SKU scope, commercial coverage.

CS-05-S3 - Given a scenario, separate product entitlement from managed-service responsibilities, service hours, response commitments and customer-retained duties.

Example concepts: licence, MDR or MSSP scope, service hours, response commitment, escalation, retained responsibility.

CS-05-S4 - Given a scenario, calculate the commercial effect of a stated security-volume change and identify whether the effect changes price, coverage, service capacity or more than one of these.

Example concepts: ingest growth, endpoint growth, workload growth, overage, coverage threshold, service capacity.

CS-05-S5 - Given a scenario, classify a security sales claim as evidenced risk reduction, supported capability, modelled expectation or unsubstantiated guarantee and choose the bounded wording.

Example concepts: risk reduction, capability claim, modelled expectation, breach-prevention guarantee, compliance guarantee, bounded wording.

CS-05-S6 - Given a scenario, prepare a renewal commercial view that separates price movement, protected-population change, service-scope change and evidence of security outcome.

Example concepts: renewal baseline, price, protected population, service scope, outcome evidence, expansion.

S6 - Deal execution: POC design, channel roles, handover and renewal

CS-06-S1 - Given a scenario, define a security POC as a buyer decision test by specifying the buyer decision, the success criteria and an explicit stop condition before testing begins.

Example concepts: buyer decision, POC hypothesis, success criterion, stop condition, demo versus decision test.

CS-06-S2 - Given a scenario, design safe, representative POC test conditions using supplied data, controlled operating conditions and explicit exclusions, and record which production conditions remain untested.

Example concepts: representative test data, controlled condition, test boundary, exclusion, production data risk, untested production condition.

CS-06-S3 - Given a scenario, allocate vendor, distributor, reseller and MSSP responsibilities for quoting, implementation, managed operation and escalation from supplied agreements while preserving the customer as the decision-maker.

Example concepts: vendor, distributor, reseller, MSSP, quote ownership, implementation, managed operation, customer decision rights.

CS-06-S4 - Given a scenario, use an equivocal or failed security POC result to choose among retest, scope change, remediation, commercial hold or no-go, with the evidence required for that next action.

Example concepts: POC result, retest, scope change, remediation, commercial hold, no-go, evidence gate.

CS-06-S5 - Given a scenario, prepare a security POC-to-production and sales-to-delivery handover that preserves coverage baseline, integrations, tuning, staffing, service hours, escalation paths, exclusions and unresolved customer actions.

Example concepts: POC-to-production gap, coverage baseline, integration, tuning, staffing, service hours, escalation, customer action.

CS-06-S6 - Given a scenario, use renewal evidence to choose the next commercial action among renew, remediate coverage, change service scope or evaluate expansion without treating absence of incidents as proof of effectiveness.

Example concepts: renewal evidence, coverage remediation, service change, expansion, incident absence, effectiveness claim.

Certification boundary: Passing the examination demonstrates the assessed commercial judgement at the named credential level. It does not make the holder a security engineer, auditor, legal adviser or holder of an external professional approval.