

THE UNIVERSITY OF THE WEST INDIES DIGITAL TRANSFORMATION PROJECT

TERMS OF REFERENCE

DELIVERY OF CONSULTANCY IN IMPLEMENTING ENTERPRISE ARCHITECTURE METHODOLOGIES AND ENTERPRISE INFORMATION SECURITY ARCHITECTURE

BACKGROUND

The University of the West Indies (UWI) has requested assistance from the Caribbean Development Bank (CDB) in financing the One UWI Digital Transformation programme. Through the Digital Transformation programme, the UWI will realize greater operational efficiencies and economies of scale that will allow the University to provide more consistent and reliable services to all stakeholders. This digitally-transformed environment will contribute significantly to The UWI achieving its strategic goals as outlined in the ‘Triple A’ Strategic Plan 2022-2027.

To enable the Digital Transformation programme, The UWI requires assistance in the implementation of Enterprise Architecture which will enable the university and its campuses to operate in a standard, secured manner in the digital space. The Consultancy will consist of two components:

1. Implementing Enterprise Architecture Methodologies; and
2. Developing and implementing the UWI’s Enterprise Information Security Architecture.

OBJECTIVES OF THE COMPONENT

The objective of the consultancy is to provide technical expertise, advice and training aimed at strengthening skills in implementing Enterprise Architecture using real world scenarios and practical exercises to explain and demonstrate, to the participants, how to apply Enterprise Architecture concepts to systems applicable to the education space. The second component is to developing Enterprise Information Security Architecture (EISA) along with the implementation of the EISA to secure the UWI’s digital ecosystem. The proposed training will include members of the UWI’s Computer Security Incident Response Team (CSIRT) with other technical members across the University.

SCOPE OF SERVICES

The scope of services is outlined in two sections:

1. Enterprise Architecture Implementation Training; and
2. Develop Enterprise Information Security Architecture.

Enterprise Architecture Methodologies Implementation

The training exercise will be executed over a 5 day period utilizing an instructor led, online format. It will incorporate both theoretical and practical sessions. At the end of each day's training exercise all participants will:

Day 1

Introduction to the concepts and establishment of the vision regarding the selected Enterprise Architecture model. Introduction of the three (3) view models including the Business View, the Link View and the Technical View, as well as the different concepts associated with each of them and their management.

Day 2

Review in detail the different concepts associated with Business Architecture, mainly covering the inputs that should be generated from the business vision for the assurance and correct understanding of the technological automations to be carried out.

Day 3

Review in detail the different concepts associated with Link Architecture, mainly covering the transformation of business inputs.

Day 4

Review in detail the different concepts associated with Technological Architecture, mainly covering the transformation of business artifacts into technical artifacts following the decoupling model and putting into practice the 9 layer Technological Architecture

Day 5

Review in detail the project cycle at the Project, Program and Portfolio level following the TOGAF models, as well as the involvement of the different profiles of the 3 views

Develop Enterprise Information Security Architecture

This component includes training for members of the UWI CSIRT in a hybrid mode, incorporating both theoretical and practical sessions. It is desirable to train all the members of the Team in the areas outlined in the Objectives section.

As part of the fulfilment of these Components, the Consultant(s) shall deliver the following services, based on a schedule to be established:

Expected Deliverables

Deliverable	Details
<p>Provide a clear and detailed roadmap for Enterprise Information Security Architecture (EISA) strategy, building blocks, and operating model</p>	<p>The consultant is expected to provide a clear path to UWI with respect to identifying the business, IT and compliance elements that must be secured to achieve key objectives and goals of the University.</p> <p>It is also expected that the roadmap should provide the ability to plan and prioritize strategic IT security investments pertinent to technology implementations and process enhancements re: UWI.</p>
<p>Assess the UWI's existing EISA maturity, conduct gap analysis, and provide recommendations</p>	<p>It is expected that in attempt to align UWI's strategic objectives with its business strategies, there may be gaps identified. The identified gaps may profoundly affect UWI's core information security requirements in its quest to complete enterprise-wide initiatives in an efficient and effective manner. An "as-is" situation, along with identified gaps and recommendations are to be documented.</p>
<p>Design an EISA framework that is aligned with the UWI's Enterprise Architecture Framework.</p> <p>(TRAINING included)</p>	<p>The proposed design should look at securing UWI, incorporating the dimensions of:</p> <p>Business – should take into consideration the way information security is practiced along with how the business of information security interrelates with the rest of UWI's through its processes, roles, responsibilities and organizational structures.</p> <p>Informational – should take into consideration the information required to run the information security function at UWI. It represents the information models used by the IT Security teams across the University, as well as, the models used to capture the security requirements for enterprise information.</p> <p>Technical – should investigate the security infrastructure architectures. It should capture the models that are used to abstract varying requirements for information security into guidance for required hardware and software configurations.</p>

Deliverable	Details
Provide cost benefit analysis and a budget estimate to build a next generation EISA with all components.	Prepare a cost benefit analysis and a budget, incorporating all campuses re: building an appropriate and updated EISA for the University.
Define process structures around Information Security Architecture (TRAINING included)	<p>The proposed structures defined should be constructed around EISA being built on appropriate policies that are enforced by effective combinations of operational processes, cultural behavior and technology. All UWI personnel and its organizational units should remain in accordance with the organization’s core goals and strategic direction while the EISA is being developed.</p> <p>The structures should help UWI as an enterprise, create, communicate, and improve its key security requirements, principals, rules, and models to help the enterprise evolve.</p>
Develop a comprehensive EISA including the key components.	<p>Business Context: Defines enterprise information use cases and their importance for reaching UWI’s business goals.</p> <p>Conceptual Layer: Provides the big picture, including the enterprise profile and risk attributes.</p> <p>Logical Layer: Defines the logical paths between information, services, processes and application.</p> <p>Implementation: Defines how the EISA should be implemented at UWI.</p> <p>Solutions: Details the software, devices, processes and other components used.</p>
Perform a current security risk assessment incorporating the areas of cyberattacks, malware, leaks of personal identifiable information (PII) and hardware and software failure events.	Conduct a current security risk assessment across the mentioned across the University and produce a report for UWI.
Ensure the EISA helps the UWI satisfy the requirements of applicable compliance standards, such as UWI’s	The proposed EISA should assist the University be in compliance with the mentioned standards.

Deliverable	Details
Data Protection Policy, PCI DSS and GDPR.	
Design EISA implementation roadmap, milestones, KPIs, and dashboard	The consultant should design an EISA implementation roadmap along with milestones, agreed KPI's and a complimentary dashboard for UWI re: the proposed EISA.

QUALIFICATION AND EXPERIENCE

The selected Consultant(s) must have a proven track record of delivering this training and experience working with diverse groups and stakeholders with the following minimum qualifications:

- Industry-recognized certification in the respective areas of training.
- Proven track record in the respective areas of Enterprise Architecture Methodologies
- Enterprise Information Security Architecture (EISA).
- Proven track record in providing teaching/learning environments in of Enterprise Information Security Architecture (EISA).
- Strong spoken and written communication skills and fluency in the English language.

KEY PERFORMANCE INDICATORS & EXPECTATIONS

- The number of UWI personnel trained.
- The number of high-risk vulnerabilities identified.
- The number of systems which fail established vulnerability scans.
- The number of resolutions achieved via designated remedial actions.
- The number of residual unresolved issues/events/incidents.
- The creation of an Enterprise Information Security Architecture (EISA) tailored for the UWI Ecosystem.

DURATION

The assignment period is expected for **six (6) months** (renewable subject to satisfactory work) and the tentative start date is October 2, 2023.

Date Last updated: July 19, 2023