Khalifa University of Science and Technology

**Continuous Auditing and Continuous Monitoring**

|  |  |
| --- | --- |
| Document | Solution Architecture Guidelines |
| Department | Internal Audit Department |
| Version | 1.0 |
| Document Reviewer | Internal Audit Team, Khalifa University |
| Document Approver | Internal Audit Director, Khalifa University |

**TABLE OF CONTENTS**

[1.0. PURPOSE AND SCOPE 3](#_Toc104929939)

[2.0. RESPONSIBILITY AND ACCOUNTABILITY 3](#_Toc104929940)

[3.0. SOLUTION ARCHITECTURE 4](#_Toc104929941)

[4.0. RISK CATEGORIZATION FOR CACM 5](#_Toc104929942)

[5.0. DATA MANAGEMENT 5](#_Toc104929943)

[6.0. SCRIPTING FOR CACM ANALYSIS 6](#_Toc104929944)

[7.0. DEPARTMENTAL VALIDATION 6](#_Toc104929945)

[8.0. DIGITAL REPORTING 6](#_Toc104929946)

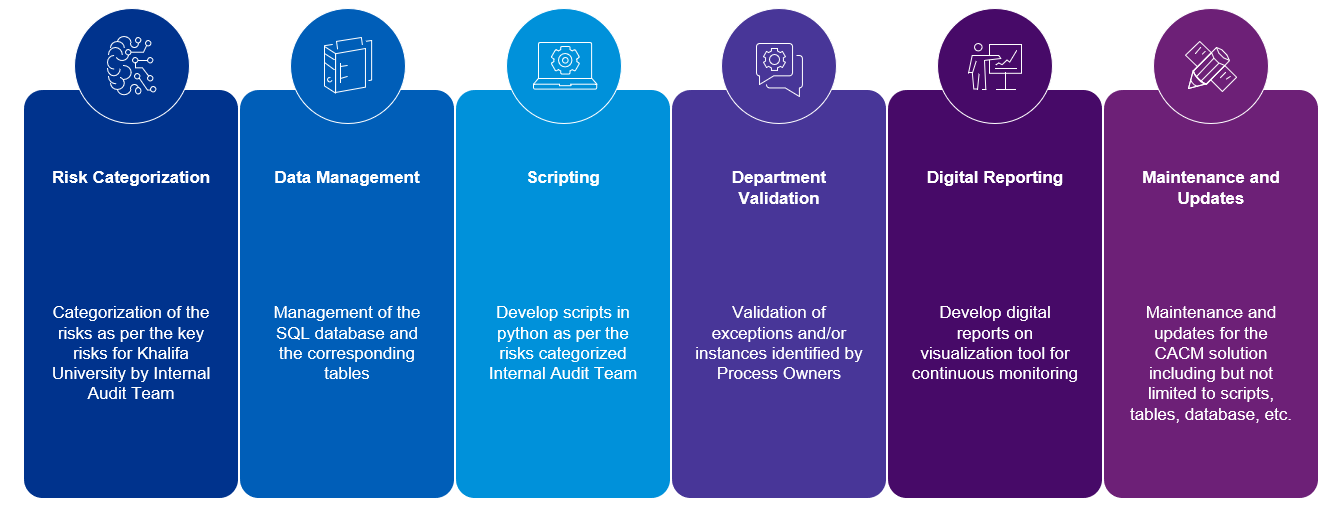
[9.0. MAINTENANCE AND UPDATES 7](#_Toc104929947)

[DEFINITIONS 8](#_Toc104929948)

# PURPOSE AND SCOPE

* 1. The purpose of this document is to provide guidance on the roles and responsibilities of the Process Owners, Internal Audit department, and Information Technology department at Khalifa University in regard to the deployment, management, and update of Continuous Auditing and Continuous Monitoring (CACM) solution deployed within Khalifa University. The oversight responsibilities include the following:
     1. effectiveness of the solution to identify and report the exceptions and/or instances identified;
     2. controls-in-place to ensure the data and solution is governed as per industry best-practices;
     3. compliance with local and regulatory requirements; and
     4. reporting protocols in-place to ensure exceptions and/or instances identified are notified, rectified and mitigated.
  2. The Internal Audit department must ensure the solution deployed is in collaboration of the Information Technology department to ensure adequate security measures and privilege user access management is maintained.

# RESPONSIBILITY AND ACCOUNTABILITY



* 1. **Database Management:** Database Management refers to the availability, scheduling, and maintenance of the SQL database within Khalifa University. Information Technology department is the owner of the SQL database within Khalifa University and is responsible for ensuring adequate controls and/or security measures are-in-place.
  2. **Risk Categorization:** Risk categorization refers to the categorization of the risks (Active Monitoring, Continuous Review, Periodic Monitoring, and No Major Concern) as High, Medium and/or Low based on the maturity of CACM implementation at Khalifa University. Internal Audit department is responsible for categorizing the risks based on the assessment of the implementation of CACM as per the availability, integrity, and quality of the data. Below are the details for risk categorization:
     1. High refers to the risks that can be automated based on the data availability, integrity, and quality as per the initial assessment;
     2. Medium refers to the risks that can be automated based on enhancements to the availability, integrity and/or quality of data as per initial assessment and recommendation to the Information Technology department and/or Process Owners;
     3. Low refers to the risks that can be automated based on significant enhancements to the availability, integrity, and/or quality of data as per the initial assessment to the Information Technology department and Process Owners.
  3. **Scripting:** Scripting refers to the development of the scripts (python, R and/or as per the Internal Audit team assessment of scripting language) to identify exceptions and/or instances of non-compliance to Khalifa University’s governance documents, policies, procedures and/or guidelines. The Internal Audit department is responsible for developing, managing, updating, and maintaining the scripts.
  4. **Department Validation:** Department validation refers to the validation of the exceptions and/or instances identified by the Process Owners through the implementation of the scripts. Process Owners of the risks (based on the risk categorization) are responsible for validating the exceptions and/or instances. Further, Process Owners must provide mitigation action plans and/or justifications for validated exceptions and/or instances.
  5. **Digital Reporting:** Digital reporting refers to developing the digital reports in data visualization software (PowerBI, Tableau, etc.) as per the Internal Audit department tool assessment. Internal Audit department is responsible for collaborating with the Information Technology department to ensure compliance with UAE’s GDPR requirements on the implementation of data visualization software which may require cloud support.
  6. **Maintenance and Updates:** Internal Audit department are responsible for collaborating with the Information Technology department to maintain the SQL database and corresponding tables required to maintain the scripts. Information Technology department is responsible for maintaining the privilege user access management and data integrity and/or quality for the SQL database in collaboration with the Internal Audit department.

# SOLUTION ARCHITECTURE



* 1. The solution architecture at Khalifa University is managed by the Internal Audit department in collaboration with the Information Technology department.

# RISK CATEGORIZATION FOR CACM

* 1. Internal Audit department at Khalifa University conducts a Risk Assessment exercise for all departments to identify the key risks in alignment with the business plan and objectives of the organization.
  2. All risks identified as part of the Risk Assessment exercise are tested against controls-in-place to estimate the residual risk rating as Active Management, Continuous Review, Periodic Monitoring, and No Major Concern.
  3. As part of the deployment of Continuous Auditing and Continuous Monitoring, the Internal Audit department identified the key risks that can be automated based on the residual risk rating and data availability.
  4. Each risk identified for automation is categorized as follows:
     1. High refers to the risks that can be automated based on the data availability, integrity, and quality as per the initial assessment;
     2. Medium refers to the risks that can be automated based on enhancements to the availability, integrity and/or quality of data as per initial assessment and recommendation to the Information Technology department and/or Process Owners;
     3. Low refers to the risks that can be automated based on significant enhancements to the availability, integrity, and/or quality of data as per the initial assessment to the Information Technology department and Process Owners.
  5. On finalization of the risks, the Internal Audit department requests the Information Technology department to access the relevant data to identify the Data Management requirements.

# DATA MANAGEMENT

* 1. The Information Technology department manages all data within Khalifa University at Khalifa University through SQL database management.
  2. Information Technology department provides the Internal Audit department access to the data through a separate CACM database instance created for the Internal Audit department.
  3. Internal Audit department requests the Information Technology department to provide access to the CACM database for relevant personnel through the user access management established within Khalifa University.
  4. Based on the authorized approval as per the user access management, the Information Technology department creates a user id for the Internal Audit personnel, through which the data can be accessed.
  5. In addition, the Information Technology department created tables within the CACM database for the Internal Audit department based on the requirements of the Internal Audit department.
  6. All users with authorized access can connect to the SQL database and extract information as required through SQL Management Tool via a server connection.
  7. Below are the details of the CACM database and the available data sources:

|  |  |
| --- | --- |
| CACM database (server connection) | PRDSQL16BADBE.kunet.ae |
| **Tables available in the CACM database** | |
| df\_AP\_invoices | Information related to the invoices at Khalifa University |
| df\_AP\_employee\_bank\_details | Information related to employee bank details, including IBAN |
| df\_AP\_employee\_leaves | Information related to employee leaves, including sick, unpaid, annual leaves, etc. |
| df\_AP\_employee\_master | Information related to an employee, including department, designation, contract, etc. |
| df\_AP\_it\_tickets | Information related to IT incidents and closure, including students related tickets |
| df\_AP\_POs | Information related to purchase orders, including the value of purchase order |
| df\_AP\_PRs | Information related to purchase requests, including quantity ordered |
| df\_AP\_student\_attendance | Information related to student attendance across courses |
| df\_AP\_student\_courses | Information related to student courses registered in each semester |
| df\_AP\_student\_master | Information related to students, including high school information, IELTS, EmSAT, etc. |
| df\_AP\_supplier\_master | Information related to vendors, including vendor address, TRN, etc. |

* 1. On finalizing the data requirements, the Internal Audit department identified the scripting language to be utilized to develop the scripts for exception analysis.

# SCRIPTING FOR CACM ANALYSIS

* 1. Internal Audit department deployed Jupyter Notebook in Khalifa University to utilize the Python language for developing scripts. Below are the details for Jupyter Notebook and Python:
     1. **Jupyter Notebook** refers to a web-based interactive development environment for notebooks, code, and data. Its flexible interface allows users to configure and arrange workflows in data science, scientific computing, computational journalism, and machine learning.
     2. **Python** refers to a computer programming language often used to build software, automate tasks, and conduct data analysis. Python is a general-purpose language, meaning it can be used to create a variety of different programs and is not specialized for any specific problems.
  2. Based on the risks identified and the data extracted from the SQL database, the scripts are scheduled and automated to run a batch process to identify the exceptions and/or instances of non-compliance to Khalifa University’s governance documents, policies, procedures and/or guidelines.
  3. Exception and/or instance log created for each risk is written back into the SQL database to create a digital report of the exceptions and/or instances on re-iteration of the script.

# DEPARTMENTAL VALIDATION

* 1. Internal Audit department is responsible for sharing the exceptions and/or instances identified as part of the scripting exercise with the Process Owners of the respective department (if applicable).
  2. Process Owners are responsible for providing feedback to the Internal Audit department on the accuracy of the exceptions and/or instances identified. In the case of false-positives, the Internal Audit department shall edit and update the relevant script to ensure the accuracy of the exceptions and/or instances.
  3. In addition, on validation of the exceptions and/or instances, the Process Owners shall provide the mitigation action plan to the Internal Audit department, including but not limited to, the management action plan, responsible owner, and date of the mitigation action.
  4. On verification of the exceptions and/or instances from the Process Owners, the Internal Audit department shall develop the digital report on a data visualization software as available within Khalifa University.

# DIGITAL REPORTING

* 1. Internal Audit department collaborated with the Information Technology department to identify a data visualization software to develop the digital reports at Khalifa University in line with the UAE GDPR requirements.
  2. Information Technology department is responsible for implementing the Microsoft PowerBI solution within Khalifa University and ensuring compliance with UAE GDPR requirements. In addition, Information Technology department provide the software to all relevant departments within Khalifa University including Internal Audit department and is responsible to maintain, update, and patch the software as required.
  3. Internal Audit department utilize the exception and/or instance log written in to the SQL database to develop the automated digital report.
  4. The report is circulated to the Senior Management and Audit & Risk Committee within Khalifa University for inputs and continuous monitoring.
  5. Further, Internal Audit department identify the frequency to run the scripts based on Khalifa University’s policies, procedures and guidelines to continuous monitor the exception and/or instance log generated.

# MAINTENANCE AND UPDATES

* 1. Information Technology department is responsible for maintaining and updating the SQL database as per the Internal Audit department directives.
  2. Internal Audit department is responsible for maintaining and updating the scripts and digital reports for the risks automated within Khalifa University for CACM.
  3. In addition, Internal Audit department is responsible for maintaining and updating any additional risks automated for CACM in collaboration with the Information Technology department in case any additional user access or data is required for scripting purposes.

# DEFINITIONS

Below are key definitions as part of the document:

**Active Monitoring** refers to the highest risk rating for risks that require active monitoring due to the high residual risk rating based on the key controls-in-place and/or the risk impact.

**Continuous Auditing and Continuous Monitoring** refers to the solution deployed at Khalifa University to continuous audit and monitor the key risks automated using database management techniques, scripting and data visualization software

**Continuous Review** refers to the risk rating for risks that require continuous monitoring due to the residual risk rating based on the key controls-in-place and/or the risk impact.

**Database** refers to the collection of tables, for e.g., student table contains student name, student personal details, high school details, high school grade, English grade, course details, program details, etc. Multiple tables in correlation refers to a database.

**Data Integrity** refers to the completeness of the table within a database.

**Data Quality** refers to the accuracy of the table within a database.

**Data Visualization** refers to the depiction of the data through visual graphs, tables and/or dashboards.

**ERP** refers to a type of software that organizations use to manage day-to-day business activities such as accounting, procurement, project management, risk management and compliance, and supply chain operations.

**GDPR** refers to General Data Protection Regulation which is enacted by the government within a jurisdiction. Khalifa University is a federal entity and is subject to the UAE GDPR regulation compliance.

**Information Technology** refers to the Information Technology department responsible for the maintenance of IT assets, software, ERP, etc. solutions within Khalifa University.

**Internal Audit** refers to the Internal Audit department responsible to ensure adequate controls are-in-place to mitigate the risks applicable to Khalifa University.

**No Major Concern** refers to the risk rating for risks that require low monitoring due to the residual risk rating based on the key controls-in-place and/or the risk impact.

**Periodic Monitoring** refers to the risk rating for risks that require periodic monitoring due to the residual risk rating based on the key controls-in-place and/or the risk impact.

**Process Owners** refers to the relevant personnel within a department responsible for the risk and/or process.

**Python** refers to a computer programming language often used to build software, automate tasks, and conduct data analysis. Python is a general-purpose language, meaning it can be used to create a variety of different programs and is not specialized for any specific problems.

**R** refers to a programming language for statistical computing and graphics supported by the R Core Team and the R Foundation for Statistical Computing.

**Risk Assessment** refers to a process to identify potential hazards and analyze what could happen if a hazard occurs

**Scripting** refers to a process that employs a high-level construct to interpret and execute one command at a time.

**SQL database** refers to a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.