DOMINICA ELECTRICITY SERVICES LIMITED

TERMS OF REFERENCE (TOR)

IT Audit for Systems Integration and Operational Efficiency

Background

The Dominica Electricity Services Limited (DOMLEC) relies on multiple information systems and digital platforms to support its operations, service delivery, and decision-making processes. Over time, these systems may have evolved independently, leading to inefficiencies, duplication of processes, limited interoperability, and increased operational risks. Moreover, a significant part of the operations depends heavily on manual processing requiring substantial paper printing and contributing to operational inefficiencies.

To address these challenges, the Company intends to conduct a comprehensive IT audit to assess current systems, identify integration gaps, and recommend improvements to enhance overall efficiency, data flow, system performance, security, resilience, governance, and alignment with business requirements.

Purpose and Balanced Audit Approach

This engagement is intended to assess the effectiveness, integration, resilience and future development of DOMLEC's technology environment and the business processes that depend upon it. It is not intended to constitute a performance assessment of the IT Department or of individual employees.

The review shall recognize and document existing capabilities, investments, controls, successful integrations, improvements already implemented, and other good practices that should be retained, while independently identifying gaps, risks and opportunities for further enhancement.

Systems integration and operational efficiency are shared organizational responsibilities. Findings shall therefore consider the roles and dependencies of business process owners, system owners, IT, vendors/service providers, management decisions and priorities, approved budgets and resources, legacy technology, contractual constraints, and historical implementation decisions.

Before attributing a weakness or integration gap to a particular function, the Consultant shall establish the relevant root cause and distinguish, where reasonably possible, between technology limitations, business-process limitations, vendor/product constraints, resource or funding constraints, governance or decision-making factors, legacy conditions, and matters within the direct control of IT.

Objectives

Assess the current IT systems architecture and infrastructure.

- Evaluate the level of integration between existing systems and applications.
- Identify inefficiencies, redundancies, and bottlenecks in workflows.
- Review data management practices, including data sharing, consistency, quality, and governance.
- Assess system performance, reliability, scalability, availability, and resilience.
- Evaluate IT governance, controls, cybersecurity practices, business continuity/disaster recovery arrangements, and compliance with applicable good practices.
- Assess the alignment between business requirements and the capabilities of existing systems.
- Provide practical, prioritized, and actionable recommendations to improve system integration and operational efficiency.
- Identify and document existing strengths, effective controls, successful integrations, and technology capabilities that should be retained or expanded.

Scope of Work

IT Systems and Applications

- Inventory of core business systems and applications.
- Assessment of system functionality, utilization, supportability, and business criticality.
- Identification of legacy/end-of-life systems and associated operational or security risks.
- Assessment of system dependencies, interfaces, and opportunities for consolidation or modernization.

System Integration

- Evaluation of integration mechanisms, including APIs, middleware, interfaces, batch transfers, and manual processes.
- Identification of data silos and integration gaps.
- Assessment of interoperability between systems.
- Identification of opportunities to reduce duplicate data entry and manual processing.

Business Processes

- Review of key business workflows supported by IT systems. The review shall use a risk-based selection of priority workflows across relevant functions, potentially including Finance, HR, Customer Service, Engineering, Transmission and Distribution, and Generation. Bidders shall specify the proposed number of workflows, selection criteria and coverage assumptions in their methodology.
- Identification of process inefficiencies, redundancies, and excessive manual/paper-based activities.

- Assessment of alignment between business needs and system capabilities.
- Assess the respective responsibilities and dependencies of business process owners, system owners, IT, vendors, and management in enabling or constraining process improvement and integration.
- Identification of opportunities for workflow automation and improved digital processes.

Data Management

- Data flow analysis across systems.
- Assessment of data quality, consistency, duplication, ownership, retention, and accessibility.
- Review of data governance policies and practices.
- Assessment of controls over data exchange and interfaces between systems.

IT Infrastructure and Resilience

- Review of hardware, network, server, storage, virtualization, hosting, and related infrastructure environments.
- System performance, availability, capacity, and scalability analysis.
- Review of backup, recovery, disaster recovery, and business continuity arrangements relevant to IT systems.
- Review of cybersecurity controls relevant to the systems and infrastructure within the scope of the audit.

IT Governance and Controls

- Review of relevant IT policies, procedures, standards, and governance arrangements. Use relevant provisions of recognized frameworks as reference points, including ISO/IEC 27001 and 27002, COBIT, ITIL and the NIST Cybersecurity Framework, as applicable. This is not a requirement for comprehensive certification or a full compliance audit against every framework.
- Review of access controls, identity/user management, privileged access, and segregation of duties.
- Assessment of change management, configuration management, vendor management, and system lifecycle practices.
- Review of IT risk management and compliance practices.
- Assessment of governance and accountability for system ownership, data ownership, and technical/security responsibilities.

Utility and Critical Infrastructure Considerations

- Where applicable, assess dependencies and integration points between corporate IT systems and operational/critical infrastructure environments.
- Consider the operational impact, resilience, cybersecurity, and business continuity implications of recommendations affecting critical utility services.

- Recommendations affecting operational technology (OT), SCADA, metering, generation, transmission, distribution, or other critical environments must take account of safety, availability, and operational continuity requirements. This engagement primarily addresses enterprise IT. Review of OT, SCADA, metering and other operational systems shall be limited to interfaces, dependencies, data exchange, governance and cybersecurity interconnections with enterprise IT. Detailed OT penetration testing, protection-system testing, equipment testing and standalone operational audits are excluded unless expressly authorized in writing by DOMLEC. No intrusive testing shall occur without an approved plan and operational authorization.

Methodology

The audit shall use a structured, evidence-based approach that may include:

- Document review, including policies, procedures, system documentation, contracts, architecture diagrams, inventories, and relevant reports.
- Stakeholder interviews with management, IT personnel, system owners, business users, and other relevant personnel.
- System walkthroughs and demonstrations.
- Data analysis and appropriate sampling.
- Process mapping and gap analysis.
- Review of system interfaces, dependencies, and integration methods.
- Validation of material findings with relevant stakeholders prior to final reporting. Facilitate a draft-findings validation workshop with relevant stakeholders before finalizing the report, with material factual disagreements and management responses appropriately documented.
- Root-cause analysis for material gaps and inefficiencies before assigning responsibility or recommending corrective action.
- Balanced assessment of both strengths and weaknesses, including controls, capabilities and integrations that are operating effectively.
- Triangulation of evidence from IT, relevant business/system owners, management, documentation and, where appropriate, vendors before reaching conclusions on material findings.

Deliverables

Inception Report

- Detailed work plan, methodology, information requirements, stakeholder engagement plan, and confirmed timeline.

Current State Assessment Report

- Overview of existing systems, infrastructure, integration landscape, key business processes, existing strengths/good practices, and material findings.

Gap Analysis Report

- Identification and assessment of inefficiencies, risks, control weaknesses, redundancies and integration gaps, including root causes and relevant organizational dependencies.

Final Audit Report

- Comprehensive and balanced findings, including strengths and effective practices, risk-rated observations, root causes, practical recommendations, and a prioritized action plan identifying suggested priority, responsible area(s), dependencies, and indicative implementation horizon. The final report shall include a consolidated risk register and a phased implementation roadmap distinguishing immediate risk-reduction actions from medium and longer term initiatives. For each material recommendation, indicate risk/priority, responsible function(s), dependencies, expected benefits, indicative effort/resources, indicative cost or cost band where reasonably estimable, and implementation horizon.

Presentation to Management

- Executive-level presentation summarizing key findings, risks, opportunities, and strategic recommendations.

Duration and Timeline

The assignment is expected to be completed within three (3) months from commencement, broadly structured as follows:

- Phase 1: Inception and Planning
- Phase 2: Data Collection and Assessment
- Phase 3: Analysis and Reporting
- Phase 4: Presentation and Finalization

Roles and Responsibilities

Consultant/Audit Team

- Conduct the audit in accordance with the agreed scope, methodology, professional standards, and approved work plan.
- Maintain confidentiality and protect all Company information and system access provided for the assignment.
- Ensure that any testing or review activity does not unnecessarily disrupt Company operations.
- Deliver all reports and presentations within agreed timelines.

DOMLEC

- Provide reasonable access to relevant systems, documentation, facilities, and personnel.
- Facilitate interviews, workshops, system walkthroughs, and data collection.
- Identify appropriate management, IT, system owner, and business representatives.
- Review and provide timely feedback on deliverables.

Reporting and Communication

- The Consultant/Audit Team will report to the General Manager or a designated representative.
- Progress updates will be provided at least every two (2) weeks.
- Material issues requiring immediate attention will be escalated promptly.
- Draft findings should be discussed with relevant stakeholders to confirm factual accuracy before finalization.
- Where a finding involves a business process, system ownership, vendor dependency, funding/resource constraint, or management decision, the relevant stakeholder(s) shall be given an opportunity to provide factual context before the finding is finalized.

Confidentiality, Security and Data Handling

All information obtained during the audit shall be treated as strictly confidential and used solely for the purpose of this assignment. The Consultant shall comply with DOMLEC's applicable security, access, confidentiality, and data-handling requirements. Company information shall not be transferred, disclosed, retained, or processed outside the agreed arrangements without prior written authorization. Any system credentials or privileged access provided for the assignment shall be protected and returned or revoked at the end of the engagement.

Required Qualifications of Auditor/Consultant

- Proven organizational experience conducting IT audits, systems integration assessments, or comparable technology assurance assignments.
- Demonstrated expertise in enterprise applications, IT architecture, infrastructure, data management, cybersecurity, governance, and resilience.
- Experience assessing complex multi-system environments and business processes.
- Relevant experience in utilities, critical infrastructure, or similarly operationally sensitive environments is highly desirable.
- Knowledge of recognized IT governance, audit, cybersecurity, service management, risk, and business continuity frameworks.
- Proposed team members should possess appropriate academic qualifications and relevant professional certifications, or equivalent demonstrable expertise, appropriate to their assigned roles on the audit. Such qualifications may include Certified Information Systems Auditor (CISA), Certified

Information Security Manager (CISM), Certified Information Systems Security Professional (CISSP), Certified in Risk and Information Systems Control (CRISC), ISO-related auditor/lead auditor certifications, or other comparable professional credentials. These qualifications provide evidence of competence in areas such as IT auditing, cybersecurity, risk management, governance, information systems controls and compliance. DOMLEC does not require every proposed team member to hold all of these certifications; rather, the combined qualifications and experience of the proposed team should demonstrate that it has the appropriate expertise to effectively undertake the full scope of the audit.

- Strong analytical, stakeholder engagement, report-writing, and executive presentation skills.
- Ability to complete the assignment within the required three-month period.

Proposal Submission Requirements

Bidders should submit sufficient information to allow DOMLEC to evaluate their technical capability and proposed approach, including:

- Firm profile and relevant experience.
- Understanding of the assignment and DOMLEC's requirements.
- Proposed methodology and work plan.
- Proposed project schedule demonstrating completion within three (3) months. The proposed schedule shall show milestones and draft/final deliverable dates within the three-month assignment, including time for DOMLEC review and the findings validation workshop.
- Identification, roles, qualifications, certifications, and relevant experience of key personnel.
- Details of at least three (3) comparable assignments, where available, including client, scope, year, and reference contact.
- Identification of any proposed subcontractors or specialist resources.
- Separate financial proposal in accordance with the accompanying RFP.

Evaluation Criteria

Proposals will be evaluated using the following weighted criteria. Technical proposals will be scored against criteria 1–8 (maximum 90 marks). The financial score (maximum 10 marks) shall equal 10 times the lowest evaluated price among technically qualified proposals divided by the bidder's evaluated price. The evaluated price shall include all applicable fees, taxes, travel and reimbursable expenses on a comparable basis. The combined score is the technical score plus the financial score, out of 100. The highest-ranked bidder will ordinarily be invited to negotiations, subject to verification and DOMLEC's reservation of rights.

Table 1 - Evaluation Criteria

No.	Evaluation Criterion	Weight (%)
1	Firm's relevant experience in IT audits, systems integration and comparable assignments	10
2	Qualifications and relevant experience of the proposed audit team	15
3	Technical approach and audit methodology	20
4	Understanding of DOMLEC's requirements and the proposed scope	10
5	Experience with enterprise systems, infrastructure, cybersecurity, data management and IT governance	10
6	Relevant utility/critical infrastructure and OT/SCADA experience	10
7	Work plan, timeline and demonstrated ability to complete within three months	5
8	References and past performance on comparable assignments	5
9	Financial proposal and overall value for money	10
	TOTAL	100

Principles for Findings and Recommendations

- Findings shall be evidence-based, objective, proportionate, and linked to the applicable business, technology, governance or risk context.
- The Consultant shall avoid attributing systemic or integration issues to the IT Department solely because the affected process involves technology.
- Where responsibility is shared, the report should identify the relevant shared dependencies rather than assigning responsibility to a single function without supporting evidence.
- Recommendations should recognize existing investments and capabilities and, where practical, build upon them rather than assume wholesale replacement. Recommendations shall consider ongoing or approved technology investments, implementation commitments, contractual obligations and integration opportunities, and shall avoid unnecessary duplication of expenditure.
- The final report should distinguish immediate risk-reduction actions from medium- and longer-term modernization or integration opportunities.

Conflict of Interest and Independence

Bidders shall disclose any actual, potential, or perceived conflict of interest that could affect the independence or objectivity of the assignment. The selected Consultant shall remain independent in the conduct and reporting of the audit and shall promptly disclose any conflict arising during the engagement.
Bidders shall disclose current or recent assignments for DOMLEC and relevant system vendors and describe any safeguards required to maintain independence.

Acceptance of Deliverables

Deliverables will be subject to DOMLEC's review and acceptance. The Consultant shall address reasonable comments, factual corrections, and agreed revisions before final acceptance.