# INTERNAL CONTROL MANUAL

| | | |
|---|---|---|
| **AUTHOR(S)** | : | Grégoire Le Mouël |
| **DOCUMENT REFERENCE** | : | 0000032 |
| **VERSION** | : | 1.2 |
| **STATUS** | : | Final |
| **SOURCE** | : | Atos |
| **DOCUMENT DATE** | : | 28 March 2022 |
| **NUMBER OF PAGES** | : | 28 |
| **OWNER** | : | Eric de l'Escalopier |

| Role | Approval |
|---|---|
| Approvers | Daniela Kirschberger |
| Quality Assurance Function | Marianna Bojarska |
| Document Owner Senior Manager | Eric de l'Escalopier |

# Contents

# List of changes

| version | Date | Description | Author(s) |
|---|---|---|---|
| 1.0 | 05/08/2020 | First version | Grégoire LE MOUËL<br>Daniela KIRSCHBERGER |
| 1.1 | 28/09/2020 | Format changes. Add-ons | Daniela Kirschberger |
| 1.2 | 28/02/2022 | Reflect updates of the Book of Internal Control structure and Org. updates<br>Quality assurance | Daniela Kirschberger<br><br>Marianna Bojarska |

# Target readers, communication method

| Target group | Distribution / publication method |
|---|---|
| All Atos Group employees | Published on Group Internal Control Public SharePoint + part of the newsletter when publishing the BIC |
| Internal Control community | Training session and shared in the Circuit Internal Control community |
| New Joiner in the Internal Control community | In the on-boarding pack |

# Terms and abbreviations

All Terms & Abbreviations are available on the SP list, please refer to them.

| Terms / Abbreviations | Description |
|---|---|
| ARCOS | Atos Risk and Compliance System |
| BIC | Book of Internal Control |
| CAP Team | Continuous Assurance Program Team (ensures testing of ITCF controls that are part of the BIC) |
| COSO | Committee of Sponsoring Organizations of the Treadway Commission<br>It provides frameworks and guidance on enterprise risk management, internal control and fraud deterrence |
| GIA | Group Internal Audit |
| GIC | Group Internal Control |
| RICC | Risk and Internal Control Coordinator |
| ICM | Internal Control Manager |

# 1 Introduction

Internal Control system is to help the group **properly and effectively achieving its objectives**. It is also a **legal requirement**, especially as Atos is a listed company, which could have severe consequences for the company if it is not correctly set and executed.
Indeed, non-compliance with legal standards could result in:

- Legal impact (criminal court - fines and imprisonment)
- Reputational impact (national or international impact)
- Financial impact which can lead, in the worst case, to bankruptcy

Over the last years, internal control deficiencies were publicly shared by the medias, leading to scandals and putting an end to some companies' existence.



The Financial Markets Authority (AMF - regulator for French listed companies) has drawn up an internal control reference framework to comply with the 4th, 7th and 8th European directives to help listed companies in supervising or developing their internal control system.
Atos is committed to compliance with French regulation (so-called Loi de sécurité Financière or Financial Security Act) and follows the **AMF framework** (which refers to COSO and ISO 31000).

Furthermore Atos has established an Atos Integrated Management System, referred to as AIMS, that integrates all Atos Management Systems (QMS – Quality Management System, ISMS – Information Security Management System, ITSMS - IT Service Management System and EMS – Environmental Management System) into one complete framework and in accordance with relevant ISO requirements (ISO 9001, ISO 27001, ISO 20000-1 and ISO 14001, respectively) which are linked to the Book of Internal Control.

An Internal Control system is to ensure:

- Compliance with applicable laws and regulations;
- Application of instructions and directional guidelines set by General Management;

- Correct functioning of company's internal processes particularly those relative to the safeguarding of its assets;
- Reliability of (financial) information.
- mitigation of risk and reduction of the possible fraud


Internal controls must be integral to every aspect of business and must be built **INTO not onto** business processes.

## 1.1 Purpose of the document

This manual is written with aim to be read by **all Atos employees**, to give them a better comprehension of internal control purpose, its referred activities and to integrate them into the internal control system. Indeed, all Atos employees, whatever their mission, function or hierarchical position, must be aware of and apply internal control within their area of responsibility. Indeed, despite certain roles and missions defined within the internal control process, everyone is concerned. All, we must always be vigilant and keep a constant watch on evolutions.

This manual is also having a specific section on Internal Control methodology (section 3 & 4), which has been specifically written for the **Internal Control community** described in section 2.1.4.

The Internal Control Manual is complementary to the Internal Control Policy in that it provides guidance for the execution of the control monitoring.

This document will be reviewed at least every 2 years. Intermediate reviews can be done in case significant changes occur.

## 1.2 Applicability and Scope

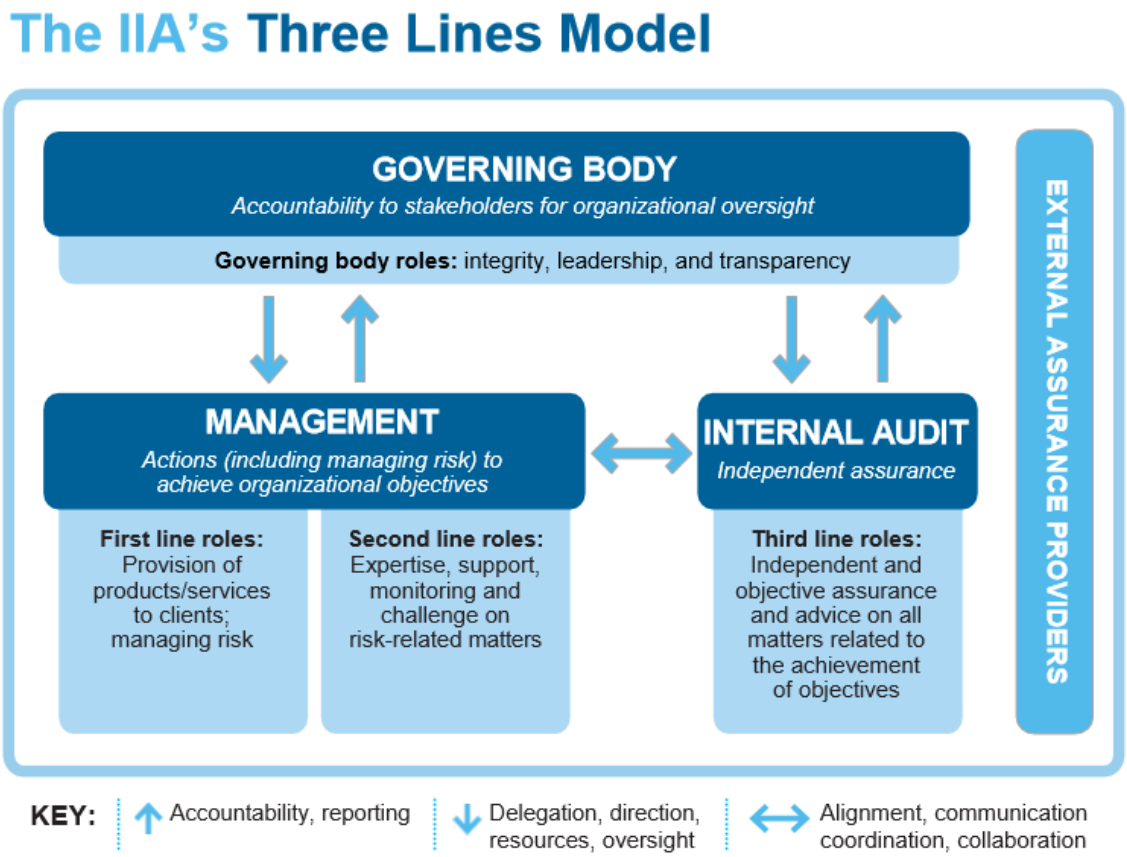
The Internal Control Manual applies to the entire group, i.e., all employees from all entities within the group. A specific focus is done on key internal control stakeholders (1st, 2nd, 3rd lines of defense) as described in the next section.

It applies to all Atos legal entities, taken into account obviously a transition period for entities which joined recently.

# 2 Roles and Responsibilities

## 2.1 Three lines model

Organizations need effective structures and processes to enable the achievement of objectives, while supporting strong governance and risk management. The Three lines model has been defined by The Institute of Internal Auditors (IIA). It clearly delineates roles and responsibilities of the governing body (The Board), as well as executive management/operational leaders, quality/compliance/risk experts and internal audit. These roles are not limited to risk management but focus on the overall governance of journey of the organization towards its objectives.




### 2.1.1 Process owners (part of the 1st line of Defense)

Process owners are the Heads of the Functions/Sub-Functions or the Operations within the Divisions/Industries. Each process owner **must** design an appropriate Internal control system for the process he/she is in charge of, by:

- Assessing the risks that may impact the process (what could go wrong);
- Designing appropriate controls, whether manual (integrated in operational procedures) or automated (embedded in IT tools);
- Enforcing those controls throughout the organization;

- Assessing the compliance of the process (spot checks) with defined principles and monitoring of remediation actions to close potential discrepancies.

Group Process Owners share their perception of risks, define controls and assess efficiency with Group Internal control to allow the consolidation and synchronization between processes and reporting to management.

### 2.1.2 Functional/Operational managers (part of the 1st line of Defense)

It is a primary responsibility of each Functional / Operational manager to ensure proper internal control system is in place in his/her area of responsibility, based on what has been defined by the process owner. This means ensuring that:

- Expected controls are included in work instructions and local operating procedures;
- Potential (emerging) risks are raised and addressed by proportionate measures;
- Tasks and controls to be executed are clearly **defined and assigned** to the relevant person, and ensure that he/she have sufficient knowledge to understand and perform the controls;
- Tools are set up to provide expected level of automated controls;
- Controls are properly formalized and supervised;
- Spot Checks are performed to ensure correct execution and if not, corrective actions are implemented in due time
- Deficiencies are timely reported to upper level of management;

Those duties are cascaded **throughout all levels of management**.

### 2.1.3 Group Internal Control (part of the 2nd line of Defense)

Group Internal Control is responsible for defining the tools and the methodology for Internal Control activities i.e. the maintenance of the Book of Internal Control (refer to section 2.2 for more details), and its monitoring (refer to section 3 BIC for more details). Group Internal Control must also report to management on Internal Control activities and alert the management in case of deficiencies.

Group Internal Control is the central pillar of the Internal Control system as it coordinates Internal Control activities between the 1st line, the other stakeholders of the 2nd line, the 3rd line of defense and the external regulators.

### 2.1.4 The Internal Control Manager (ICM) / The Risk and Internal Control Coordinator (RICC) – (part of the 2nd line of Defense)

An Internal Control Manager (ICM – dedicated position in Quality, Risk, Compliance, Internal Control areas) or Risk and Internal Control Coordinator (RICC – not dedicated position) should be appointed in each Global Support Function and Business Lines. Their appointment is managed in close collaboration with Group Internal Control. Some additional relays (local ICM/local RICC) may be appointed at regional level (e.g. Finance, HR).
The ICM / RICC is:

- Driving the function input (strong collaboration with the process owners) into the development and updating of the Book of Internal Control, standard processes, policies & procedures in line with any applicable re-organizations and changes (e.g. process improvements, offshoring, acquisitions).
- Playing an active part in the implementation of key controls (Book of Internal Control) and standard processes as well as increasing the control maturity level in close collaboration with the Process Owners. This means to organize training/support sessions and closely work with the 1st line of defense.

- Assessing the maturity of the control environment through control testing / Self-assessment campaigns launched by Group Internal Control and defining corrective actions with the management for any deficiencies observed (monitoring if failures).
- Assisting audits (internal & external) and follow-up remediation actions.

Global ICMs/RICCs are working in close cooperation with Global process owners and Group Internal Control. Local ICMs/RICCs are cascading group processes, if needed adapting Group practices to local context and provide bottom-up feedback on local activities.

### 2.1.5 Business assurance functions (part of the 2nd line of Defense)

In addition to Internal Control, several other business assurance functions (including Quality, Compliance, Security, Risk Management, Legal and Controlling) contribute to the Internal Control System by supporting operational/Functional managers and process owners notably for:

- Identifying and assessing risks in their respective areas of expertise (e.g. ISO requirements)
- Designing risk mitigation measures,
- Monitoring the effectiveness and efficiency of processes and controls in their specific domains.

A close coordination between the activities of Business Assurance Functions, as well as with Group Internal Control, is essential for the consistency of initiatives and efficient use of resources.

### 2.1.6 Group Internal Audit (GIA) – (3rd line of Defense)

Internal Audit provides an **independent** and ongoing evaluation of the internal control and supports operational management in the definition of action plans for continuously improving internal processes. Internal Audit operating principles are defined in the Group Internal Audit Charter, which is validated by Group Management. Audit reports are issued to the Atos Global Management. The Audit Committee also receives regular reports on the Internal Audit work plan, objectives of assignments, and associated results and findings.

### 2.1.7 Board of directors supported by Audit Committee (governing bodies)

The Board of Directors prepares governance rules detailing the Board's role supported by its committees. Those committees play a key role to enlighten the Board as to the quality of the internal control system. In particular, the Audit Committee is informed of the content and the implementation of internal control procedures used to ensure the reliability and accuracy of financial information and stays informed about the proper implementation of the Internal Control System.

## 2.2 Book of Internal Control content

**The Book of Internal Control** is a **mandatory framework** that is listing the internal control activities that must be implemented throughout the group.

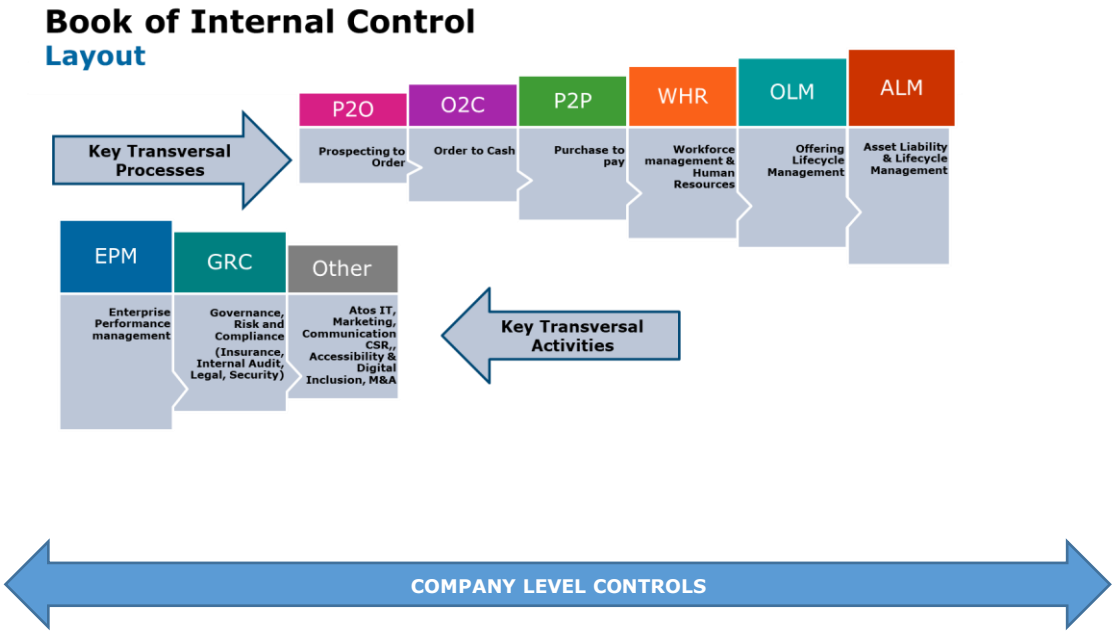
**Control activities** are found everywhere in the organization, at every level, and in every department. They include controls focusing on **prevention or detection** of errors and frauds, **manual or automated** controls, and controls built into the reporting structure.
In any event, control activities are determined in the light of the nature of the objectives with which they are associated and are proportionate to the underlying risks of each process.
The **formalization** of controls (and control evidences) is essential to allow management's monitoring and auditors' review. **Each process must be designed** to ensure the production and safeguarding of control evidences.
The **Book of Internal Control** (BIC) shared with all entities complements the different procedures by addressing the key control objectives of each process to achieve an adequate level of internal control.
Each **process owner is responsible for updating** the corresponding controls in the BIC (with the support of Group Internal Control), whenever the process changes or new risks arise.

The BIC is maintained by Group Internal Control who validates all changes. Any deviation should be fully justified and reported to the Global ICM / RICC in charge.

## 2.3 Book of Internal Control overview

The BIC is structured in three main categories:

- Company Level Controls
- Key Transversal Processes
- Key Transversal Activities




The **Company Level Controls (CLC)** encompass all control activities that are relevant across the organization and need to be applied in every Function/Business Line/entity.

The **Key Transversal Processes (KTP)** include:

- ***Prospecting to Order (P2O)***: it defines the establishment of Sales Strategy, the Governance, Marketing and the Business Enablers. It also outlines the management of Demand and opportunities as well as the Development of client business and of channel program operations.
- ***Order to Cash (O2C):*** it takes over from the Opportunity to Order process at the point when the customer has decided to buy goods and services from Atos. The process includes all the steps including validation of the order, arranging for the goods and services to be provided, providing the goods and services through to the point where the cash has been received following successful delivery. As the process includes the steps involved in delivery to the customer, all of the methods and processes involved in delivery relate to this key transversal process.
- ***Purchase to Pay (P2P):*** it provides visibility of the entire life cycle of a transaction from the way an item is ordered by Atos up to its payment and is booking providing full insight into cash-flow and financial commitments.
- ***Workforce Management & Human Resources (WHR):*** it defines the establishment of HR Strategy and plans as well as the management of recruitment, total reward, HR Operations (personnel administration, on/off boarding), workforce (foundation, capacity planning, mobility), employee development and engagement and finally the monitoring of HR Services.
- ***Offering Lifecycle Management (OLM):*** it refers to the handling of a good as it moves through the typical stages of its product life: identification, definition, realization, launch, growth, maturity/stability, and retirement.
- ***Asset Liability and Lifecycle Management (ALM):*** it is the set of business practices that join financial, contractual, and inventory functions to support asset and contract life-cycle management and strategic decision making for the IT environment. Assets include all elements of software and hardware that are found in the business environment. IT inventory management helps organizations manage their systems more effectively and saves time and money by avoiding unnecessary asset purchases and promoting the harvesting of existing resources. ALM is composed of processes that help with: § Redeployment from stock before new purchases are made § Data for assets/contracts is properly created and maintained.

For each process there is a **Global Process Owner** defined who is responsible for implementing the process and the embedded controls within the organization.

The **Key Transversal Activities (KTA)** are function related and represent activities and not a process. There are 3 KTAs and their sub-topics existing:

- **Enterprise Performance Management (EPM):** Activity embeds Financial processes, supported by control points to ensure financial figures are correct, prevent fraud and be efficient whatever the organization is. It includes Budget and Forecast, Business Expenses, Consolidation, Controlling & Reporting, General Finance & Accounting, Pensions, Tax Treasury
- **Governance, Risk and Compliance (GRC)** linked to Insurance, Internal Audit, Legal and Security
- **Other (OTH)** topics Communication, Marketing, Corporate Social Responsibility, Accessibility & Inclusion, Atos IT, Mergers & Acquisition

The BIC formalized the Key controls to be executed across the organization; however, **the starting point is always the policies and related procedures**. Policies and procedures contribute to an appropriate control environment: Main ones are gathered in the Book of Internal Policies and stored in a common repository (available on Group Quality Sharepoint).
Along with the centralization of the Group Policies, the "Atos IT-Enterprise Architecture team" focuses on creating an Atos Enterprise Architecture model, in coordination with the Atos IT-End to End Applications Towers teams, together with business process owners and the assurance functions (e.g. Internal Control, Quality, Security…). The Enterprise Architecture community, supported by

process analysts, is responsible for documenting existing and targeted business processes, including the supporting organization, KPIs, and internally and externally mandated compliance parameters.

## 2.4 Detailed structure of the BIC

BIC controls are described with the following fields (based on version 12, published in February 2022):

**Key data**:

- **Master Control ID**: Control unique reference number
- **KTP/KTA**: E2E process or Activities where the control is executed
- **Process/Sub-process**: Process/Sub-process where the control is performed
- **Risk type**: Risk embedded in risks frameworks (ERM, LRM, EvRM) – see section 2.6
- **Control Objective Description** (Get reasonable assurance that…): Key statement on a significant risk to be covered
- **Master Control Description** (how): Action (way to control) to address or mitigate the risk
- **Evidence** (what): Document formalizing the control performed
- **Operating Test Procedure**: Way to test the control effectiveness (performed by the 2nd/3rd lines of defense)
- **Frequency** (when): Periodicity of the control execution

**Governance:**

- **Execution zone:** Global/Local or outsourced control
- **Control Executor** (who): person or department in charge of performing the control
- **Control Owner** (who): person or department accountable to ensure the accuracy and effectiveness of the control
- **Type:** Functional or Operational control
- **Applicability:** Organization where the control is applicable (not considering the geographical dimension)

**Specificities:**

- **Current Related policy**: Atos policy name addressing the control objective
- **Link to the policy**
- **Atos Frameworks**: control part of a framework:
  - Internal Control Framework for all control under the Atos Group Internal Control accountability
  - IT Control Framework for delivery processes under RACG (Risk Audit and Compliance Governance Function within Business Lines) accountability
  - Closing file & Permanent File for Financial closing activity under Finance department accountability
- **Critical control[1]:** Priority control mitigating top risks in the process
- **Fraud control**: control related to the risk of fraud
- **Sustainability control**: control contributing to the achievement of Atos sustainability goal

[1] A **critical control** is differentiated from others in the sense that it cannot be compensated by other measures and that if it fails (i.e. it is not embedded in the process or not executed properly), it is highly unlikely that material errors will be prevented or timely detected. It therefore might impact directly company objectives through claims, reputational damage (fraud / misstatement) and financial losses.

- **Level of Automation**: 3 possible levels
    - Automate: there is no manual test/review, all is executed automatically
    - Semi-automated: part of the control is executed automatically but requires manual activity on top
    - Manual control: Control executed entirely manually
- **Control-ISO/COSO/SOC2 Mapping:** Mapping of the control with ISO standards (9001, 140001, 20000 and 27002), SOC2 framework and COSO principles

## 2.5 Benefits of the BIC (Why)?

Advantages of having the Book of Internal Control are:

- Helping **protect assets**, **people** and broadly the company
- **Reducing the possibility of fraud/corruption**
- Increasing **financial reliability** and integrity (accounts and financial statements)
- Ensuring **compliance with laws and regulations** (in particular AMF as Atos is a listed company on the French stock-exchanges)
- Ensuring compliance with internal processes and guidelines (homogeneous approach across the Group)
- Improving **efficiency** in Functions/ Operations
- Establishing **monitoring** procedures
- Supporting management to be able to **make sound decisions**
- Improved **risk-awareness** through uniform perception of risks and understanding for controls
- Enhancing **trust** of investors due to increased transparency, avoidance of loss of reputation and protection from the unexpected
- Enhancing security for the board of directors and management
- Increasing **quality** (and customer satisfaction)
- Enhancing **audit readiness** (internal and external)

## 2.6 When and how is the BIC communicated?

It is reviewed on a continuous basis and officially published on GIA and GIC public Sharepoint or twice a year if significant changes occur. It is communicated along with a release note including major changes to the Internal Control community and via Group Intranet (MyAtos News) to all employees. The ICMs / RICCs are then the relays for communication in their specific domain.

## 2.7 Risk Management impact on BIC

The Book of Internal Control is part of the Internal Control System which is related to the Risk Management activities (refer to the Atos Risk Policy more details). Those include a yearly **Enterprise Risk Management** (ERM) which is an integral part of Corporate Governance, focusing on the company's objectives, risks related and involves all levels of management. ERM exercise (see Enterprise Risk Management Framework and Approach document for more details) enables to identify and assess the strategic risks.

In parallel, other dedicated risk assessments using the ERM methodology are performed within departments such as in Legal and Compliance, Security, Environment, and Corporate Social Responsibility.

Those initiatives allow to identify and analyze Atos' main risks and to prioritize mitigation measures. **Implementation of controls** could be one of the measures; therefore, risk types are embedded into the Book of Internal Control (i.e. each control activity are associated to a risk type, to better understand the area of action of the control). Other's mitigation measures can be a transfer of the consequences (through insurance or equivalent) or an adaptation of the organizational structure.

# 3 BIC Monitoring

The Internal Control System requires on-going monitoring. The aim is to verify its relevance and appropriateness to the company's objectives.
The supervision of internal control, called 'monitoring' is required to:

- Measure the control effectiveness (design and/or operational) and the proper functioning of the process
- Check if controls are aligned with business and strategic objectives
- Highlight deviations requiring process/ BIC adaptation

Monitoring is:

- Primarily, the responsibility of each process owner (1st line of defense); he/she must monitor the effectiveness of the internal control activities on his/her process.
- Secondly, the responsibility of each manager (1st line of defense) who must supervise the proper execution of the controls and related processes for the area he/she is managing.
- Thirdly, the responsibility of the internal control organization (Group Internal Control, ICMs/RICCs, Business Assurance - 2nd line of defense). To do so, they are following 2 approaches:
  - **Control Testing** campaign: assessment of the execution of the controls through evidence based (generally sampling)
  - **Self-Assessment** campaign: assessment of the execution of the controls through the perception of the control owner
- Internal / External audits (3rd line of defense): mandated by Atos General Management or Regulators.

In addition, some indicators can measure directly or indirectly the effectiveness of controls, allowing for corrective actions when thresholds are not met.

## 3.1 Control Testing

Control Testing campaigns (BIC related) are launched by Group Internal Control. Other Business assurance functions are also conducted testing on some specific requirements (e.g., ISO, ITCF by CAP team).

Control testing is performed on a sample based according to a defined methodology described hereafter.

### 3.1.1 Information Produced by Entity (IPE)

According to COSO Principle 13: 'The organization obtains or generates and uses relevant, quality information to support the functioning of internal control.'
This means the information obtained need to be validated/verified if accurate and complete and is from a reliable source.

| Document category | Category description | Evidence | Verification |
|---|---|---|---|
| System generated (not editable) | Parameters (e.g. period covered or Business Units) need to be set in order to generate the document. The document is generated in a non-editable format (PDF for instance) | **Screenshot** showing the source of the document and the filters applied/parameters set to generate the report. Please make sure that the screenshot shows the date on which it was taken + obtain the name of the person who took the screenshot | Verify that the parameters entered were correct (i.e. the appropriate period/appropriate BU selected) |
| System generated (editable) | Parameters (e.g. period covered or Business Units) need to be set in order to generate the document. The document is generated in an editable format such as a spreadsheet | **Screenshot** showing the source of the document and the filters applied/parameters set to generate the report. Screenshot showing the number of lines contained in the document. Please make sure that the screenshot shows the date on which it was taken + obtain the name of the person who took the screenshot | Verify that the parameters entered were correct (i.e. the appropriate period/appropriate BU selected)<br><br>Verify that the number of lines contained in the document provided is the same as the one on screen |
| Non-system generated | The document is not generated by a system (file maintained manually) | Document explaining:<br>-document owner (responsible for maintaining the document)<br>-source of data: where do the data used to feed the document come from?<br>-document access: who can access the document? How (by what means)?<br>-document protection: is the document password protected? Is access to the document restricted and if so how?<br>-controls: what controls are performed to ensure that the document is complete and accurate? | Verify that controls are in place to ensure the completeness and accuracy of the document (verification on totals / check with source data performed by the Control Owner or a team member with sufficient knowledge |

### 3.1.2 Define the scope

Before launching the Control Testing campaign, the scope must be defined in terms of:

- Controls: Selection of the controls to be tested are decided based on e.g. the criticality of the risks related, the legal requirements, the specific situations that occurred and raising some doubts on the correct execution of controls.
- Applicability (Business Lines, Functions)
- Geographies (e.g. Global, RBUs, countries, legal entities, GDC)
- Period (e.g. last 12 months, last 6 months)

Definition of the scope is performed in collaboration with Global ICMs/RICCs. Process owners can be consulted as well as the Internal Audit to avoid overlaps. Exclusions of the scope requires a justification and must be documented accordingly.

### 3.1.3 Determine the population

The population of all 'events/occurrences' for the period in scope has to be determined. It is the pre-requisite to be able to select the samples.
For example:

- All closing files for the months January to June;
- All new contracts added into the tool for the period October to December;
- All Security Incidents that occurred in May.

The way how the population was determined must be documented (see IPE requirement) to ensure the population is accurate and complete.

### 3.1.4 Define the Sample size

The sample size is based on the control frequency (how often the control activity is executed) and need to be applied according to the following table:

| Control Frequency | Sample size (12 months coverage) | Sample size (6 months coverage) |
|---|---|---|
| Continuously | 2-15 | 2-10 |
| Daily | 10-15 | 10 |
| Weekly | 8 | 6 |
| Bi-weekly | 6 | 4 |
| Monthly | 4 | 3 |
| Quarterly | 2 | 2 |
| Semesterly | 2 | 1 |
| Yearly | 1 | 1 |
| Every 2 years | 1 | 1 |
| Every 3 years | 1 | 1 |
| On occurrence | 10% of the occurrences (not more than 15) | 10% of the occurrences (not more than 10) |

For controls that are fully automated (by system) the sample size is one.

### 3.1.5 Sample selection

The most independent way to select samples is to use a randomizer tool. For selecting your records, use a random number generator like www.random.org/integers.
Another option is the use of (non-statistical) judgmental sampling techniques to select the 'rule vs the exception' (e.g. regular vs post holidays dates, most common vs rare change, more frequent vs. less frequent, common vs. uncommon occurrences).

Note: It is important to document how the samples were selected (e.g. screenshot of the randomizer results) so that it is traceable for others (e.g. auditors).

### 3.1.6 Collecting evidences and Naming conventions

A listing of suggested evidences is available for each control activity in the Book of Internal Control (BIC). The suggested evidences help to achieve the control objective but are not limited to. All evidences should be saved in a standard repository or Arcos tool (see section 4 for more details).
In order to ensure traceability, the following naming convention is proposed:
Master Control ID_OTR ID_File name

### 3.1.7 Testing Results (conclusion and documentation)

After reviewing the evidences, a conclusion whether the control activity is effective or not need to be documented.
When writing a conclusion, it is important that the control activity was performed, and it is formally explained with corresponding evidences. It should include a reference to the evidences reviewed and a brief description of what has been reviewed and the results (effective or ineffective). It must be phrased in a comprehensive and traceable manner (Arcos tool) so that it can be understood by others (e.g. auditors).
IMPORTANT: If one part of the control fails (one test/item of the sample failed), the entire control fails and need to be rated as "ineffective".

### 3.1.8 Control deficiencies (findings)

In case a control is rated as 'not effective', it is a control deficiency (finding) and need to be addressed by the management concerned through an action plan and followed-up accordingly (ICM/RICC responsibility).
Corrective actions should be assigned to the proper action executor, risk level (high, medium, low) and a due date need to be agreed. Information related to corrective actions are traceable in the Arcos tool (see section 4 for more details)

| Risk Level | Definition |
|---|---|
| **High** | No evidence available<br>Failure of controls that could lead to a qualified opinion in external audit reports |
| **Medium** | (some) Evidences not available |
| **Low** | Documentation or Tooling error<br>(e.g document in draft or not approved, fields not filled according to process) |

### 3.1.9 Follow-up and reporting of control deficiencies (findings)

Action plans need to be followed-up by the responsible ICM/RICC and their closure status is reported to the Audit Committee and/or Atos Executive Board in due time by Group Internal Control.

The ownership of the closure of deviations is with the Action Executor. The Action Executor as owner of a deviation shall actively inform the ICM/RICC by providing:

1. Regular status updates
2. Comments describing planned and realized actions in detail,
3. Documents of evidence

It is recommended that the ICM/RICC provides regular reminders to the Action Executor to ensure that actions are closed by the agreed target date.

### 3.1.10 Closure of control deficiencies (findings)

The closure of an action plan must be authorized by the FICM/RICC.
At this point he must verify that the actions taken are sufficient to close the deviation.

All action plans should be closed within the following timelines:

| Risk Level | Closure rule for deviations |
|---|---|
| **High** | 60 days |
| **Medium** | 90 days |
| **Low** | Less than 60 days (assumption easy to fix) |

### 3.1.11 Perform spot checks on Test results and Action closure

The conducted tests and closed actions are reviewed through random spot checks to ensure that the quality of the tests is as expected by Group Internal Control. It may be valuable to hold peer reviews of conducted tests to ensure that the documentation and evidence collected are sufficient. Feedback and further training for FICMs/RICCs may be identified at this time.

### 3.1.12 Identify Improvements

Improvement actions resulting from tests to take action on should be identified and implemented, e.g. refine BIC control, awareness training.

## 3.2 Control Self-Assessment

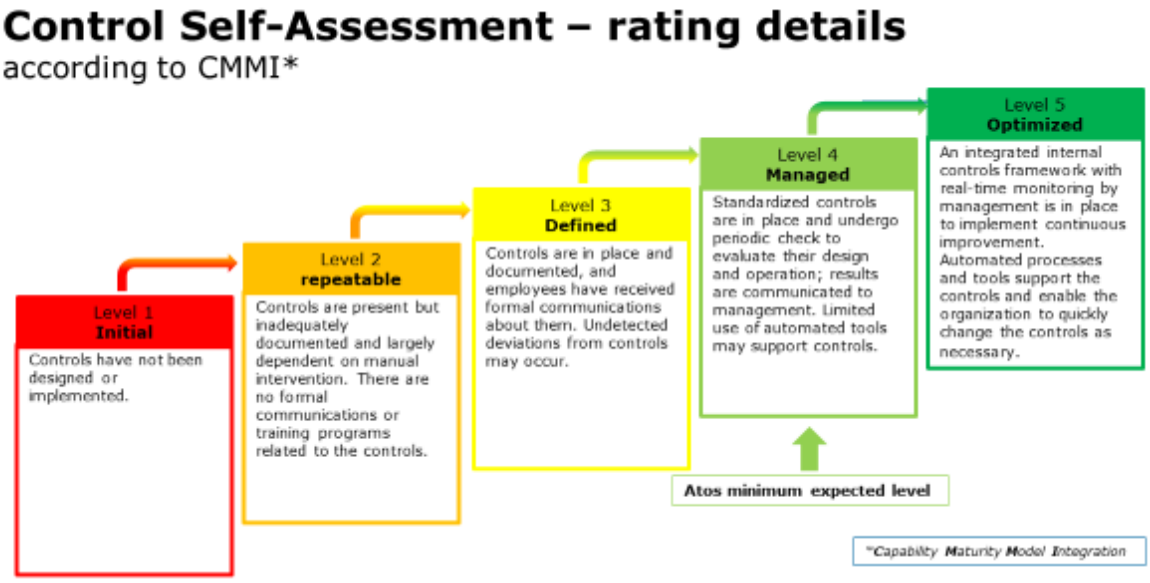
Control Self-Assessment is launched by Group Internal Control as well as some Business assurance Functions. It is happening an ad-hoc basis and aims to get a perception, from the control owner, of the maturity of the controls & processes implemented. The rating is done based on the CMMI maturity model.

### 3.2.1 Definition of the scope

Same approach as the Control Testing (refer to section 3.1.2).

### 3.2.2 Self-Assessment methodology

For the Self-Assessment the CMMI (**C**apability **M**aturity **M**odel **I**ntegration) model is used. The Control Owners should rate the controls in scope in alignment with the business on a rating scale from Level 1 (Initial) to Level 5 (Optimized) illustrated in the picture below.
The results are captured by the ICMs/RICCs for BIC related controls, in ARCOS (refer to section 4).




### 3.2.3 Improvement actions

In case of deficiencies perceived, corrective actions need to be defined by the control owner and followed-up by the ICM/RICC (outside Arcos tool).

# 4 ARCOS – BIC digitalization

## 4.1 Business objectives

In the course of the year 2020, a major change took place as Group Internal Control got the validation to develop a software for the management of internal control activities across the Group. This software is ARCOS (Governance, Risk and Compliance tool), the ARCHER software developed by RSA for ATOS, already being used by Group Internal Audit and Quality departments.

ARCOS allows to digitalize Internal Control activities as followed:

- Get the BIC updated from anywhere at any time by any authorized person
- Work on a single platform to assess control environment (control testing and self-assessment) and have a single repository for all information provided by the entities, countries, RBUs and Functions/Business Lines
- Facilitate the tracking on update & monitoring progress as well as on follow up on actions
- Perform continuous Control testing to increase coverage
- Enable the identification of potential deviations from the Group Internal Control framework by any Finance department
- Provide quickly and easily reports which will serve as an input to measure effectiveness
- Further alignment between internal control and internal audit activity

## 4.2 BIC update in ARCOS

As a result of the BIC digitalization and thus to ARCOS, The BIC can be improved/updated continuously, on a single platform, through the intermediary of the ICMs/RICCs working with process owners. ICMs/RICCs raise a change request in the tool, approved or rejected by Group Internal Control (see appendix B for more details). The change request involves two main requests: either to request a change of an existing content or to request a new content. The official BIC publication (extract from the tool) remains once or twice a year on GIA&IC public SharePoint for all employees.

## 4.3 Internal Control monitoring in Arcos

Control testing and Self-assessment campaigns (BIC related) are set-up in the system and launched by Group Internal Control. Assessment is documented by the ICM/RICC in the system (including evidences attached for Control testing). A workflow is embedded for review by the Global ICM/RICC or Group internal Control, to ensure correct execution (see appendices C & D for more details).

## 4.4 Reporting in Arcos

Various reports/charts in ARCOS are available to share with the stakeholders (e.g. Process Owner, Management, Local Business etc.), the Control testing status/results, the self-assessment status/results.

# 5 Related Documentation

| Document ID | Title | Document location |
|---|---|---|
| ASM-IAE-0002 | Internal Control Policy | https://atos365.sharepoint.com/sites/100000120/PublishedStorage/Forms/All%20Documents%202.aspx?id=%2Fsites%2F100000120%2FPublishedStorage%2FInternal%20Control%20Policy%2Epdf&parent=%2Fsites%2F100000120%2FPublishedStorage |
| ASD-IAE-0003 | Enterprise Risk Management (ERM) Framework and Approach | https://atos365.sharepoint.com/sites/100000120/PublishedStorage/Forms/All%20Documents%202.aspx?id=%2Fsites%2F100000120%2FPublishedStorage%2FEnterprise%20Risk%20Management%20%28ERM%29%20Risk%20Framework%20and%20Approach%2Epdf&parent=%2Fsites%2F100000120%2FPublishedStorage |
| ASM-BIP-0005 | Risk Policy | https://atos365.sharepoint.com/sites/100000120/PublishedStorage/Forms/All Documents 2.aspx?id=%2Fsites%2F100000120%2FPublishedStorage%2FAtos Risk Policy%2Epdf&parent=%2Fsites%2F100000120%2FPublishedStorage |
| | Group Internal Audit Charter | https://atos365.sharepoint.com/sites/690002068/CharterPolicies/Forms/AllItems.aspx?RootFolder=%2Fsites%2F690002068%2FCharterPolicies%2FAudit%20Charter&FolderCTID=0x01200077ADE8D5124F4145940947260FBF1B99 |
| AMS-BIP-0001 | Atos Management System Manual (part of AIMS core Documentation) | https://atos365.sharepoint.com/sites/100000450/SitePages/GQM-Home-Page.aspx |

# 6 Appendices

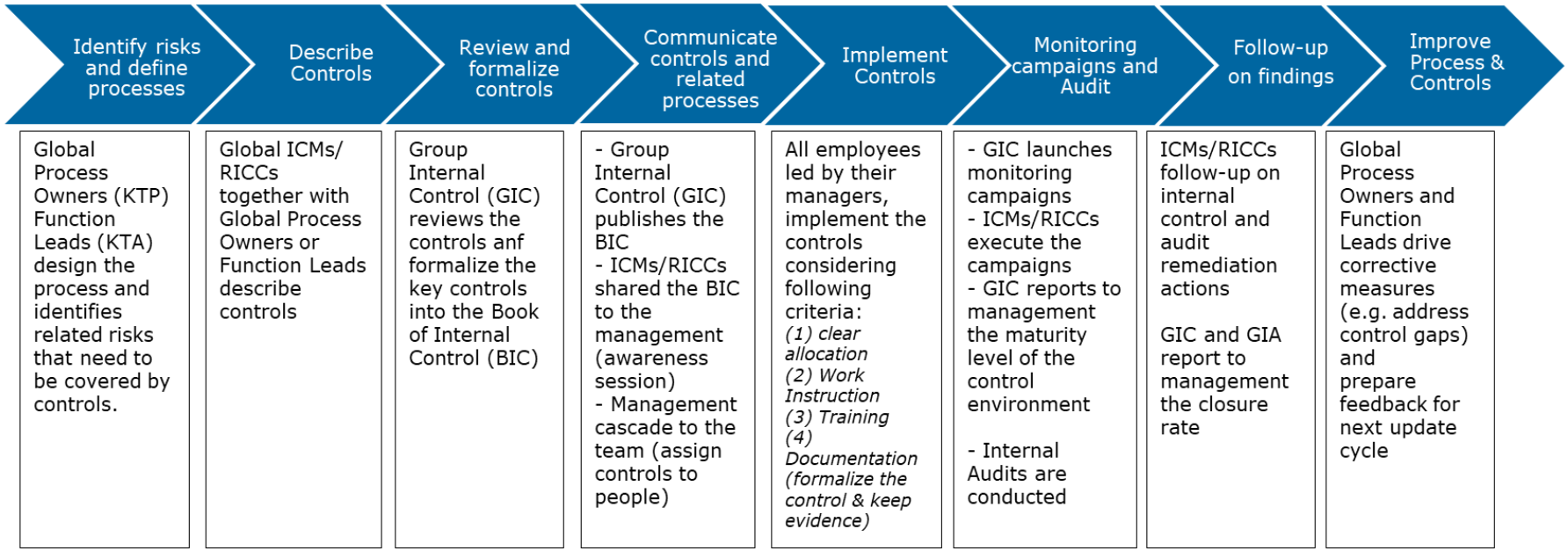
## *6.1* Appendix A1 - RACI matrix for Internal control Stakeholders

The main roles and responsibilities are summarized hereafter.
RACI: R: Responsible A: Accountable C: Contributor I: Informed

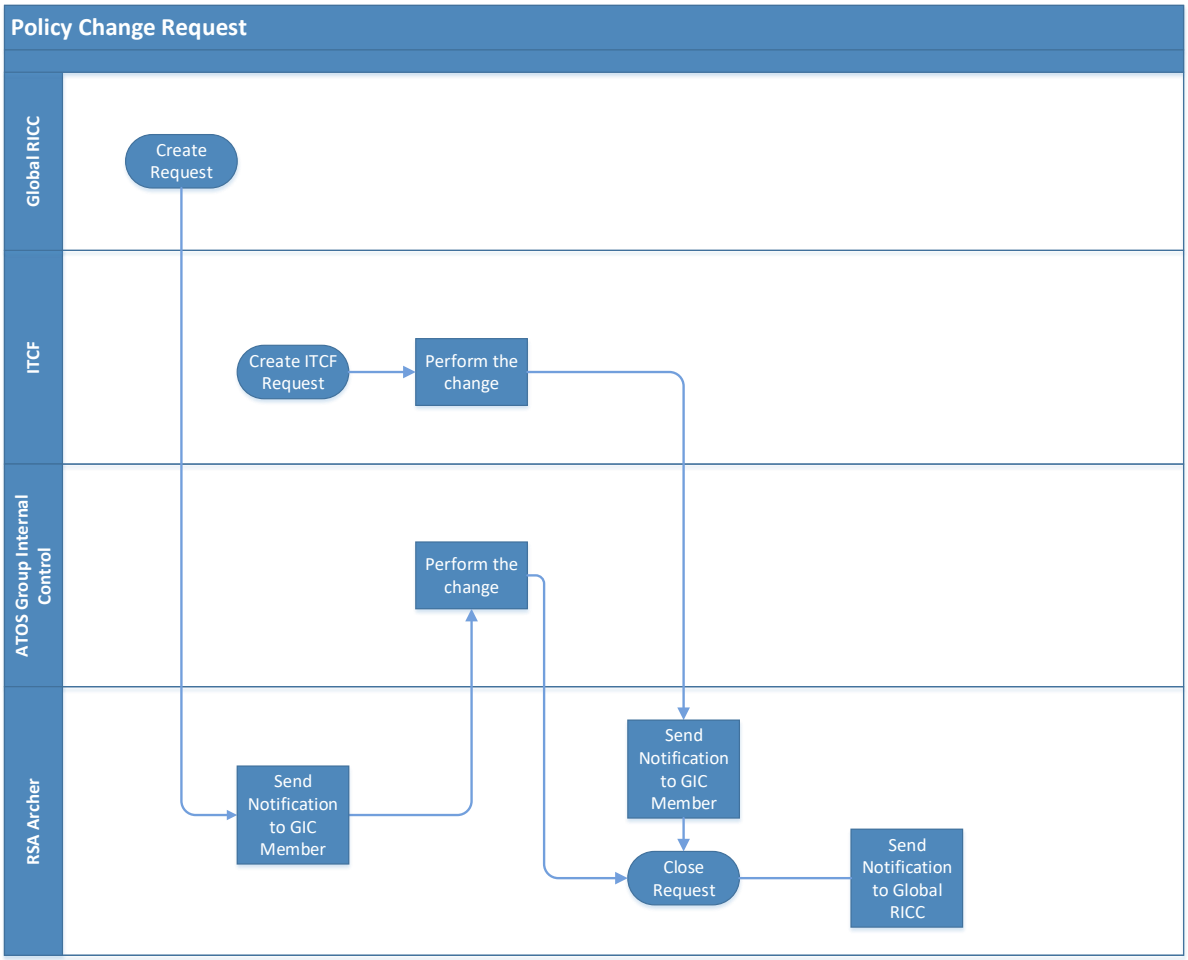
| Task/Activities | Senior management | Process owners | ICM / RICC | Group Internal Control | Assurance functions | Operational/ Functional managers | Internal Audit |
|---|---|---|---|---|---|---|---|
| [Plan] | | | | | | | |
| Set internal control objectives and "tone at the top" | A/R | I | C | C | I | I | I |
| [Deploy] | | | | | | | |
| Assess process risks and design appropriate controls | I | A/R | R | C | C | C | I |
| Maintain consistent control framework | I | C | R | A/R | I | I | I |
| Deploy controls throughout the organization (including corrective actions) | | A/R | C | C | | R | |
| [Monitor] | | | | | | | |
| Define assessment requirements (plan) | I | I | C | A/R | C | I | C |
| Run continuous monitoring and periodic self-assessments / Testing on controls | I | A | R | R | C | R | I |
| Perform independent assessment on internal control system | I | I | C | I | I | C | A/R |
| Monitor implementation of improvement actions (related to audit findings) | I | C | A/R | I | C | C | A/R |
| Monitor implementation of improvement actions (related to internal control findings) | I | c | A/R | A/R | C | C | I |
| [Report] | | | | | | | |
| Report on Internal Control status to management | I | C | C | A/R | C | C | I |
| Report on Audit recommendation closure | I | C | C | I | C | C | A/R |

## 6.2 Appendix A2- Stakeholders overview

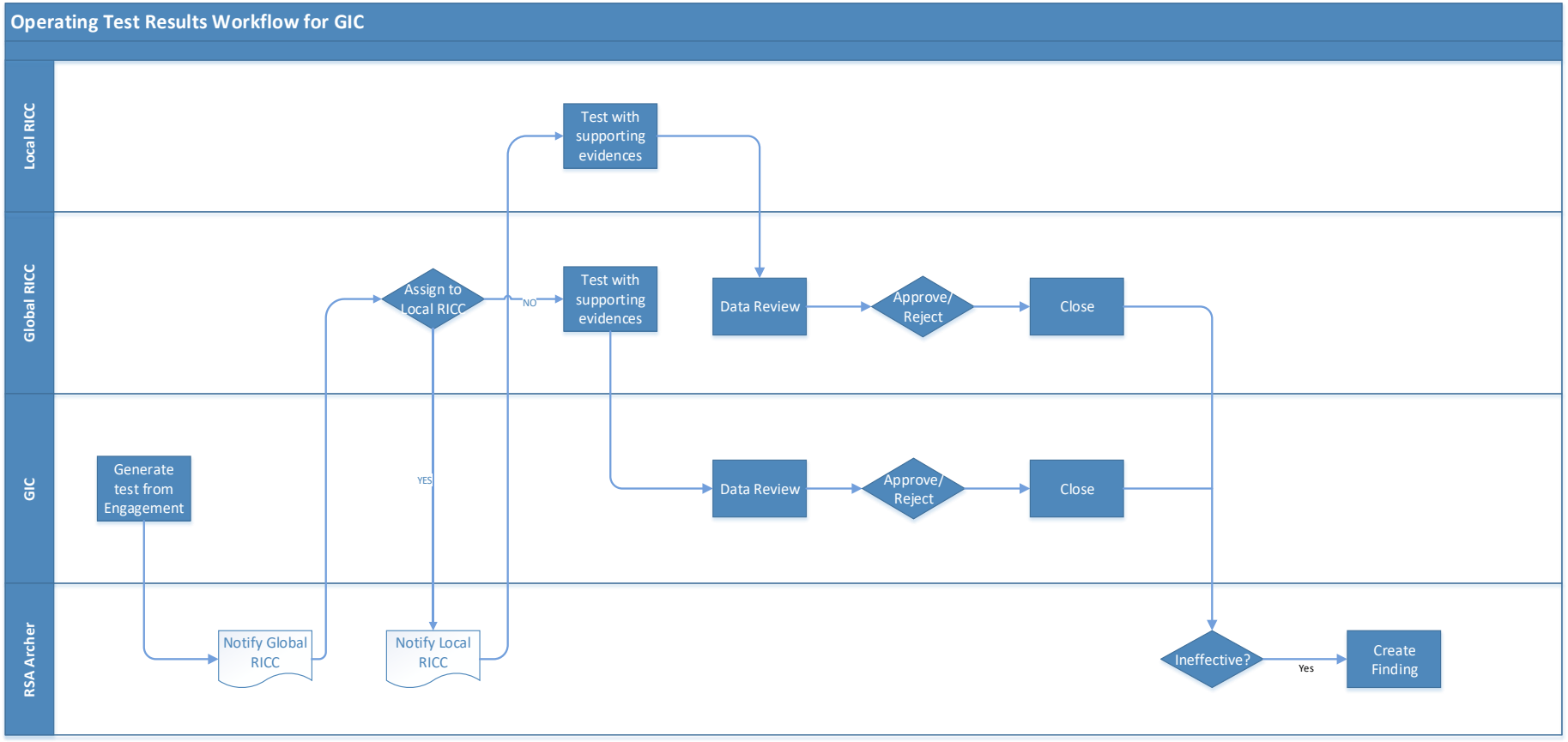
The following process flow illustrates in which step the different stakeholders are involved:



## 6.3 Appendix B- Policy Change Request workflow in ARCOS



## 6.4 Appendix C- Operating Test Result workflow in ARCOS



## 6.5 Appendix D- Control Self-Assessments workflow in ARCOS