PROTOCOL AND USER GUIDELINE

ASCC Database for Monitoring and Evaluation System

The ASEAN Secretariat | 2024

Contents

Introduction

To effectively monitor and evaluate the implementation of the ASEAN Socio-Cultural Community (ASCC) Blueprint 2025 and the ASCC Post-2025 Strategic Plan, the ASCC recognizes the critical need for a comprehensive data management system to support and enhance socio-cultural development and progress across the region.

The ASCC Database for Monitoring and Evaluation (ADME) System enhances evidence-based and informed policy and decision-making. It addresses critical data challenges; ensures accurate, timely, and reliable data; and promotes transparency and accountability within the ASCC. The system also fosters collaborative efforts across Member States and sectoral bodies. The ADME System will enable ASCC sectoral bodies to track progress better, analyze outcomes, and make informed decisions — ultimately driving socio-cultural development in the ASEAN region.

This document provides a summary of the protocols of the ADME System, which covers data management, collection, organization, validation, storage, and publication. It also presents a guideline for users to operate the ADME System.

ADME System Protocol

The ADME System Protocol elaborates data management processes, including data collection/compilation, organization and cleaning, standardization and validation, analysis, data storage, dissemination, and publication, as well as a comprehensive and secure web-based database system for the ASCC. The ADME System feature the following databases:

Database A will include Tool 1 (Framework for Reporting on ASCC Sectoral Bodies' Implementation of the Sectoral Work Plans), Tool 2 (Monitoring Matrix of the Follow-Up Actions to Declarations), and Tool 3 (ASCC Blueprint 2025 Results Framework Monitoring Database (RFMD)).

Database B will include the ASEAN Socio-cultural Official Statistics Monitoring Database (OSMD), encompassing a comprehensive list of socio-cultural official statistical indicators produced and published by ASEANstat and/or international organizations such as the United Nations (UN) and the World Bank.

Database C will include the ASEAN Socio-cultural Administrative Records-Based Monitoring Database (ARBMD), developed from administrative records regularly prepared and managed by 15 Sectoral Bodies under ASCC across ASEAN Member States. This will complement the existing ASCC Blueprint Key Performance Indicators (KPIs).

Objectives

A protocol is a set of rules specifying how to format data, ensuring that the data entered into the system can be coded correctly and avoid errors resulting from differences in data entry. Protocols are necessary in the ADME System to ensure that all data entered separately by users responsible for monitoring ASCC activities and documents can be processed correctly by the system, thus yielding accurate data.

The specific objectives of the ADME System protocol are:

1. To ensure efficiency in data management, enhance overall quality, and uphold the reliability of collected data.
2. To standardize available socio-cultural data, thereby maintaining data integrity and accuracy while also serving as checkpoints for identifying and rectifying discrepancies and errors that may arise during data collection.
3. To specify formats, channels, and timelines for data publication with stakeholders, thereby fostering transparency and facilitating accessibility.
4. To establish security protocols for the web-based database system, prioritizing authentication, authorization, and encryption mechanisms to safeguard the system against unauthorized access and potential data breaches.
5. To institute procedures for addressing issues or errors that may be encountered by the system's intended users, ensuring effective resolution and continued functionality.

Data Collection Protocols

Since each ADME System database incorporates diverse data sources, there exists a potential for variance in the entered data, which may impact the data collection process and raise concerns regarding reliability. The three databases of the ADME System have distinct data collection needs and responsible agencies:

Database A

Database A is divided into three Tools: Tool 1, Tool 2, and Tool 3.

1. Tool 1 encompasses a detailed list of activities under ASCC Sectoral Bodies' Sectoral Work Plans, which was previously collected through the ‘Framework for Reporting on ASCC Sectoral Bodies’ Implementation of the Sectoral Work Plans’. This data is collected and updated by ASCC Sectoral Divisions of the ASEAN Secretariat.
2. Tool 2 comprises detailed information on the follow-up actions to the ASCC Declarations as collected through the ‘Monitoring Matrix of the Follow-up Actions to Declaration’. Data collection is conducted by ASCC Sectoral Divisions, and appointed officers of ASCC Sectoral Bodies are responsible for updating their respective national follow-up actions.
3. Tool 3 contains the Key Performance Indicators of the ASCC Blueprints, including targets, baselines, mid-term evaluations, and forthcoming end-term evaluation results. The data is entered into the ADME System by the ASCC Monitoring Division of the ASEAN Secretariat.

Database B

Database B contains official data from reputable organizations such as ASEANStats, ASEAN Centres, the World Bank, the United Nations, the Asian Development Bank, and other international bodies. In terms of data inclusion priority, ASEANStats and ASEAN Centres are accorded primary status, followed by other international organizations as guided by ASCC Sectoral Divisions.

1. **Data from the ASEANstats**
   Real-time connectivity to the ADME System is facilitated via an Application Programming Interface (API)

2. **Data from Other Organizations**
   In the context of data sourced outside of the ASEANStats, additional considerations arise, including public availability and ethical data collection. Each indicator on Database B has been reviewed to ensure accurate linkage.

   For the websites that can be directly linked to the ADME System, such as the World Bank, data can be automatically collected periodically. Meanwhile, for websites that cannot be linked to the ADME System, such as the Asian Development Bank, updates will be done manually by the ASCC Monitoring Division as the Overall Admin. The process of the data syncing is as follows:
   a. The ADME System downloads the data from identified sources.
   b. Upon completion of the download process, the system converts the data into a table or selected chart format so users can download the data through the ADME System interface.

Database C

Database C is the ASEAN Socio-cultural Administrative Records-Based Monitoring Database, comprised of administrative records collected and managed by the ASCC Sectoral Bodies across ASEAN Member States. To link the administrative records collected and maintained by the ASCC Sectoral Bodies to the ADME System, the following protocol is followed:

1. ASCC Sectoral Divisions or Sectoral Bodies may propose or request indicator inclusions for Database C to the ASCC Monitoring Division as needed.
2. The ASCC Monitoring Division, in consultation with ASCC Sectoral Divisions or Sectoral Bodies, determines the data sources
3. If data is sourced from Sectoral Bodies or Ministries websites, Data Management Specialists will explore the feasibility of direct linkage with the ADME System
4. In cases where direct linking is not feasible, the ASCC Monitoring Division will manually inputs and updates data into the ADME System through data forms.

Data Verification

To ensure that the data collected by the ADME System is accurate, complete, and reliable, the following measures and procedures are implemented for the data submission process:

Data Validation

The ADME System incorporates robust data validation protocols to systematically assess uploaded. Validation checks are designed to identify errors, inconsistencies, or outliers, ensuring the integrity of the data.

Data Verification

Procedures for data verification are established to confirm the authenticity and correctness of collected information. This involves conducting verification checks with relevant stakeholders to validate the accuracy of the data.

Standardized Data Collection Processes

The ADME System employs standardized data collection processes to ensure uniformity and consistency in the way data is gathered. This minimizes variations in data entry methods and enhances the overall reliability of the collected information.

Automated Error Detection

The ADME System is equipped with automated error detection mechanisms that actively identify and flag potential errors or inconsistencies during data entry or import processes. This enables prompt corrective action to maintain data accuracy.

Regular Data Audits

Periodic data audits are conducted to systematically review the accuracy, completeness, and reliability of stored data. These audits involve thorough examinations of random samples to validate the consistency of information within the system. The audits will be conducted by the ASCC Monitoring Division.

Feedback and Correction Loop

The ADME System incorporates a feedback mechanism, allowing users to report discrepancies or suggest improvements. This feedback loop facilitates continuous improvement, addressing data quality issues promptly and enhancing the overall reliability of the system. The data specialist team will assist in addressing improvements or fixes until the end of 2024.

Data Storage and Security

To ensure secure data storage within the ADME System, the following protocols have been established: Data Storage Security Protocols Rigorous measures have been implemented to ensure secure data storage in the ADME System. These encompass detailed procedures for physical and electronic storage:

1. **Physical Storage:** ADME System servers are housed in secure data centers with restricted access. Strict controls are enforced to prevent unauthorized physical access to the servers.

2. **Electronic Storage:** Data is encrypted using advanced algorithms during transmission and at rest in databases. Regular backups are scheduled to prevent data loss, and access controls are managed to restrict entry to authorized personnel only. These measures collectively prevent unauthorized access, data corruption, or loss, ensuring the integrity and security of the socio-cultural data within the ADME System.

Backup Procedures

Weekly backup procedures have been implemented to safeguard against data loss due to unforeseen circumstances such as system failures, hardware malfunctions, or emergencies. Backups are stored in secure locations to ensure data recoverability.

Data Access Permissions

Access to data within the ADME System is controlled through role management to ensure that only authorized personnel can access specific data sets. The ADME System user roles are as follows:

1. **Viewers:** Can only view and interact with the landing page and access aggregated data available to the public (Database B). This role is applied to the general public.
2. **Contributor:** Can add and edit databases. This role is assigned to ASCC Divisions, ASCC Secondment Officers, and ASCC Sectoral Bodies.
3. **Content Manager:** Can edit, move, and validate submitted data from Contributors. ASCC Divisions Assistant Directors or Senior Officers are assigned this role.
4. **Overall Admin:** Can edit, move, delete, and verify submitted data, as well as add or remove other users. This role is exclusively assigned to the ASCC Monitoring Division to ensure data quality and prevent loss.

The subsequent section will explain in more detail the roles and responsibilities of the ADME System users.

Encryption Mechanisms

Advanced encryption mechanisms are employed to secure data during transit and stored within the ADME System. This safeguards sensitive information from unauthorized interception or tampering, enhancing the overall confidentiality and integrity of the data.

User Authentication Protocols

Strict user authentication protocols are in place to verify the identity of users accessing the ADME System. These protocols include strong passwords, multi-factor authentication, and authentication logging setup.

Audit Trails and Monitoring

Certain users, namely the Content Managers and Overall Admins, can track user activities and changes to the data. For instance, the Content Managers receive notifications when their data is edited, and the Overall Admins are notified of any requested data removal. This ensures accountability and enables the identification of any unusual or unauthorized actions that may compromise data security.

Periodic Security Audits

Regular security audits are conducted to evaluate the efficacy of security measures within the ADME system. These audits entail comprehensive reviews of system configurations, access logs, and security policies to detect and mitigate potential vulnerabilities.

For these security audits, the OWASP (Open Web Application Security Project) checklist tool is employed. The OWASP is a nonprofit organization dedicated to enhancing software security. Their tool adheres to a set of guidelines aimed at bolstering website security.

Specifically, the ADME System utilizes the OWASP Top Ten, identifying the most critical web application security risks. These risks encompass issues such as injection attacks, broken authentication, sensitive data exposure, and others. The OWASP Top Ten list is periodically updated to reflect the evolving landscape of web application security threats. A detailed OWASP checklist is provided in Annex 1.

Protection Against Unauthorized Access

Additional security layers are implemented to mitigate unauthorized access attempts within the ADME System. These measures include deploying firewalls, intrusion detection systems, and other preventive mechanisms to strengthen the overall security posture of the ADME System.

Ethical Considerations

The development and implementation of the ADME System prioritize ethical conduct across all stages and processes, guided by several key considerations. By integrating these ethical guidelines into the ADME System, we aim to uphold the highest standards of integrity, transparency, and respect for the rights and well-being of all stakeholders involved in the Monitoring and Evaluation (M&E) process within the ASEAN Socio-Cultural Community.

1. **Protecting Sensitive Data**
   Recognizing the diverse socio-cultural context within the ASEAN community, the ADME System incorporates tailored measures to protect sensitive data such as data involving vulnerable populations by restricting access to country data and several databases that contain sensitive data such as Database C.

2. **Maintaining Confidentiality**
   Access controls, encryption, and anonymization techniques are implemented to prevent unauthorized access and protect the identity of individuals or entities contributing data.

Roles and Responsibilities

The success of the ADME System heavily depends on the clear definition of roles and responsibilities for each user of the system. Tables 1 to 4 outline the detailed roles of the users for Database A, B, and Menu:

Table 1. User Roles and Responsibility for Database A

No	Roles	Database A											
		Tool 1				Tool 2				RFMD			
		Overview	Upload	Edit	Approval	Overview	Upload	Edit	Approval	Overview	Upload	Edit	Approval
1	Public	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖	✖
2	Contributor	✔	✔	✔	✖	✔	✔	✔	✖	✔	✖	✖	✖
3	Content Manager	✔	✔	✔	✔	✔	✔	✔	✔	✔	✖	✖	✖
4	Overall Admin	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔	✔

Table 2. User Roles and Responsibility for Database B

No	Roles	Database B				
		Overview	Upload	Edit	Approval	Remove
1	Public	✔	✖	✖	✖	✖
2	Contributor	✔	✖	✖	✖	✖
3	Content Manager	✔	✖	✖	✖	✖
4	Overall Admin	✔	✔	✔	✔	✔

Table 3. User Roles and Responsibility for Database C

No	Roles	Database C				
		Overview	Upload	Edit	Approval	Overview
1	Public	✔	✖	✖	✖	✖
2	Contributor	✔	✖	✖	✖	✖
3	Content Manager	✔	✖	✖	✖	✖
4	Overall Admin	✔	✔	✔	✔	✔

Table 4. User Roles and Responsibility for Menu

No	Roles	Menu							
		About	Need Help	AMS	Article Menu	Sectoral Bodies	Indicators	Users	Roles
1	Public	✔	✔	✖	✖	✖	✖	✖	✖
2	Contributor	✔	✔	✖	✖	✖	✖	✖	✖
3	Content Manager	✔	✔	✖	✖	✖	✖	✖	✖
4	Overall Admin	✔	✔	✔	✔	✔	✔	✔	✔

Feedback & Support

To ensure continuous improvement and support of the ADME System, several features and protocols have been developed:

1. **User Feedback Mechanism**
   A user-friendly feedback mechanism has been implemented within the ADME System to encourage users to report issues, provide suggestions, and share their experiences. This mechanism can be accessed through an online feedback form or a designated support email, allowing users to communicate their concerns effectively.

2. **Response Time Target**
   A user-friendly feedback mechanism has been implemented within the ADME System to encourage users to report issues, provide suggestions, and share their experiences. This mechanism can be accessed through an online feedback form or a designated support email, allowing users to communicate their concerns effectively.

No	Priority	Definition	Response Time	Resolution Time
1	Severity 1 (S1)	**Major Impact** The issue that prevents users from accessing the system as a whole.	1 hour	4 hours
2	Severity 2 (S2)	**Significant Impact** The system's performance is significantly reduced, but the system's operations continue to run.	2 hours	1 day
3	Severity 3 (S3)	**Moderate Impact** The issues that occurred result in limited system operations.	4 hours	2 days
4	Severity 4 (S4)	**Low Impact** The issues that occurred do not result in the loss or non-operation of services.	1 day	3 days

3. **Dedicated Support Team**
   Until the end of 2024, a dedicated support team will be available to manage user inquiries, address technical issues, and handle feedback. The Data Management Specialists will provide contact information, including email addresses, phone numbers, or access to a dedicated helpdesk team within the ADME System, ensuring users have multiple avenues to seek assistance. By 2025, the ASCC Monitoring Division will manage user inquiries as well as addressing minor or basic technical issues.

4. **Knowledge Base**
   The Data Specialist Team will progressively develop and maintain a knowledge base or Frequently Asked Questions (FAQs) section within the ADME System. This centralized resource will serve as a repository for users to access self-help solutions and find answers to common queries, enhancing user experience and facilitating efficient problem resolution.

Compliance with Regulations

The ADME System operates within a comprehensive legal compliance framework encompassing regional, national, and international laws pertinent to data management, privacy, and socio-cultural development.

1. **Legal Compliance Framework**
   The ADME System operates within a legal compliance framework that considers regional, national, and international laws relevant to data management, privacy, and socio-cultural development.

2. **Regulatory Adherence**
   ADME System protocols adhere to regulatory requirements specific to the ASEAN region. This includes adherence to guidelines established by ASEAN bodies, national governments, and other relevant regulatory authorities overseeing data collection, storage, and analysis.

3. **Communication Change**
   Any updates to the ADME System Protocol resulting from regulatory changes will be communicated transparently to stakeholders and users. This communication includes clear documentation of alterations, the rationale behind the changes, and guidance on how users can adapt to the updated protocols.

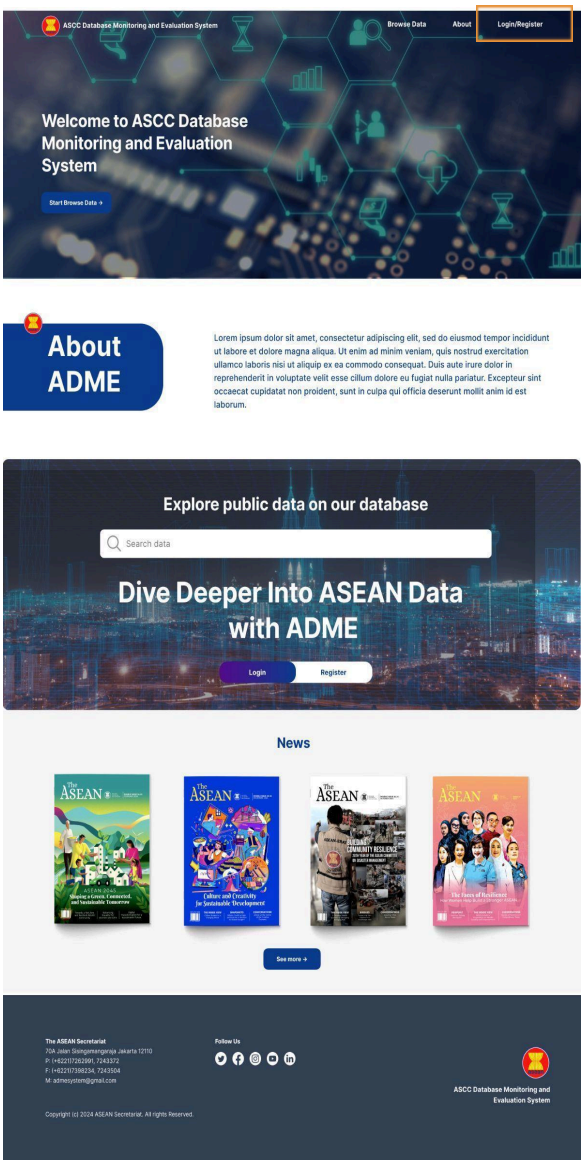
By ensuring a commitment to legal and regulatory compliance, the ADME System not only meets current standards but also anticipates and adapts to changes in the regulatory environment. This ensures the continued trust of our users and stakeholders in the accuracy, security, and ethical use of socio-cultural data within the ASEAN Socio-Cultural Community.

User Guideline

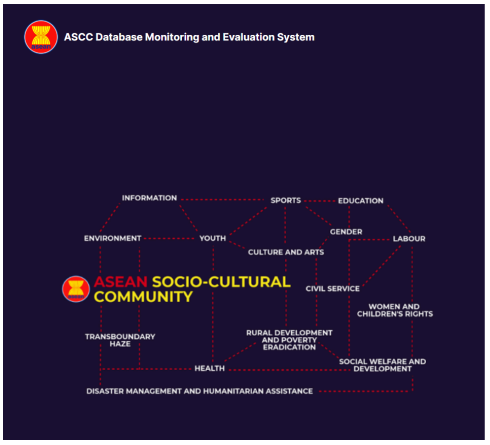
This section provides a detailed guideline to ensure effective utilization of the ADME System. By following these guidelines, users can maximize the benefits of the ADME System while ensuring the integrity, security, and ethical use of socio-cultural data within the ASEAN Socio-Cultural Community.

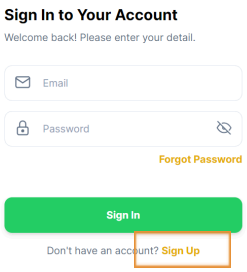
Sign Up

1. **Visit the Login Page**
   Go to the ADME website (adme.asean.org) and look for the "Login/Register" button. Click on it to open the login page.



2. **Visit the Registration Page**
   Click the "Sign Up" button to begin the registration process.

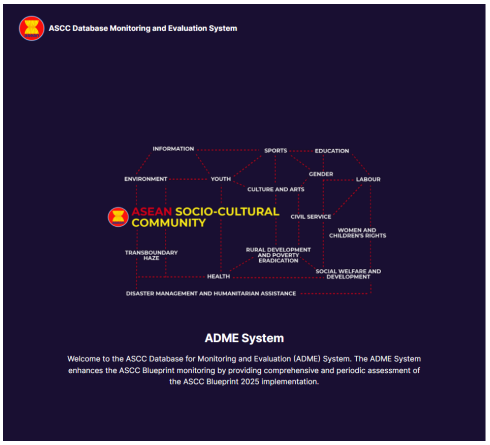


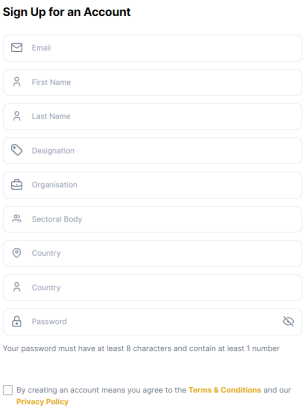


3. Fill in Your Basic Information

Once on the sign-up page, you will be asked to provide some information, such as:

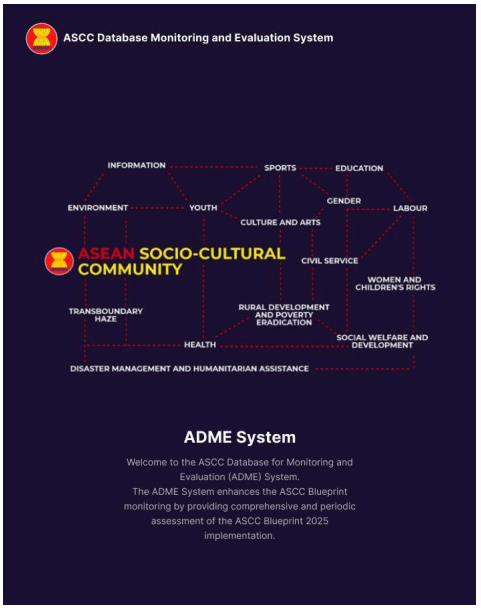
- Email Address (Please use your work email address or any active email address)
- First Name
- Last Name
- Designation
- Organization
- Sectoral Body
- Country
- Password (The password must be a minimum of 8 characters with number and letter)

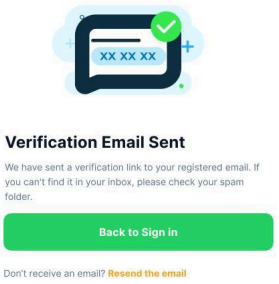




4. Account Verification

To secure your account, a verification code will be sent to the email address you provided. Check your inbox and enter the code on the verification page. If the email cannot be found in your inbox, please check your spam folder.



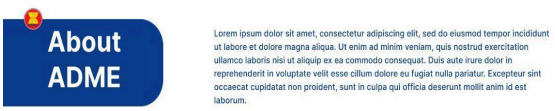


5. **Admin Verification**
   After your verification is complete, ASCC AMD and relevant ASCC Divisions will verify your request for an account. The process for the verification and granting of access may take approximately five working days. During the verification, you will be assigned roles based on your designation, organization, and sectoral body (if applicable). You will receive a confirmation email after you have been successfully verified.

6. **Enjoy ADME System!**
   Congratulations! You've successfully signed up. Explore the platform, discover new features, and make the most of your experience.

Login

1. **Access Login Page**
   Visit our homepage and locate the "Login" or "Sign In" button. Click on it to proceed to the login page.

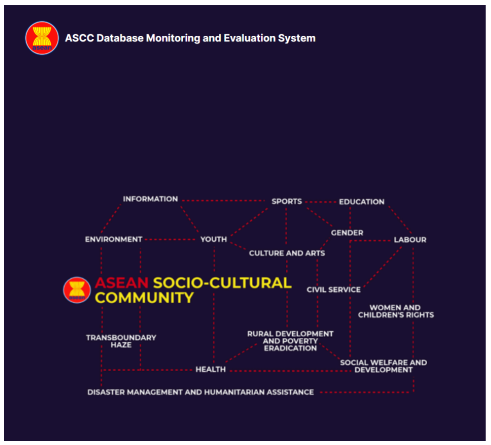


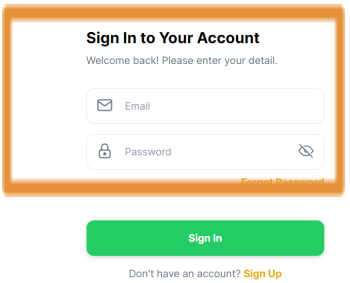
2. Enter Your Credentials

On the login page, enter the credentials associated with your account:

- Email Address
- Password

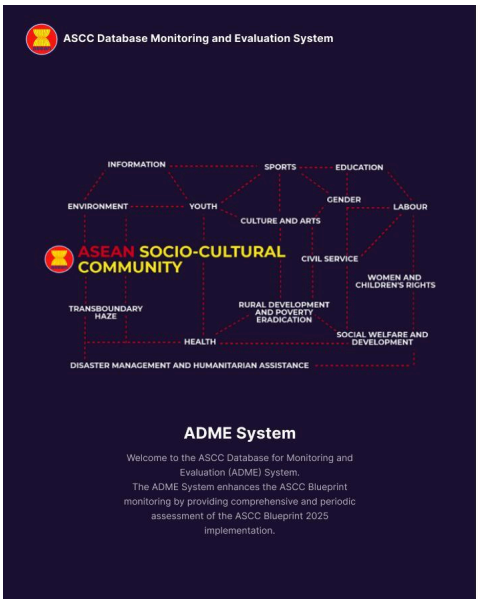
Please ensure that you enter the correct credentials. Click “Sign In” to proceed.

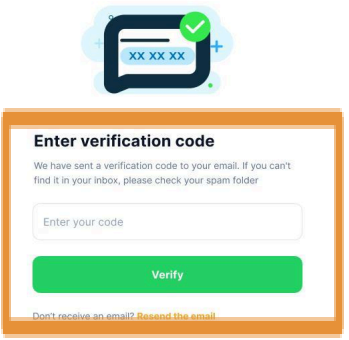




3. Two-Factor Authentication

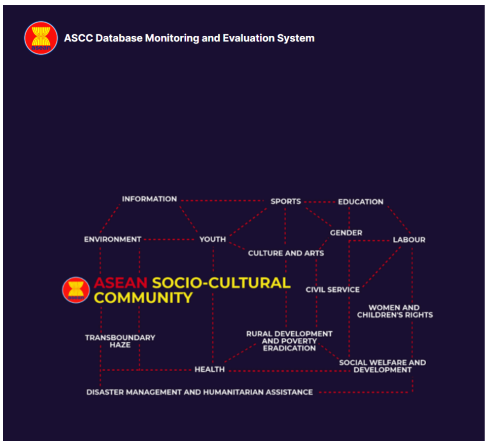
You will receive an authentication code in your registered email inbox. Enter this code to the field to complete the login process.

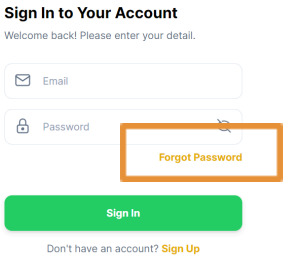


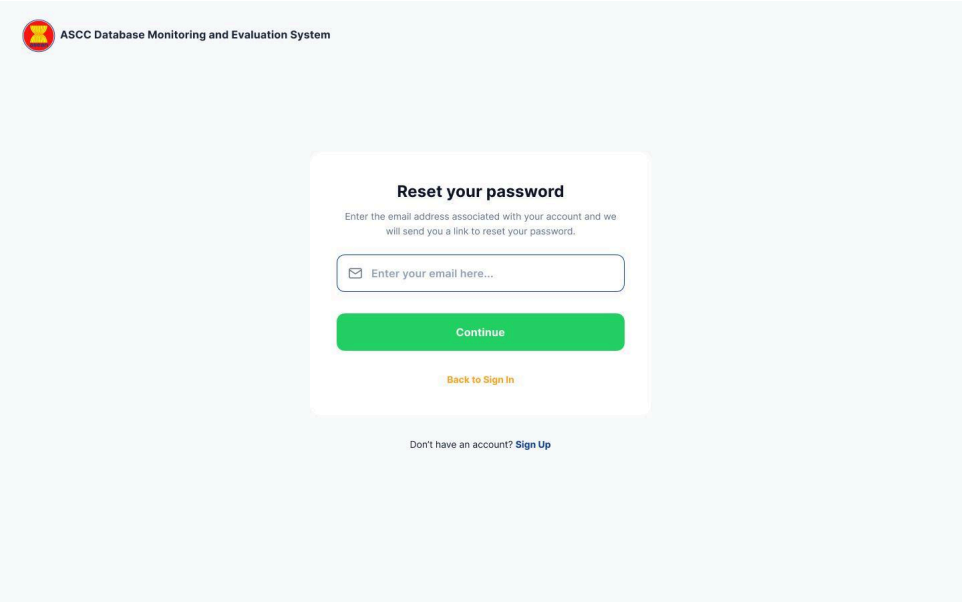


4. Forgot Password? Reset it

In case you forget your password, click on the "Forgot Password" on the login page. Follow the prompts to reset your password securely.







5. **Stay Secure - Avoid Public Devices**
   For added security, avoid logging in from public computers or devices. Remember to log out after your session if you must use a shared device.

6. **Update Account Information**
   Regularly update your account information, including password, to enhance security.

7. **Log Out Securely**
   After finishing your session, click on the "Log Out" button to ensure the security of your account.

Browsing ADME System Databases (For Guests)

Guest Mode

1. **Homepage Overview**
   Upon landing on our homepage, take a moment to explore key sections such as:
   - About ADME System
   - Browsing data button

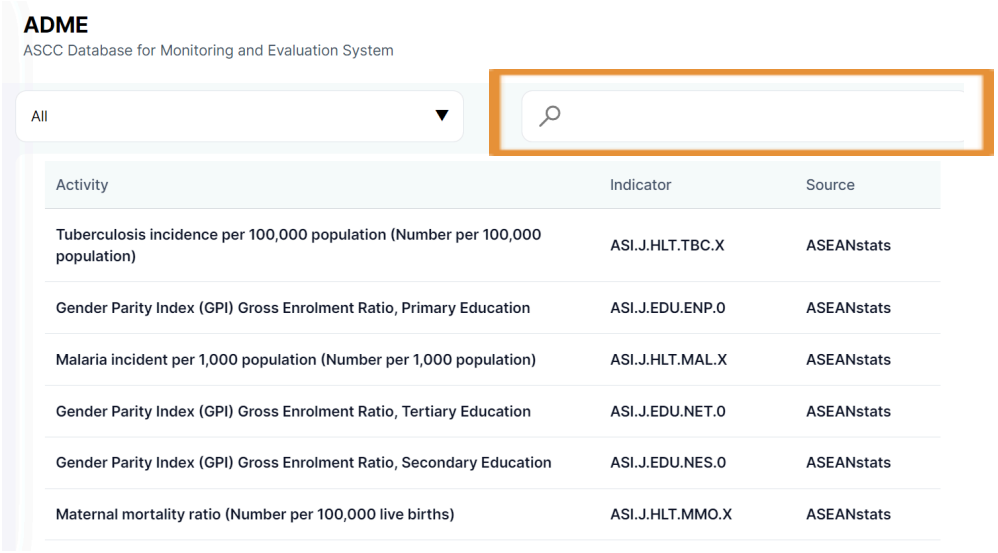
- Public database search feature
- Link to ASEAN Magazine

2. Browsing the Public Databases

As viewers, you can still browse for public indicators, which is Database B. To browse

for indicators, click on the “Browse Data” button.

On the Database B page, input the keywords you to search on the search bar and click enter. The system will show you the indicators that are closest to the keywords you searched.



Browsing Database (For Registered Users)

Browsing Overview All Database in ADME System

Based on your assigned roles, you will be able to gain a deeper access of the ADME System Databases. To get this access, you must Sign Up to the system and be assigned a role by the Overall Admin/ASCC AMD.

There are four roles available within the ADME System:

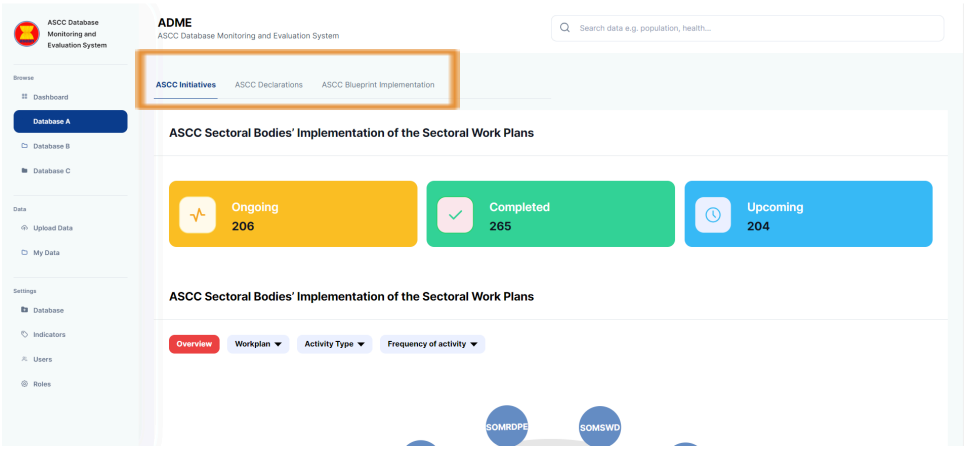
- Viewer (can only view and interact with Dashboard). This will apply to the general public and other stakeholders of the ASCC.
- Contributor (add and edit database). This will apply to ASCC Divisions, ASCC Secondent Officers, and ASCC Sectoral Bodies Officers.
- Content Manager (add, edit, move). This will apply to ASCC Divisions' ADRs or SOs for updating and editing of submitted data.
- Overall Admin (add, edit, move, delete data, add or remove users). This role will be assigned exclusively to the ASCC Monitoring Division to ensure data quality and prevent possible loss.

All user roles will have access to the overview page of Databases A, B, and C.

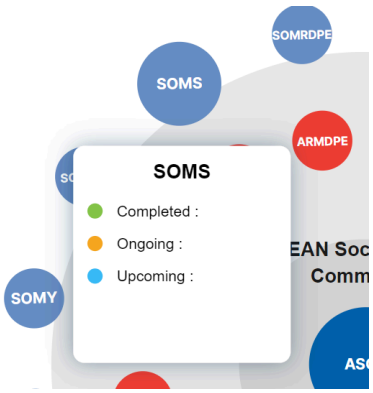
Browsing ASCC Sectoral Bodies' Implementation of the Sectoral Work Plans (Database A Tool 1 - ASCC Initiatives)

1. In the main menu on the right side of the homepage, select Database A.

2. The Overview of Database A - ASCC Initiatives page will appear.

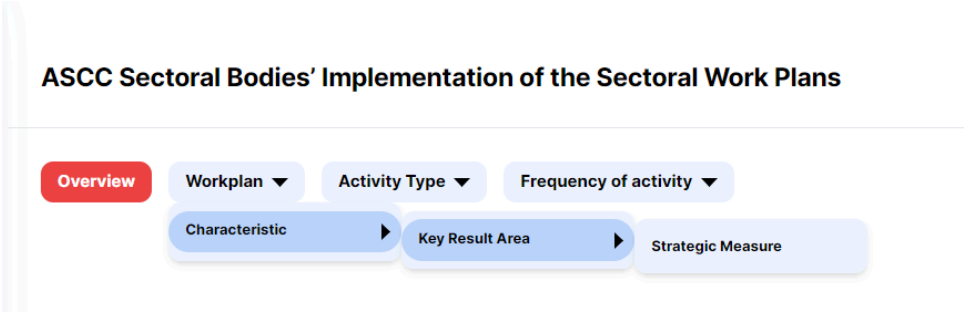


3. Click on one of the sectoral body circles, and then a pop-up description of the activity status of that sectoral body will appear.



4. If you are a member of that sectoral body, a "See All" button will appear in the pop-up. If you click the button, you will be redirected to a new page consisting of the list activities under the workplan of the sectoral body.

5. You can also use a filter feature to screen the activity details.

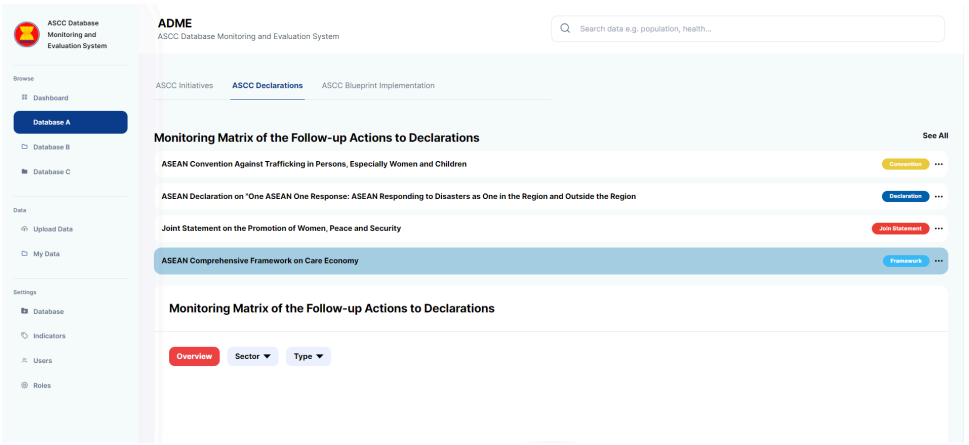


Browsing ASCC Monitoring Matrix of the Follow-up Actions to Declarations (Database A Tool 2 - ASCC Declarations)

1. On the main menu on the right side of the homepage, select Database A.

2. The Overview Database A - ASCC Initiatives page will appear, and next click the tab option of ASCC Declarations.

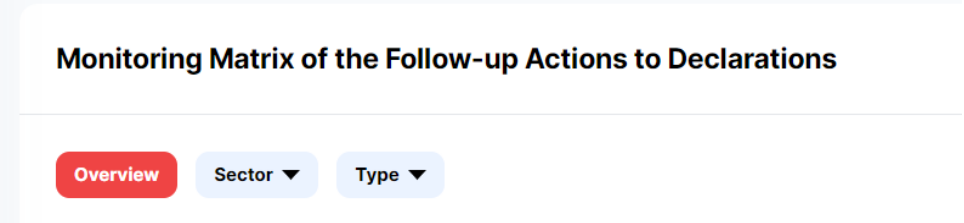
3. The Overview Database A - ASCC Declarations page will appear, which consists of two sections. The first section displays a list of the latest declaration documents, and the second one shows the follow up action to ASCC declaration from each AMS.



4. Click the "See All" button in the top right corner of the document list to see the entire list of documents stored in the database.

5. If you want to see more on the follow up action of each AMS, click on one of the AMS circles in the second section. A pop-up description of the follow-up action to the declaration of the AMS will appear.

6. You can also use the filter feature to screen the follow-up action.

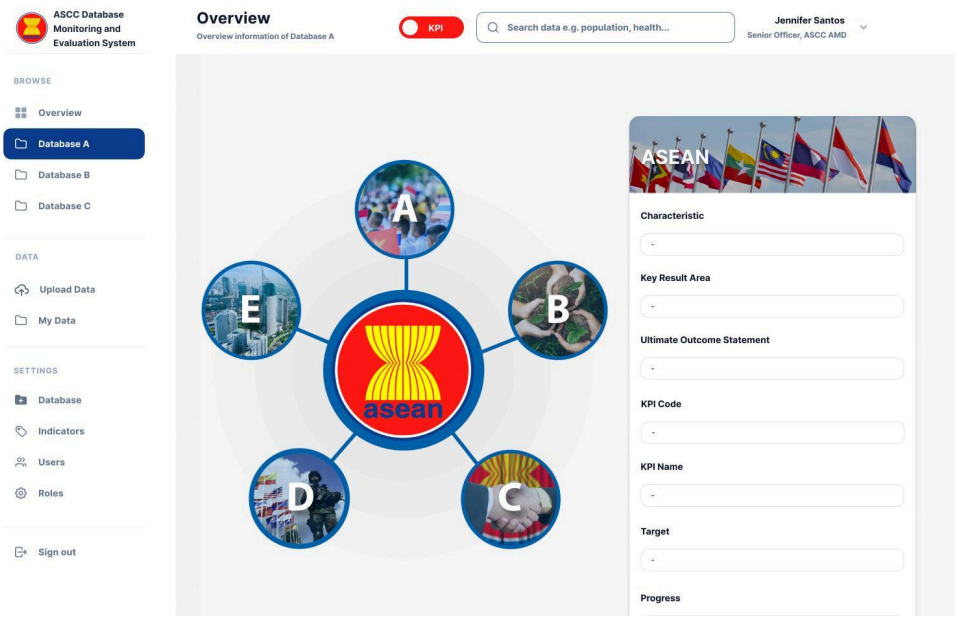


Browsing ASCC Blueprint 2025 Results Framework Monitoring Database (Database A Tool 3 - RFMD)

1. In the main menu on the right side of the homepage, select Database A.

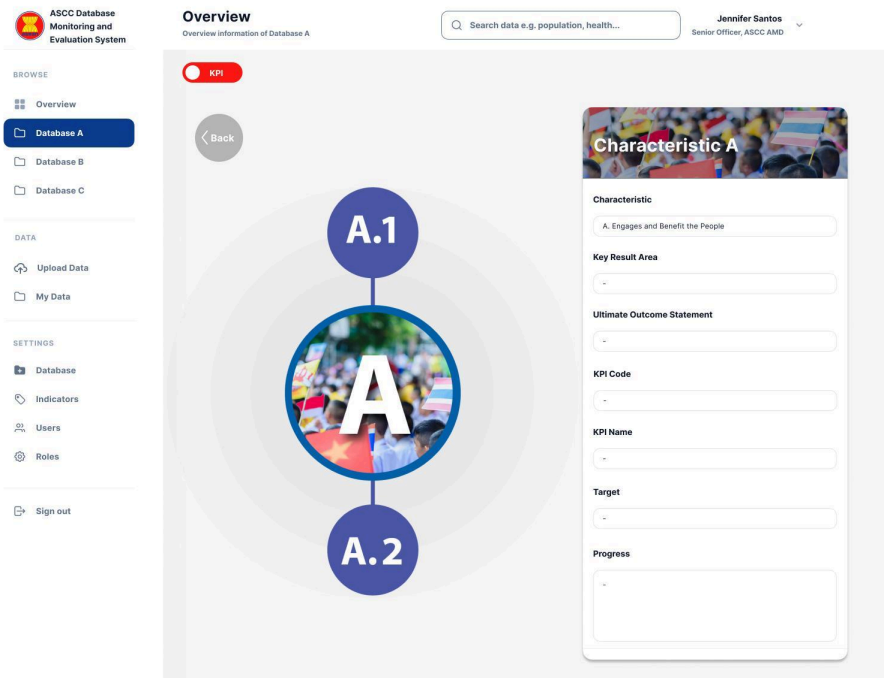
2. The Overview Database A - ASCC Initiatives page will appear, and the next click tab option of ASCC Blueprint Implementation.

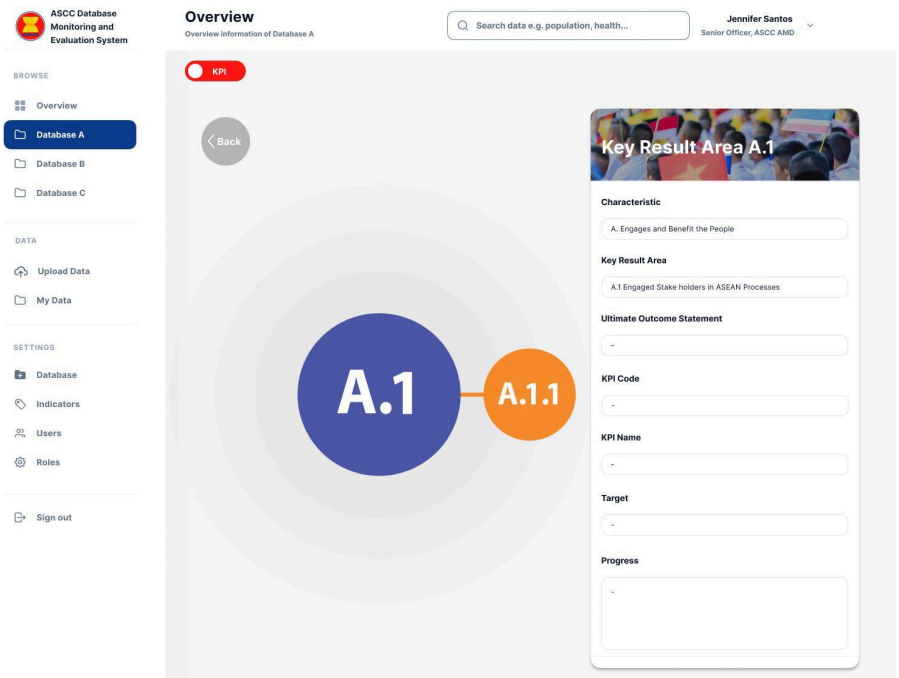
3. The Overview Database A - ASCC Blueprint Implementation page will appear, which consists of ASEAN symbol with five branches that representing the characteristic and element of ASCC Blueprint 2025.

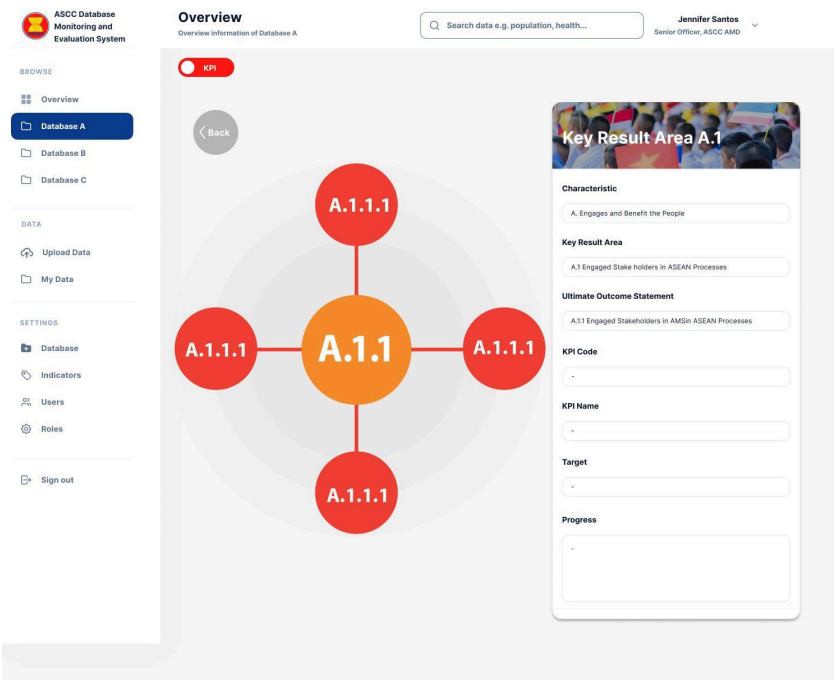


4. You can hover over each circle to see the details of each characteristic code in the table next to the chart. When you click one of the circles, the chart will change and display all key result areas within that characteristic.

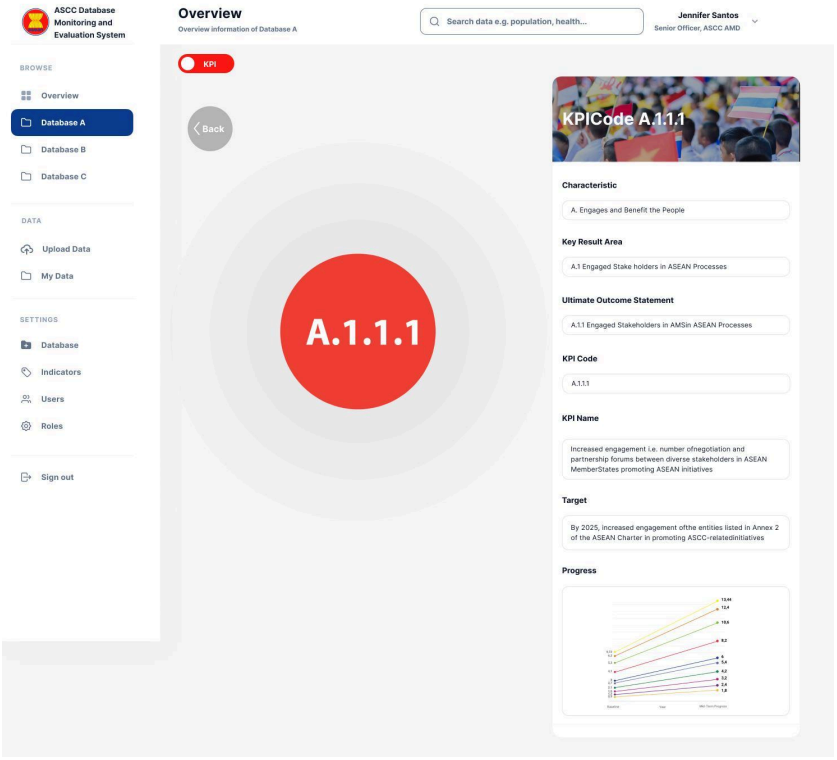
5. You can repeat the steps to search deeper. The order of data specifications is Characteristic → Key Result Area → Ultimate Outcome Statement → Key Performance Indicators





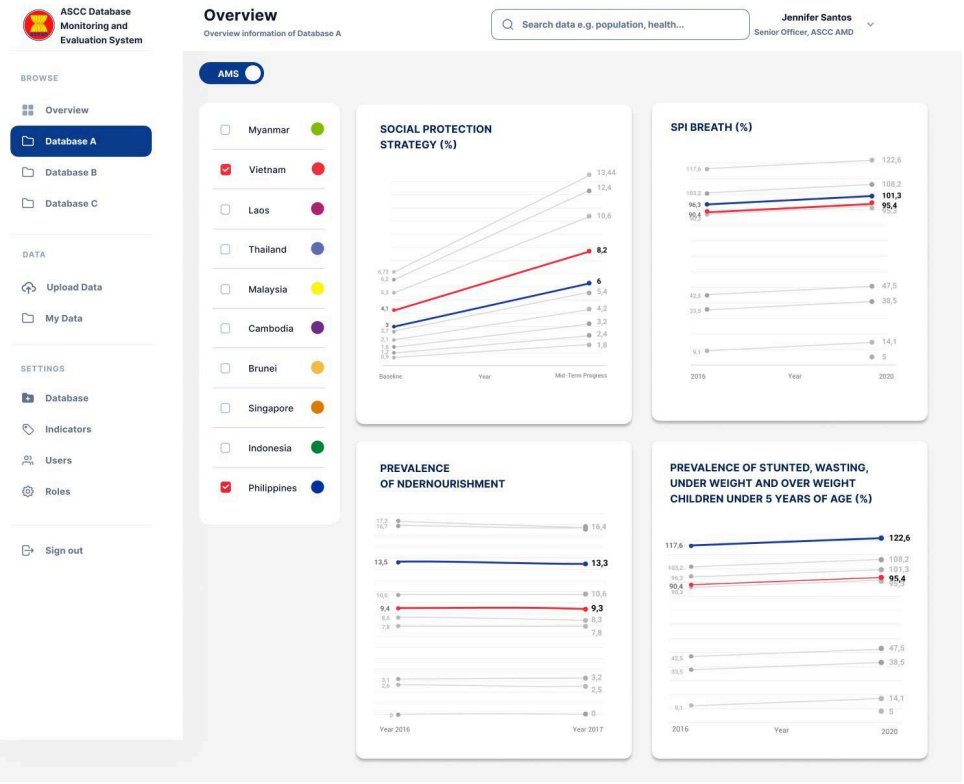


6. After arriving at the KPI page, a description of the KPI code will appear in the table along with the targets and progress of each indicator in chart form.



7. You can also see the progress of each AMS to achieve its KPI by pressing the switch button at the top of the chart.

8. When you click the button, it will switch to AMS mode and show all charts representing the progress of all KPIs from each AMS.

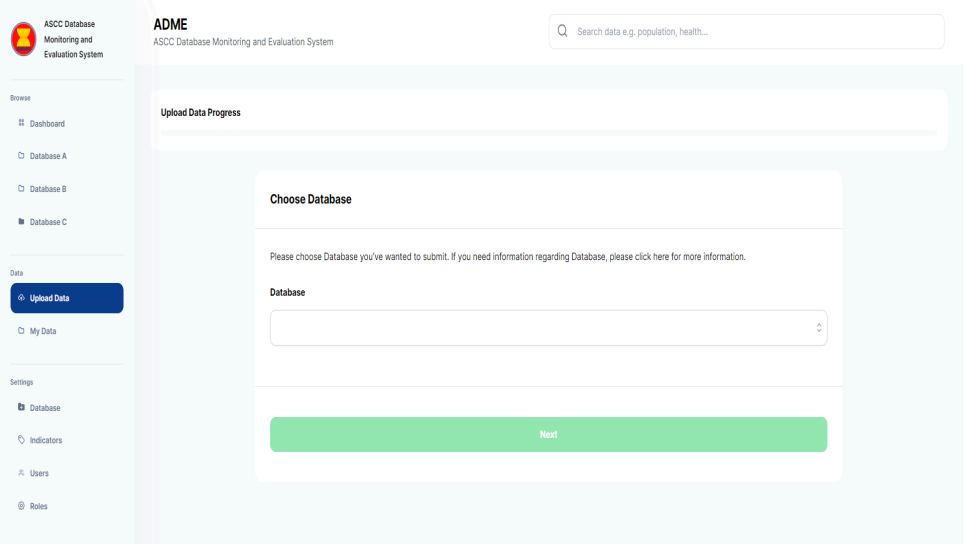


Updating Database (For Contributors)

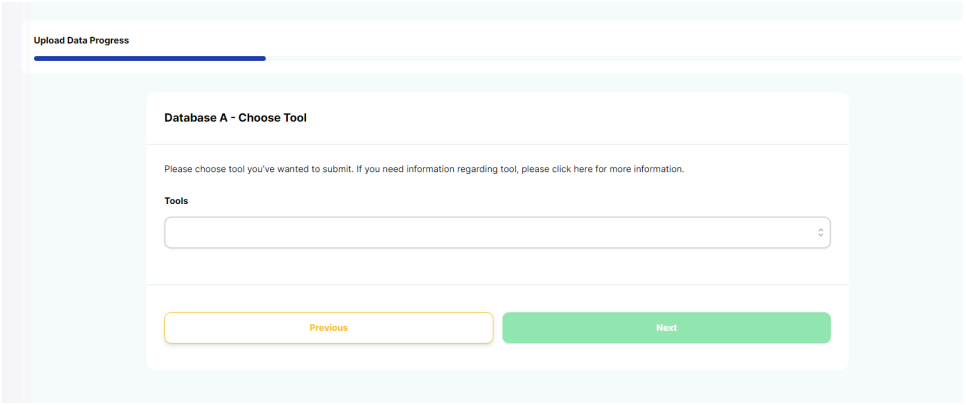
Add New Document

1. In the main menu on the right side of the homepage, select Upload Data.

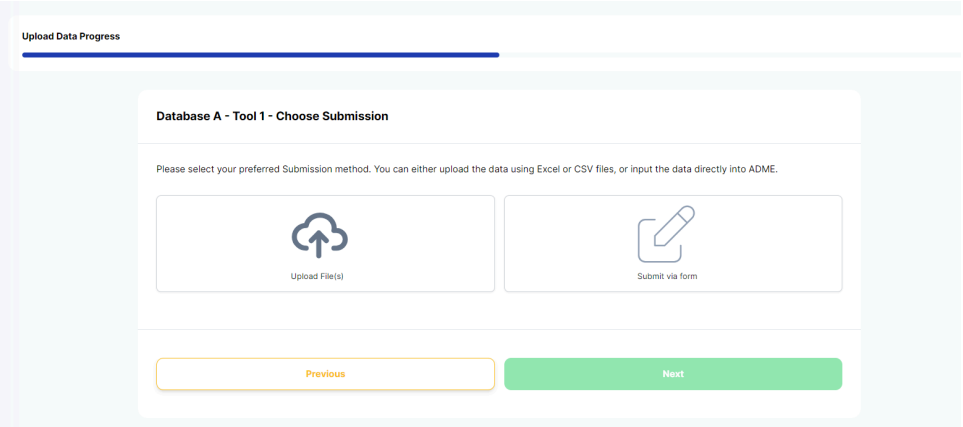
2. The Upload data page will appear. You can choose which Database you want to work on and click the Next button.



3. Next you can choose which tool you want to update. For example, in Database A, there are three options. The first one is for ASCC Sectoral Bodies' Implementation of the Sectoral Work Plans, the second one is for ASCC Monitoring Matrix of the Follow-up Actions to Declarations, and the last one is for ASCC Blueprint 2025 Results Framework Monitoring Database. After choosing the tools, you can click the "Next" button, or you can choose the previous button to go back to the database.

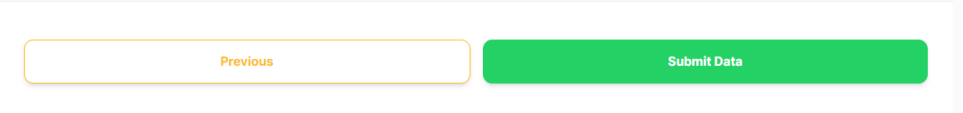


4. Then you have to choose the submission method. You can either upload the data using Excel or CSV files or input the data directly into the ADME System. After choosing the method, you can click the next button, or you can choose the previous button to go back to choosing the tool.

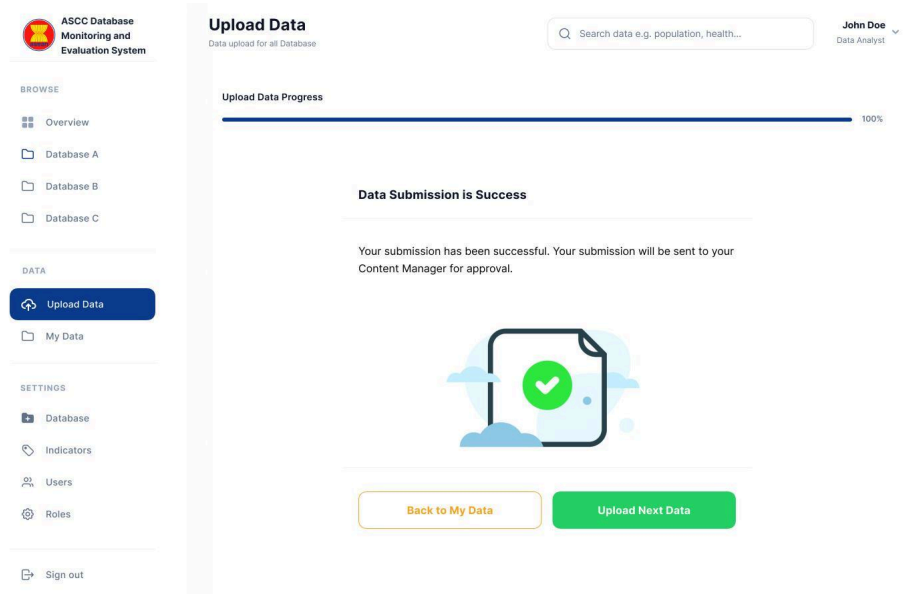


5. If you choose to submit via the form method, you will find an empty form for submitting a new document. The questions that appear on the filling sheet will vary depending on the data presented in each tool from each database.

6. After filling in the data related to the document following the directions on the filling sheet, you can click the Submit Data button to complete the upload process, or you can choose the previous button to go back choosing another method.

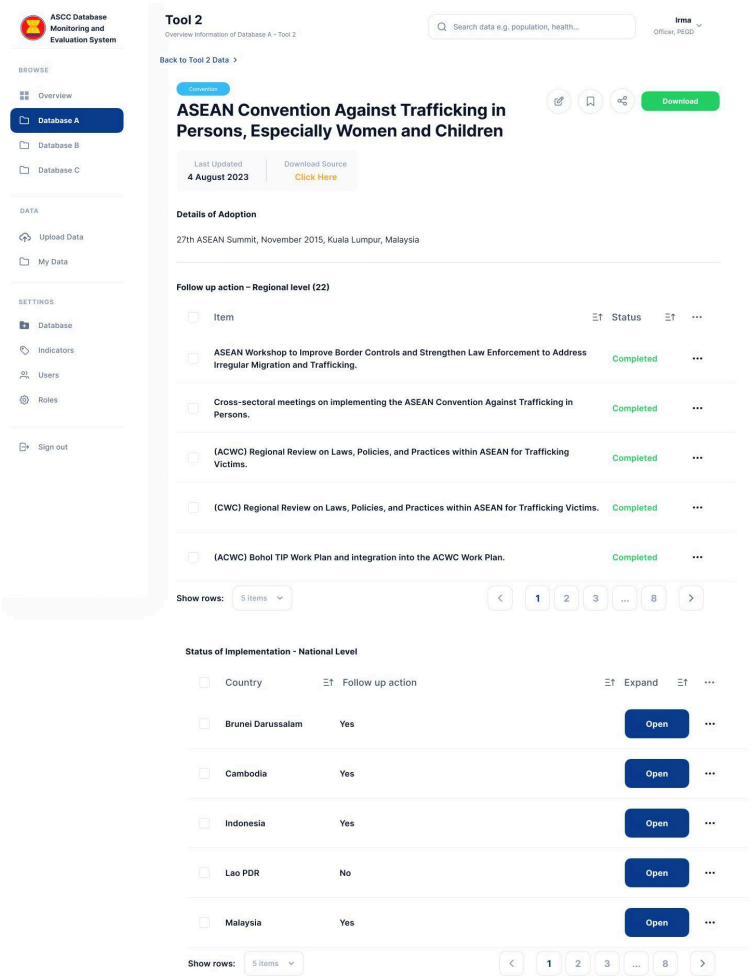


7. A pop-up notification will appear and show that you have successfully added a new document to the system and the document you submitted will be sent to the Content Manager for approval.



Update the Published Document

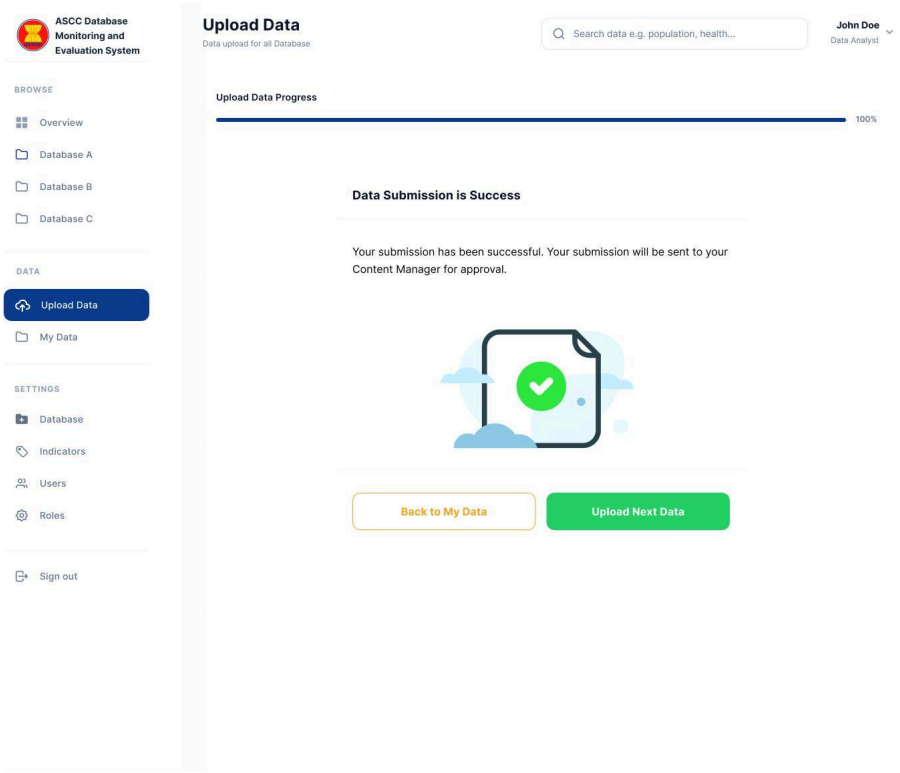
1. Open the document details page from Database A or C.



2. Press the edit button at the top of the page. This button will only appear if you have the role to edit the document.

3. The document edit page will open and you can update the data. Next, you can click the Submit Data button to submit the edited document, or you can choose the previous button to go back to the document details page and any changes you have made will not be saved.

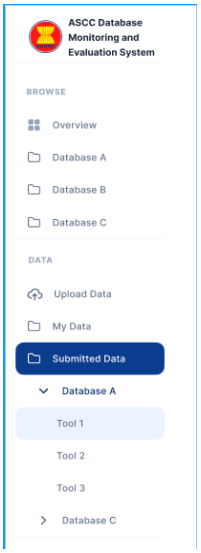
4. A pop-up notification will appear and show that you have successfully submitted the edited document. but for this updated version to be published still needs approval from the Content Manager.



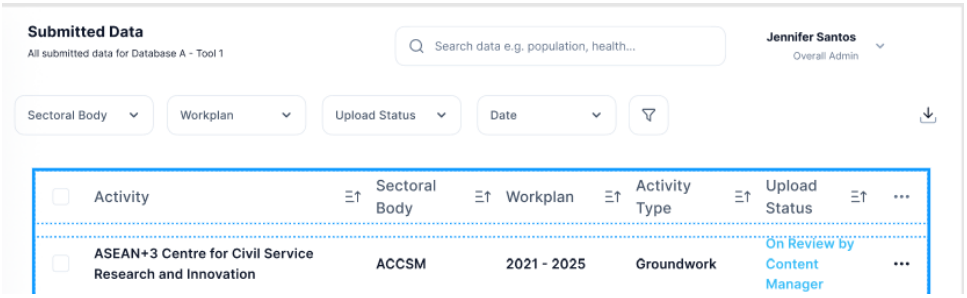
Verifying Database Updates (For Content Managers)

1. Content Managers check whether there are submitted documents from their Contributors that need to be accessed by checking the Submitted Data button from the main menu on the right side of the homepage.

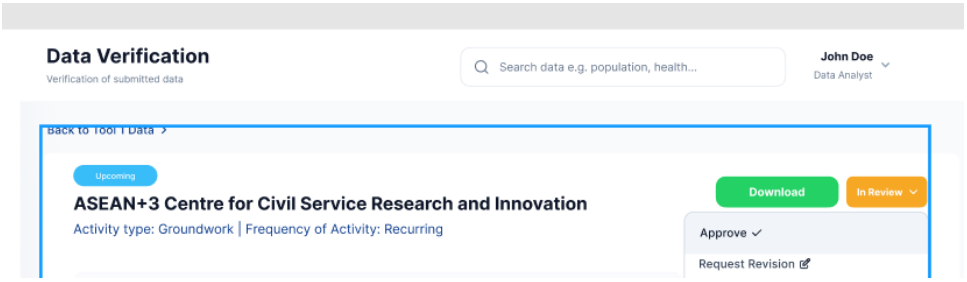
2. You can click the button and choose from which Database you want to check. Then the list of submitted documents from a specific database will be shown.



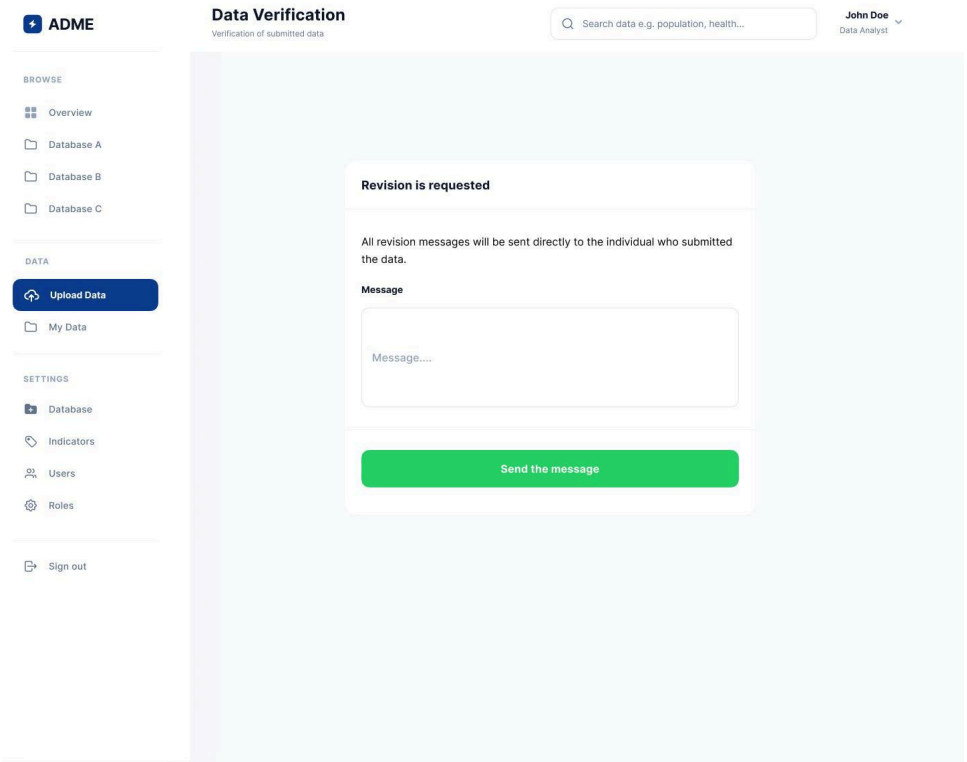
3. Choose one document that needs your approval, and click the action button (three dots button) from that document row.



4. The document details page will appear and you can verify the content of the document. After that you can choose to approve or request some revision for the document. If you approve it, the document will be sent to the Overall Admin for the verification process.



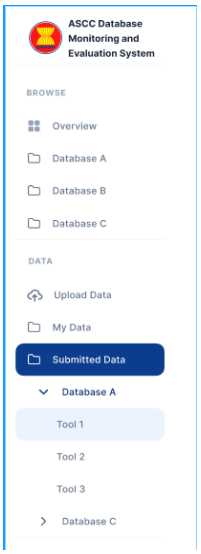
5. If you disapprove the document or request some revision from the contributor who made it, you must include the reasons for rejecting the submitted document and points that need to be revised before the contributor submits the document again. The document that needs to be revised, will be sent back to the contributor who made it.



Validating Database Updates (For Overall Admin)

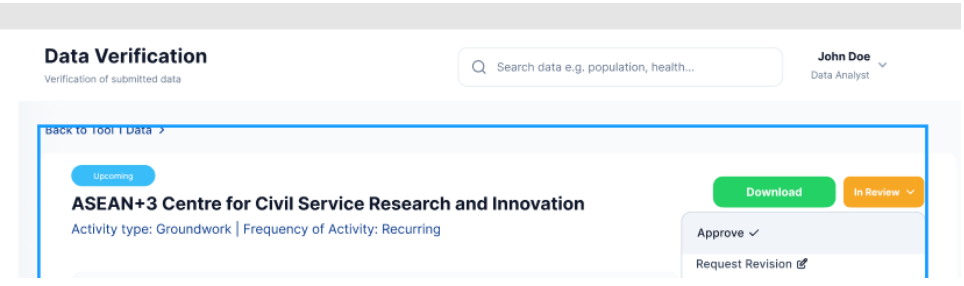
1. Overall Admin can check whether there are submitted documents that have already received approval from Content Managers and need Admin validation by checking the Submitted Data button from the main menu on the right side of the homepage.

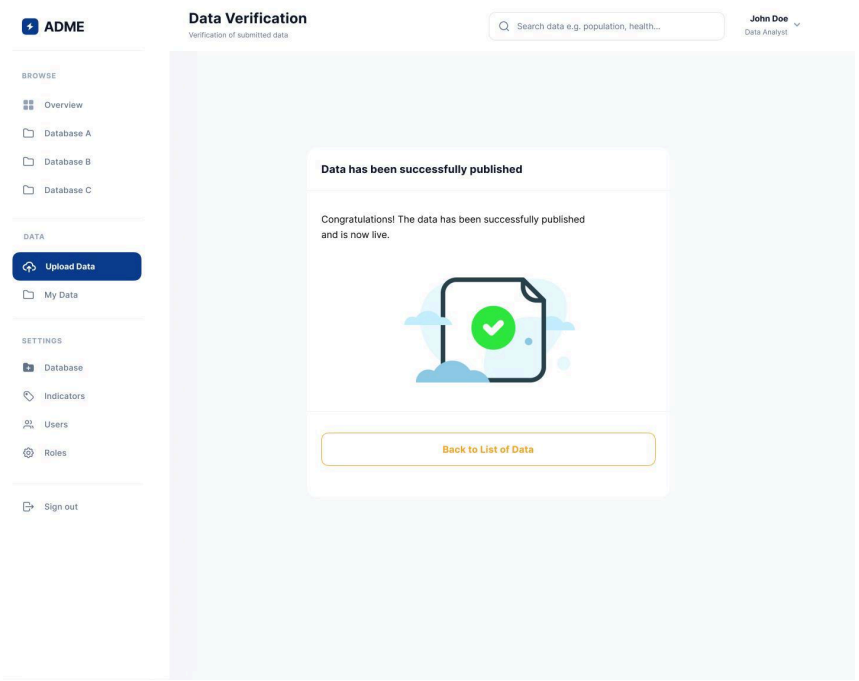
2. You can click the button and choose from which Database you want to check. Then the list of submitted documents from a specific database will be shown.



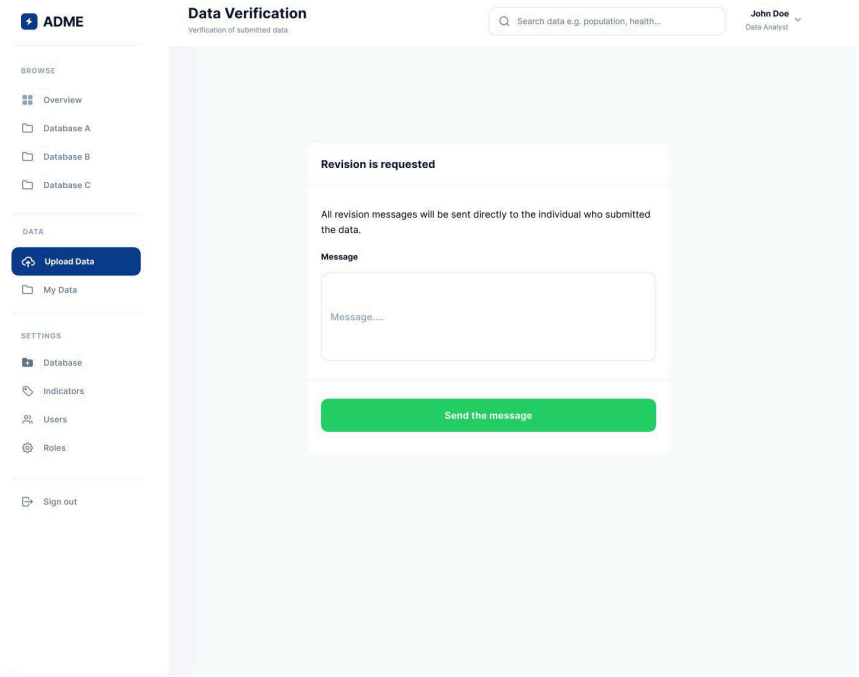
3. Choose one document that needs your approval, and click the action button (three dots button) from that document row.

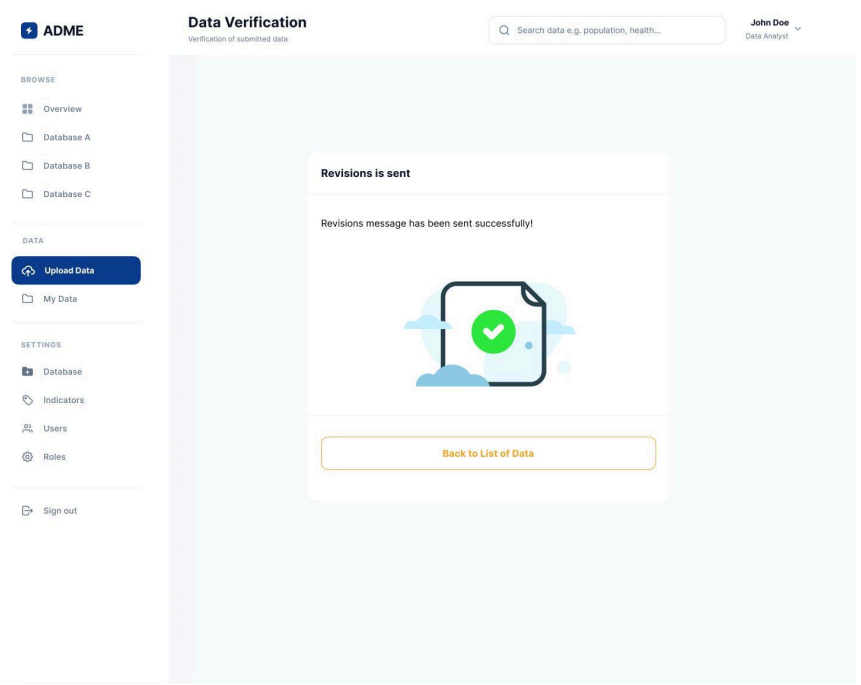
4. The document details page will appear and you can verify the content of the document. After that, you can choose to approve or request revisions for the document. If you approve it, the document will be published and you can set up anyone who can access the document.

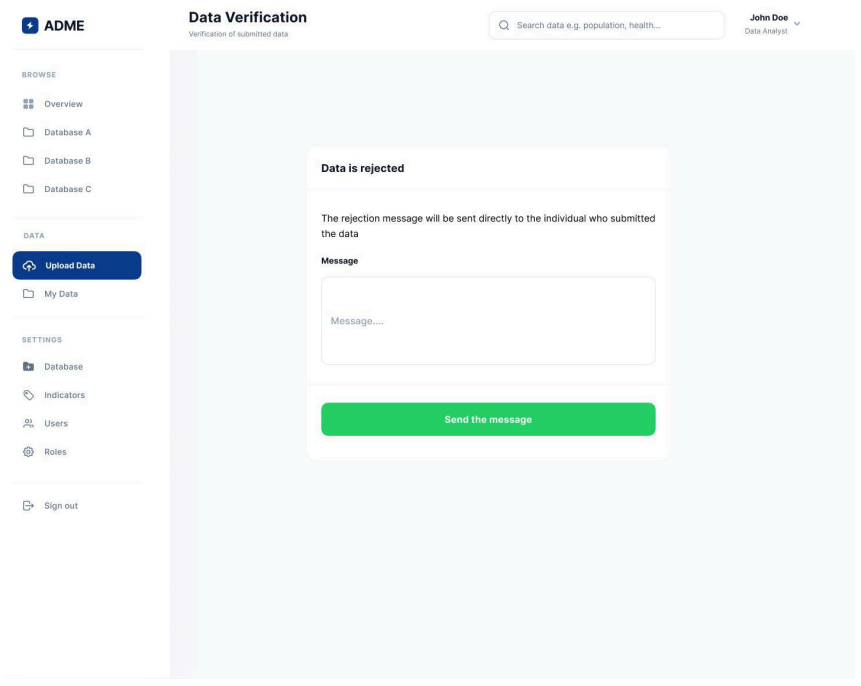


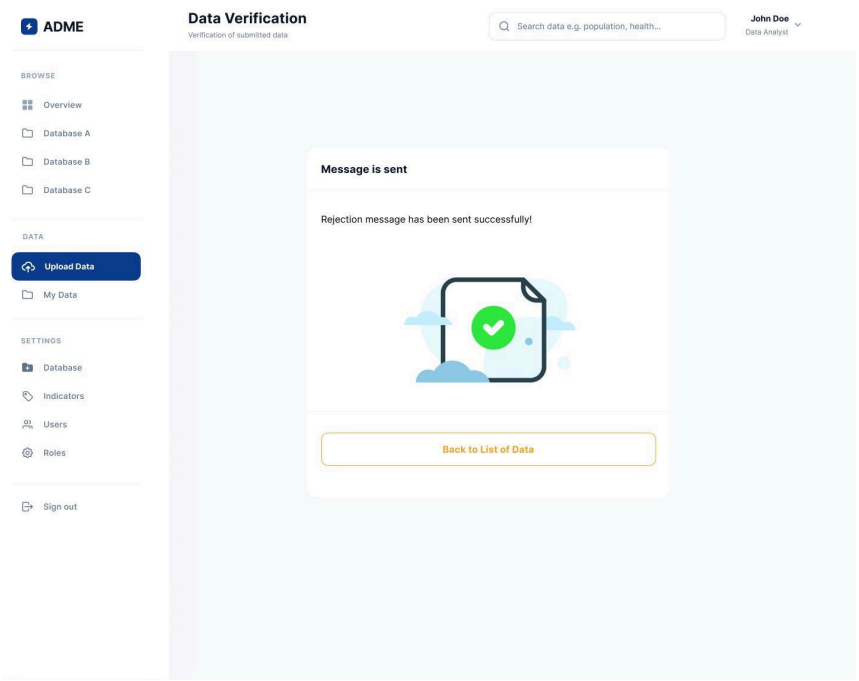


5. If you disapprove the document or request some revision, you must include the reasons for rejecting the submitted document and points that need to be revised before the maker submits the document again. The document that needs to be revised, will be sent back to the user who made it.




ADME
Data Verification
Verification of submitted data
Search data e.g. population, health...
John Doe
Data Analyst
BROWSE
Overview
Database A
Database B
Database C
DATA
Upload Data
My Data
SETTINGS
Database
Indicators
Users
Roles
Sign out
Revisions is sent
Revisions message has been sent successfully!
Back to List of Data


ADME
Data Verification
Verification of submitted data
Search data e.g. population, health...
John Doe
Data Analyst
BROWSE
Overview
Database A
Database B
Database C
DATA
Upload Data
My Data
SETTINGS
Database
Indicators
Users
Roles
Sign out
Data is rejected
The rejection message will be sent directly to the individual who submitted the data
Message
Message....
Send the message



6. Published documents can be seen by users who have access permission on the document database page, and data from the document will be combined with data from the same database tool whose status can be seen on the related database overview page.

Annex 1 - Open Web Application Security Project (OWASP) Checklist

Source: OWASP Web Application Security Testing Checklist

Information Gathering

- Manually explore the site
- Spider/crawl for missed or hidden content
- Check for files that expose content, such as robots.txt, sitemap.xml, .DS_Store Check the caches of major search engines for publicly accessible sites
- Check for differences in content based on User Agent (eg, Mobile sites, access as a Search engine Crawler)
- Perform Web Application Fingerprinting Identify technologies used
- Identify user roles
- Identify application entry points Identify client-side code
- Identify multiple versions/channels (e.g. web, mobile web, mobile app, web services) Identify co-hosted and related applications
- Identify all hostnames and ports Identify third-party hosted content

Configuration Management

- Check for commonly used application and administrative URLs Check for old, backup and unreferenced files
- Check HTTP methods supported and Cross Site Tracing (XST) Test file extensions handling
- Test for security HTTP headers (e.g. CSP, X-Frame-Options, HSTS) Test for policies (e.g. Flash, Silverlight, robots)
- Test for non-production data in live environment, and vice-versa Check for sensitive data in client-side code (e.g. API keys, credentials)

Secure Transmission

- Check SSL Version, Algorithms, Key length
- Check for Digital Certificate Validity (Duration, Signature and CN) Check credentials only delivered over HTTPS
- Check that the login form is delivered over HTTPS Check session tokens only delivered over HTTPS Check if HTTP Strict Transport Security (HSTS) in use

Authentication

- Test for user enumeration
- Test for authentication bypass
- Test for brute force protection
- Test password quality rules
- Test remember me functionality
- Test for autocomplete on password forms/input Test password reset and/or recovery
- Test password change process
- Test CAPTCHA
- Test multi factor authentication

- Test for logout functionality presence
- Test for cache management on HTTP (eg Pragma, Expires, Max-age) Test for default logins
- Test for user-accessible authentication history
- Test for out-of channel notification of account lockouts and successful password changes
- Test for consistent authentication across applications with shared authentication schema/SSO

Session Management

- Establish how session management is handled in the application (eg, tokens in cookies, token in URL) Check session tokens for cookie flags (httpOnly and secure)
- Check session cookie scope (path and domain) Check session cookie duration (expires and max-age) Check session termination after a maximum lifetime Check session termination after relative timeout Check session termination after logout
- Test to see if users can have multiple simultaneous sessions Test session cookies for randomness
- Confirm that new session tokens are issued on login, role change and logout
- Test for consistent session management across applications with shared session management Test for session puzzling
- Test for CSRF and clickjacking

Authorization

- Test for path traversal
- Test for bypassing authorization schema
- Test for vertical Access control problems (a.k.a. Privilege Escalation)
- Test for horizontal Access control problems (between two users at the same privilege level) Test for missing authorization

Data Validation

- Test for Reflected Cross Site Scripting
- Test for Stored Cross Site Scripting
- Test for DOM based Cross Site Scripting
- Test for Cross Site Flashing
- Test for HTML Injection
- Test for SQL Injection
- Test for LDAP Injection
- Test for ORM Injection
- Test for XML Injection
- Test for XXE Injection
- Test for SSI Injection
- Test for XPath Injection
- Test for XQuery Injection
- Test for IMAP/SMTP Injection
- Test for Code Injection
- Test for Expression Language Injection
- Test for Command Injection
- Test for Overflow (Stack, Heap and Integer)

- Test for incubated vulnerabilities
- Test for HTTP Splitting/Smuggling
- Test for HTTP Verb Tampering
- Test for Open Redirection
- Test for Local File Inclusion
- Test for Remote File Inclusion
- Compare client-side and server-side validation rules Test for NoSQL injection
- Test for HTTP parameter pollution Test for auto-binding
- Test for Mass Assignment
- Test for NULL/Invalid Session Cookie

Denial of Service
- Test for anti-automation
- Test for account lockout
- Test for HTTP protocol DoS
- Test for SQL wildcard DoS

Business Logic
- Test for feature misuse
- Test for lack of non-repudiation
- Test for trust relationships
- Test for integrity of data
- Test segregation of duties

Cryptography
- Check if data which should be encrypted is not
- Check for wrong algorithms usage depending on context Check for weak algorithms usage
- Check for proper use of salting Check for randomness functions

Risky Functionality - File Uploads
- Test that file size limits, upload frequency and total file counts are defined and are enforced
- Test that file contents match the defined file type
- Test that all file uploads have Anti-Virus scanning in-place.
- Test that unsafe filenames are sanitized
- Test that uploaded files are not directly accessible within the web root
- Test that uploaded files are not served on the same hostname/port
- Test that files and other media are integrated with the authentication and authorization schemas

HTML 5
- Test for Web Storage SQL injection Check CORS implementation Check Offline Web Application