Terms of Reference

Accreditation Knowledge Management System (AKMS)

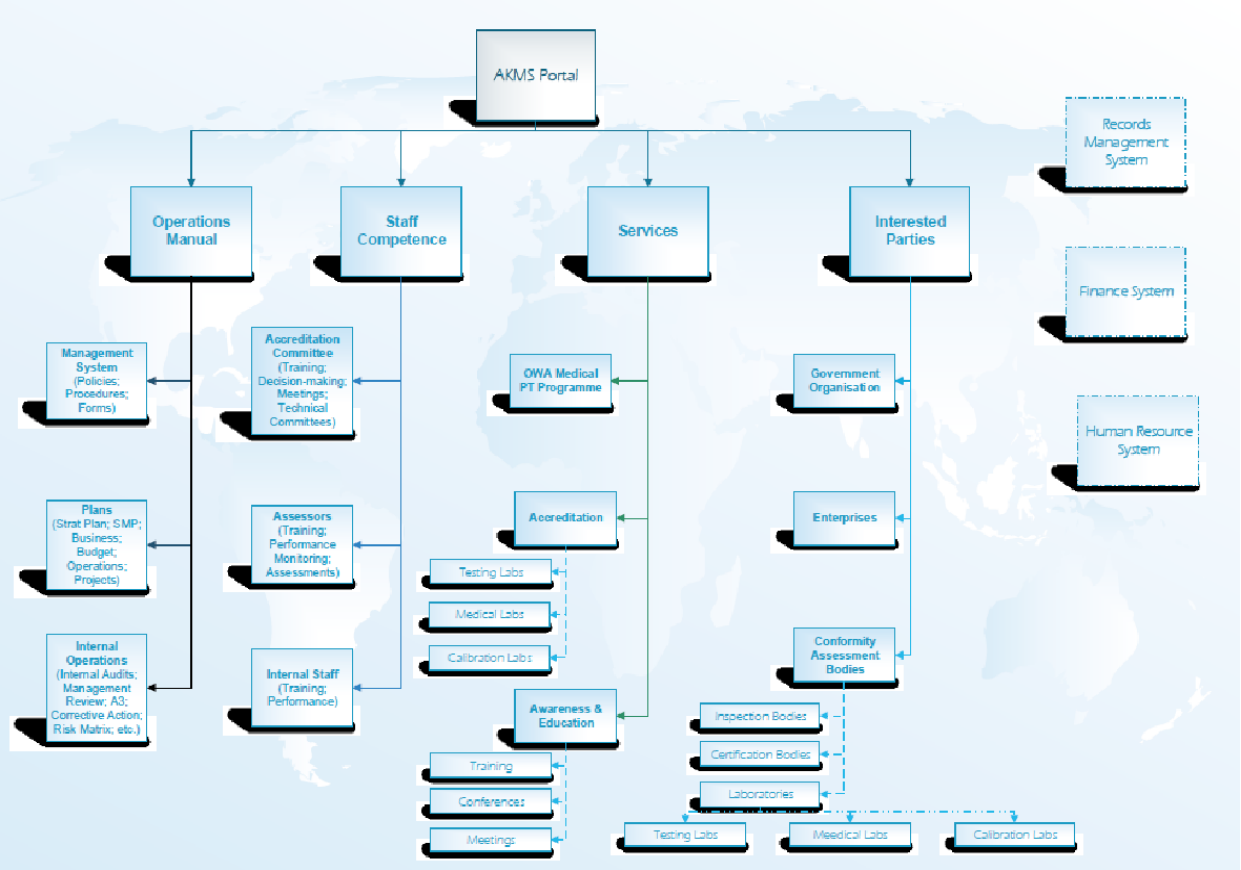
1. Introduction

The processes of the Accreditation Body are defined below in the body of this document. Figure 1 captures the processes operated by TTLABS that will require support from the Accreditation Knowledge Management System (AKMS). The schema is a named collection of information systems/platforms including logical structure.

1. **Interested Parties Platform,** which can be considered the Enterprise Customer Relations Management knowledge management information systems that holds complete information on the interested parties, and their business and interactions with the accreditation body.
2. **Service Platform**, which will provide access to the records of services offered by the accreditation body (accreditation; training; meetings; medical proficiency testing; conferences) which is linked to both the Interested Parties Platform and the Accounting Package for the accreditation body.
3. **Personnel Competence Platform,** which holds the records of personnel, both internal and contingent – assessors and Laboratory Accreditation Committee members that provide services for assessment and training programmes for the accreditation body and would include their training, mentoring and authorisation to perform these services.
4. **Accreditation Body Operations Manual Platform,** which holds all the documents that facilitate the operations of the accreditation body from the strategic plans, projects, policies, procedures, forms.
5. **Record Management Platform,** which holds the records as described in the record management system for the accreditation body and to which the appropriate platforms mentioned above are linked.

The dashed lines on Figure 1 are an indication of either expansion in services, such as Inspection Bodies, or systems outside of the AKMS, such as the Human Resource System.

Figure 1 Proposed AKMS Schema



The design of the AKMS is intended to facilitate the following services/processes. Please note that clarification for each area of consideration can be provided upon request.

A. Customer Request per Service

- Application Upload
- Training/Event Registration Upload
- Proficiency Testing (PT) orders

B. Processing of requests

- Notification of receipt of request via email to designated staff

C. Accreditation Service

- Verification that all documents were submitted and payment made
- Assignment of the assessment team
- Document review by the assessment team and report upload

D. Training or Event Registration

- Invoicing the customer
- Addressing logistical needs

E. Proficiency Testing

- Place order with supplier
- Invoicing customer

2. Service Processes

A. Accreditation service

- Onsite assessment and NC reports upload
- Non-conformity close-out
- Decision making)
- Schedule of Accreditation/Certificate generation and issuance

B. Training or Event registration

- Certificate generation and issuance

C. PT

- Maintenance of customer account
- Certificate download

D. Accounts– Application of business logic/rules are needed for this area.

2.D.1. Accounts receivable (terms of business)

- **Accreditation** – assessment fee (50% down payment and 50% balance payment after assessment and before assessment report), annual fee, close-out fee – to be paid before accreditation decision is released).
- **Training or Event Registration** – payment is due before or on the start of the event unless a payment agreement has been approved.
- **PT** – payment thirty days after date on invoice or schedule on approved payment installment plan.

2.D.2. Accounts payable (terms of business)

- **Accreditation** – Payment of assessors.
- **Training or Event** – Logistics (including but not limited to venue, catering, purchasing of standards, training material/presentations, tokens, Facilitator/Speaker, certificates)
- **PT** – payment of customs broker and supplier

3. Points for consideration

The technical proposal should outline a phased approach with key elements of the AKMS and extra functionalities delivered at the earliest time possible. See Figure 1 and the explanation in the Introduction for more information. The priority is a system that is interoperable and secure, while being used on varying devices and from varying users/locations/sources such as smartphones/tablets, interfaces with external providers, external user account set-up, business rules for validation, generation of reports through the system, and exceptions in management can be delivered in a next phase.

4. Design Requirements

A. Access

4.A.1. External – Web access

- Customer accounts must allow the customer access to track/monitor the service process
- Assessor Access Authorization for areas of access
- Staff accounts for tracking time/monitoring and identification (Assessors log in/out and report)
- Confirmation of uploading documentation will trigger email notifications to be sent to the linked party.
- Read only access for customer (closed files/records e.g. reports and invoices/receipts; LAC decision makers to customer reports)
- Provide a lost password or change password function with two factor verification for security (email and or phone security question)
- Ensure fast and efficient loading of page and uploading of information Enable data input through responsive devices such as smartphones, tablets, laptops, desktops, Chromebooks etc. and ensure compatibility;

4.A.2. Internal access

- Portal to Platform(s) – Interested Party or Stakeholder platform, Accreditation customer platform, PT customer platform, Assessor platform, LAC platform and Event or training platform
- Forms, standardized letters, certificates
- Electronic signatures – integrated
- Allow for creation and deletion of user accounts and modification of access rights by administrator;
- Super administrator access (all access for manager); Editing access (internal staff); Read only access (e.g. administrative assistant to customer reports);
- Provide a lost password or change password function with two-factor verification for security (email and or phone security question).

- Enable data input through responsive devices such as smartphones, tablets, laptops, desktops, Chromebooks etc. and ensure compatibility

B. AKMS

- Open source software for the knowledge management information systems development is preferred;
- Designed to ensure data integrity – Physical integrity, Logical integrity (entity, referential, domain and user defined);
- Allow the input of Symbols and Greek Alphabet (i.e. ≤, é, ≥, ±, ©, µ, α, °);
- Unique identifiers (stakeholder platform – per customer (to be determined); accreditation platform – per customer LAS-XXX M/T/C; PT platform per customer – MOHTT number; Training or event platform (to be determined)
- Fields to be completed depending on the type of platform (with format check e.g. to ensure numbers are entered as specified such as a twelve digit number; and code check e.g. postal codes or project codes or the PT MOHTT number). Certain fields will need to be expandable.
- Ensure that the user has completed all mandatory data entry fields before enabling registration of a new record. An instructive pop-up warning/message should inform the user of the data entry error as well as the reasons for the error (context sensitive help);
- Uniqueness check to ensure that information is not duplicated in the system (i.e. forms which require attachments should not accept duplicate attachments/files/records). If a duplicate record is found, the system should provide means of handling the duplicate record, e.g., merging already created records or deletion.
- Presence of unique dataset identifier within dataset to link all records relating to a given request.
- Enable quick and easy search for specific datasets, which should not be case sensitive (customer name, unique identifier and date in the specific format of year and month).
- Provide functionality to sort search results in either ascending or descending order.
- Provide flexibility when creating reports as well as when redefining report parameters.
- Reporting capability must include the generation of reports using multiple criteria as well as provide automatic calculation features.
- Ability to derive statistical data from the AKMS. For example, how many laboratories, assessors, length of time on assigned projects etc. and enable the easy creation of graphics based on datasets.

C. Security

- Designed to ensure data security
- Two factor verification – email address, user name, password;
- Provide an encryption mechanism for securing the entire AKMS (data at rest);

- Secure in terms of confidentiality, integrity and availability.
- System architecture should be designed to detect, track and measure any performance degradation including measuring AKMS performance, gathering AKMS statistics, automatic performance diagnostics and comparing AKMS performance over time.
- Security measures and dataset need to be compliant with defined ISO/IEC standards or Technical Requirements; for example ISO/IEC 9075 SQL standard, and compliance with the Trinidad and Tobago Data Protection Act are required;
- User authorization by type of user; this is by user type and service that the user is accessing; and
- Time out for no activity after five minutes or extended log-in.

D. Administration management

4.D.1. Improvement and updates

- Ability to update records and regenerate new notifications or requests;
- Ability to update forms.

4.D.2. Traceability and audit

- Data access (date and time, user, activity, duration) with the possible graphical presentation of this data;
- Audit for data integrity
- Provide secure and automated audit capability for recording activities in the system, as well as changes made to data records;
- A history for all modifications must be permanently retained;
- Suspected attempts to access the system from unauthorized sources or manipulate data must be logged and reported to the Administrator, recording audit trail activities (nature of event, identity of user/system component, point of origin of event, date and time, identity of the data or system resources affected, duration of event and time out etc.);
    - Provide intrusion detection systems including error notification via email to the administrator;
- Provide means of ensuring that audit trails and log files cannot be altered or deleted;
- User Updates and corresponding logs shall be sent as an email notification to administrator for review of risk to data integrity and data security and possible additional corrective actions;
- Backup jobs reports, including success, failure and any issues with the backup process.

E. Backup and recovery

- Frequent automatic backups of the AKMS: differential backups on a daily basis to data storage designate one, full backups on a weekly and monthly basis to data storage designate two;
- Recommend data recovery process and disaster recovery process plans.

F. Archiving

- Archive Interested Party or Stakeholder platform – after eight years;
- Archive Accreditation customer platform – after twelve years;
- Archive PT customer platform – after two years;
- Archive Event or training platform – after two year;
- Archive Assessor platform – twelve years after the assessor no longer works for the Accreditation Body;
- Archive LAC platform - twelve years after the member is no longer a part of the Accreditation Body;
- Archive Accounts (separate programme) – after twelve years;
- Archive Human Resource (separate programme) – eight years after leaving the Accreditation Body.

G. Deliverables

1. Project plan for finalization within two weeks from the inception meeting.
2. Interim reports on progress of the project (time line to be decided suggested fortnightly).
3. Beta testing of the knowledge management information systems with TTLABS Staff.
4. Finalization of the AKMS.
5. Submission of user manuals and design manuals.
6. Requisite training, which will be recorded, for applicable personnel in the user and the design manuals.
7. Close out report two weeks after the end of training.
8. Six-month warranty for after-sale service.
9. Negotiations of an SLA for post implementation.