
Tender Evaluation

PROJECT NAME

Demo Sample

AUTOMATE WHAT CAN BE REPEATED
GUIDE WHAT MATTERS



Tender & Bidder Information

Contracting Authority	Demo Metropolitan Technology Authority
Tender Title	Secure Edge Compute Hardware Refresh Program
Bidder	Company A - Edge Hardware Bidder

Pass/Fail Criteria Evaluation

Total	Pass	Fail	Inspection Required
10	7	2	1

Pass/Fail Summary

Overall result: 7 Pass, 2 Fail, 1 inspection. Deficiencies relate to an expired ISO 27001 certificate, unproven U.S. spare-parts logistics, and an unclear Day 90 acceptance milestone.

Criterion	Status	Comment
(1. Bidder Cases) 1.1.1 Submit offer through the designated secure procurement portal	Pass	Offer submitted through the designated portal as required.
(1. Bidder Cases) 1.1.2 Offer must consist of FOLDERS A, B, C, D, E, and F	Pass	All required folders are present in the bidder package.
(3. Mandatory Supporting Documents) 3.1 FOLDER A: Responsible declaration regarding absence of conflict of interest	Pass	Declaration of no conflict of interest provided.
(3. Mandatory Supporting Documents) 3.2 FOLDER B: Responsible declaration (financial capacity)	Pass	Financial capacity declaration provided; declared revenue exceeds the RFQ threshold.
(3. Mandatory Supporting Documents) 3.3 FOLDER C: Technical compliance declaration for mandatory hardware requirements	Pass	Technical compliance declaration provided and linked to supporting technical files.

Criterion	Status	Comment
(8. Technical and Professional Capacity Requirements) 8.1 Edge compute nodes meet minimum CPU, memory, storage, and network specifications	Pass	Core hardware specifications meet or exceed the RFQ minimums.
(8. Technical and Professional Capacity Requirements) 8.2 Secure Boot, TPM 2.0, signed firmware, and audit logging capabilities	Pass	Required hardware security controls are documented.
(10. Certificates / Standards / Compliance Requirements) 10.1 Valid ISO 27001 certification at proposal submission date	Fail	ISO 27001 certificate expired before the proposal submission date.
(11. Other Mandatory Requirements) 11.1 U.S.-based critical spare parts availability with next-business-day dispatch	Fail	U.S.-based inventory and next-business-day dispatch are not proven for all critical components.
(11. Other Mandatory Requirements) 11.2 Delivery and acceptance readiness within 90 calendar days	Inspection Required	Acceptance-readiness milestone is ambiguous against the 90-day deadline.

Weighted Criteria Evaluation

Scoring Note

The weighted technical score is based on four evaluation categories, each assessed on a 0–10 scale and contributing 25% to the overall result.

Criterion	Score	Max Score	Comment
Hardware Architecture and Performance	8	10	Strong core hardware proposal, with limited workload-specific validation.
Cybersecurity and Compliance Assurance	6	10	Technical controls are credible, but current certification evidence is weak.
Delivery and Implementation Readiness	8	10	Implementation plan is structured and credible, but acceptance timing needs confirmation.
Documentation Quality and Traceability	9	10	Submission is well organized and traceable, with limited evidence gaps.

Detailed Pass/Fail Documentation

1.1.1 Submit offer through the designated secure procurement portal

Pass

1. Bidder Cases

Detailed Reasoning

The submission receipt confirms that the offer was uploaded through the designated secure procurement portal before the deadline. The portal timestamp and receipt record provide sufficient procedural evidence that the required submission channel was used correctly.

No indication of late upload, use of an unauthorized channel, or missing portal confirmation was identified in the submitted material. On that basis, the criterion is assessed as Pass without the need for further evaluator inspection.

Evidence

- **File:** Company A - Folder A.pdf
- **File:** Submission_Receipt_CompanyA.pdf

1.1.2 Offer must consist of FOLDERS A, B, C, D, E, and F

Pass

1. Bidder Cases

Detailed Reasoning

The bidder package contains all required Folders A, B, C, D, E, and F. The structural submission requirement is therefore satisfied, while the substantive compliance of each folder is assessed separately under the relevant criteria.

This result confirms completeness at folder level only. It does not mean that every document inside each folder is compliant, but that the required submission structure is present and can be evaluated.

Evidence

- **File:** Company A - Folder A.pdf
- **File:** Company A - Folder B.pdf
- **File:** Company A - Folder C.pdf
- **File:** Company A - Folder D.pdf
- **File:** Company A - Folder E.pdf
- **File:** Company A - Folder F.pdf

3.1 FOLDER A: Responsible declaration regarding absence of conflict of interest

Pass

3. Mandatory Supporting Documents

Detailed Reasoning

Folder A contains a signed declaration confirming the absence of conflict of interest. No contradictory information was identified elsewhere in the submitted package.

The document addresses the required declaration directly and is not merely a generic administrative statement. No missing signature, missing date, or conflicting bidder information was identified in the reviewed material.

Evidence

- **File:** Company A - Folder A.pdf

3.2 FOLDER B: Responsible declaration (financial capacity)

Pass

3. Mandatory Supporting Documents

Detailed Reasoning

Folder B contains the required financial capacity declaration together with supporting revenue figures. The declared average annual revenue appears to exceed the RFQ threshold.

The supporting corporate profile provides additional context on the bidder's operating history and financial standing. Based on the submitted evidence, the financial capacity requirement is assessed as satisfied.

Evidence

- **File:** Company A - Folder B.pdf
- **File:** Company A - Corporate_Profile.pdf

3.3 FOLDER C: Technical compliance declaration for mandatory hardware requirements

Pass

3. Mandatory Supporting Documents

Detailed Reasoning

Folder C includes the bidder's formal technical compliance declaration for the proposed hardware solution. The declaration is present and cross-referenced to the technical proposal, bill of materials, datasheets, and cybersecurity annex.

The declaration is not evaluated in isolation. It is supported by technical files describing the proposed hardware configuration, including compute, storage, networking, and security-related components.

Evidence

- **File:** Company A - Folder C.pdf
- **File:** Company A - Folder D.pdf
- **File:** Company A - Technical_BOM.xlsx

8.1 Edge compute nodes meet minimum CPU, memory, storage, and network specifications

Pass

8. Technical and Professional Capacity Requirements

Detailed Reasoning

The proposed ECN-24X edge compute nodes meet the minimum CPU, memory, storage, and network thresholds stated in the RFQ. The technical proposal and product datasheet support the declared configuration.

The bill of materials is consistent with the declared configuration, reducing the risk that the bidder is relying only on unsupported narrative claims. The available documentation supports a Pass result for minimum hardware compliance.

Evidence

- **File:** Company A - Folder D.pdf
- **File:** Product_Datasheet_ECN-24X.pdf
- **File:** Company A - Technical_BOM.xlsx

8.2 Secure Boot, TPM 2.0, signed firmware, and audit logging capabilities

Pass

8. Technical and Professional Capacity Requirements

Detailed Reasoning

The cybersecurity annex documents Secure Boot, TPM 2.0, signed firmware validation, role-based access control, and audit logging. These controls match the mandatory hardware security requirements requested in the RFQ.

The controls are relevant to secure edge infrastructure because they address firmware integrity, privileged access, and operational traceability. Based on the submitted evidence, the technical security-control requirement is satisfied.

Evidence

- **File:** Company A - Cybersecurity_Compliance.pdf
- **File:** Product_Datasheet_ECN-24X.pdf

10.1 Valid ISO 27001 certification at proposal submission date

Fail

10. Certificates / Standards / Compliance Requirements

Detailed Reasoning

The ISO 27001 certificate provided by the bidder was valid from 14 March 2022 to 13 March 2025, while the proposal submission date was 20 June 2026. No renewal certificate or other current validation evidence was provided.

This is a material compliance issue rather than a minor documentation gap. The requirement calls for valid certification at the relevant tender date, and an expired certificate does not prove current certification status.

Evidence

- **File:** Company A - Folder C.pdf
- **File:** Certificate_ISO27001_CompanyA.pdf
- **File:** Submission_Receipt_CompanyA.pdf

11.1 U.S.-based critical spare parts availability with next-business-day dispatch

Fail

11. Other Mandatory Requirements

Detailed Reasoning

The support model refers to a regional logistics partner but does not explicitly confirm U.S.-based inventory for all critical spare parts or next-business-day dispatch for all covered components.

The evidence uses broad support and logistics language, whereas the RFQ requires a more specific commitment. Because the mandatory support requirement is not proven, the criterion is marked as Fail.

Evidence

- **File:** Company A - Folder E.pdf
- **File:** Company A - SLA_and_Support_Model.pdf

11.2 Delivery and acceptance readiness within 90 calendar days

Inspection Required

11. Other Mandatory Requirements

Detailed Reasoning

The delivery plan indicates an 88-day delivery and staging timeline, but the acceptance-readiness milestone is shown as Day 88–92. Because readiness by Day 90 is not stated clearly, the criterion requires further review or bidder clarification.

The plan is close enough to the requirement that it should not be treated as an automatic fail. However, it is not precise enough to be marked as a clean Pass without clarification from the bidder or judgment by the evaluation committee.

Evidence

- **File:** Company A - Folder E.pdf
- **File:** Company A - Delivery_Gantt.pdf

Detailed Weighted Documentation

Hardware Architecture and Performance

Score

8

Max Score

10

Weight %

25

Weighted Score

20

Summary

Strong core hardware proposal, with limited workload-specific validation.

Detailed Reasoning

The proposed ECN-24X nodes present a strong baseline architecture for the secure edge compute refresh, meeting or exceeding RFQ requirements for CPU, ECC memory, NVMe storage, networking, power supplies, and out-of-band management.

The proposal, datasheet, and bill of materials tell a consistent hardware story. The score remains below maximum because workload-specific validation is insufficient to show the sizing is optimized for the authority's actual edge workloads.

Points Lost / Reasoning

Two points were deducted because the proposal is strong at configuration level but weaker at validation level. The bidder provides specifications and datasheets, but not workload modeling, benchmarks, stress-test results, or scenario-based sizing.

This is not a compliance failure, but it prevents a maximum score because the evaluator cannot confirm the architecture is optimized for real operating conditions rather than merely meeting minimum thresholds.

Evidence

- **File:** Product_Datasheet_ECN-24X.pdf

Cybersecurity and Compliance Assurance

Score

6

Max Score

10

Weight %

25

Weighted Score

15

Summary

Technical controls are credible, but current certification evidence is weak.

Detailed Reasoning

The bidder provides a credible set of technical cybersecurity controls for the proposed hardware platform, including Secure Boot, TPM 2.0, signed firmware validation, role-based administrative access, audit logging, and controlled firmware updates.

From a technical-control perspective, the submission is aligned with the security features expected in enterprise-grade edge hardware. The main weakness is the expired ISO 27001 certificate, which materially reduces governance and compliance assurance at the time of submission.

Points Lost / Reasoning

Four points were deducted because the technical controls are present, but the bidder failed to prove current certification status at submission. A bidder may document strong security features in the hardware and still have weak cybersecurity assurance if governance evidence is outdated.

The expired ISO 27001 certificate weakens auditability and the contracting authority's ability to rely on the bidder's security-management maturity. A higher score would require current certification evidence, such as a renewed certificate or formal validation from the certification body.

Evidence

- **File:** Company A - Cybersecurity_Compliance.pdf

Delivery and Implementation Readiness

Score	Max Score	Weight %	Weighted Score
8	10	25	20

Summary

Implementation plan is structured and credible, but acceptance timing needs confirmation.

Detailed Reasoning

The bidder provides a structured implementation plan covering procurement, configuration, staging, logistics, site installation, validation, and transition to support. This gives the contracting authority reasonable visibility into the sequence of work and the dependencies between activities.

The Gantt-style plan indicates that delivery and staging can be completed within an 88-day window, which is broadly aligned with the 90-calendar-day requirement. The remaining concern is that acceptance readiness is shown as Day 88–92, so Day 90 compliance is not fully conclusive.

Points Lost / Reasoning

Two points were deducted because the implementation plan is sound in structure but ambiguous in final commitment. The plan does not clearly state that the full acceptance-ready condition will be achieved no later than Day 90.

If the RFQ requires readiness for acceptance testing within 90 calendar days, a Day 88–92 milestone range leaves room for non-compliance. The deduction reflects schedule-risk ambiguity rather than a weak implementation model.

Evidence

- **File:** Company A - Delivery_Gantt.pdf

Documentation Quality and Traceability

Score	Max Score	Weight %	Weighted Score
9	10	25	22.5

Summary

Submission is well organized and traceable, with limited evidence gaps.

Detailed Reasoning

The bidder's documentation package is well structured, with administrative files, declarations, technical proposal, bill of materials, datasheets, cybersecurity annex, delivery plan, support model, and pricing folder clearly separated.

The hardware configuration and security controls can be traced across multiple supporting files, which makes the submission efficient to review. Material gaps remain, however, on current certification, spare-parts commitments, and the acceptance deadline.

Points Lost / Reasoning

One point was deducted because the documentation is highly usable but not fully evidence-complete in every material area. The ISO certificate is present but expired, the spare-parts model lacks an explicit U.S.-based inventory commitment, and the delivery plan does not state the acceptance deadline with enough precision.

These issues do not make the whole documentation package poor, but they prevent a perfect score because some of the most important compliance claims are not backed by decisive evidence.

Evidence

- **File:** Company A - Folder D.pdf

Conclusion

Overall Pass/Fail Result

N/A

Inspection Required

Exclusion Decision

Inspection Required

Weighted Evaluation

Yes

Weighted Summary

The weighted evaluation is broadly positive, supported by strong hardware architecture, implementation planning, and documentation quality. However, the proposal is not award-ready without remediation of the expired ISO 27001 certificate, unproven U.S. spare-parts logistics, and the ambiguous acceptance-readiness milestone.

Recommended Next Action

The Contracting Authority should request:

- A valid current ISO 27001 certificate or formal renewal evidence.
- Written confirmation of U.S.-based critical spare-parts inventory with next-business-day dispatch.
- A revised milestone statement confirming readiness for acceptance testing no later than Day 90.

If the bidder cannot remedy the two failed mandatory items, the authority should consider exclusion on formal compliance grounds.

Recommendation

The Contracting Authority should request:

- A valid current ISO 27001 certificate or formal renewal evidence.
- Written confirmation of U.S.-based critical spare-parts inventory with next-business-day dispatch.
- A revised milestone statement confirming readiness for acceptance testing no later than Day 90.

If the bidder cannot remedy the two failed mandatory items, the authority should consider exclusion on formal compliance grounds.

Files Used

RFP/RFQ Files

- RFQ-HW-2026-041_Main_Tender_Document.pdf
- Attachment_A_Technical_Specifications.pdf
- Attachment_B_Evaluation_Methodology.pdf
- Attachment_C_Service_Level_Agreement.pdf

Bidding Files

- Company A - Folder A.pdf
- Company A - Folder B.pdf
- Company A - Folder C.pdf
- Company A - Folder D.pdf
- Company A - Folder E.pdf
- Company A - Folder F.pdf
- Certificate_ISO27001_CompanyA.pdf

Αποποίηση Ευθύνης:

- Το παρόν υλικό αποτελεί εσωτερικό βοηθητικό έγγραφο για την αξιολόγηση προσφορών που παράγεται για ενημέρωση και εργασιακή υποστήριξη και σε καμία περίπτωση δεν υποκαθιστά ούτε υπερισχύει της επίσημης διαδικασίας αξιολόγησης, της συμβατικής συμμόρφωσης ή των αποφάσεων των αρμοδίων οργάνων ή επιτροπών.
- Το παρόν υλικό δεν αποτελεί επαγγελματική ή νομική γνώμη, ούτε δεσμευτική εισήγηση για οποιαδήποτε πράξη ή παράλειψη από τον εκάστοτε αναγνώστη.
- Το παρόν υλικό είναι εμπιστευτικό και δεν επιτρέπεται η κοινοποίησή του σε τρίτους χωρίς εξουσιοδότηση.

Disclaimer:

- This material is an internal supporting document for tender bid evaluation. It is produced for information and operational support and does not replace or override the formal evaluation procedure, contractual compliance assessment, or decisions of the competent authorities or evaluation panels.
- This material does not constitute professional or legal advice, nor a binding recommendation for any act or omission by any reader.
- This material is confidential and must not be disclosed to third parties without authorization.