

# SAGRADO

Universidad del Sagrado Corazón

## **Internal Audit Manual**

Effective: 2026.03.06

## Table of Contents

<b>I.</b>	<b>Purpose</b>	<b>3</b>
<b>II.</b>	<b>Scope</b>	<b>3</b>
<b>III.</b>	<b>Authority</b>	<b>3</b>
<b>IV.</b>	<b>Standards, Ethics, Competency, and Due Professional Care</b>	<b>4</b>
<b>V.</b>	<b>Governance of the Internal Audit Function</b>	<b>4</b>
	• Internal Audit Charter	
	• Independence & Oversight	
	• Resources & Quality	
<b>VI.</b>	<b>Building the Risk-Based Internal Audit Plan</b>	<b>5</b>
	• Inputs and Understanding	
	• Risk Assessment Method	
	• Dynamic Updates	
<b>VII.</b>	<b>Engagement Lifecycle and Deliverables</b>	<b>9</b>
	• Audit Initiation & Notification	
	• Planning Documents	
	• Fieldwork Documentation	
	• Audit Reporting	
	• Findings monitoring and closure	
<b>VIII.</b>	<b>How to Execute an Audit: Detailed Procedures</b>	<b>11</b>
	• Engagement Communication and Kickoff	
	• Engagement Risk Assessment	
	• Audit Program Development	
	• Fieldwork – Gathering Evidence	
	• Workpaper Preparation – Required Content	
	• Sampling for Testing	
	• Findings – Development and Root Cause	
	• Recommendations and Action Plans	
	• Audit Conclusions and Ratings	
	• Follow-up and validation	
<b>IX.</b>	<b>Data Analytics in Audits</b>	<b>18</b>
<b>X.</b>	<b>Fraud Risk Considerations</b>	<b>19</b>
<b>XI.</b>	<b>Quality Assurance &amp; Improvement Program</b>	<b>19</b>
<b>XII.</b>	<b>Third-Party Considerations</b>	<b>20</b>
<b>XIII.</b>	<b>Questions about this manual</b>	<b>20</b>
<b>XIV.</b>	<b>Reporting Violations</b>	<b>21</b>

## **I. Purpose**

This audit manual describes the key processes within the Internal Audit function applicable to the Universidad del Sagrado Corazón (University) in Puerto Rico. It aims to define the methodology and procedures for risk-based assurance and advisory services aligned to the Global Internal Audit Standards (GIAS), published by the Institute of Internal Auditors in 2024.

The Internal Audit function helps strengthen the institution's capacity to achieve its academic, research, and operational goals by offering independent, risk aware, and objective assessments of university processes and by providing guidance and forward-looking insights that help protect resources, enhance performance, and support long-term institutional value. This includes evaluating the effectiveness of governance structures, financial stewardship, compliance with regulatory and accreditation requirements, and the efficiency of administrative and academic support activities.

By serving as a trusted partner to the University leadership, Internal Audit helps ensure that the University remains resilient, transparent, and well positioned to fulfill its educational mission and public responsibilities

## **II. Scope**

This manual is applicable to Internal Audit staff and external audit service providers supporting the Internal Audit function. It covers key audit processes such as planning, fieldwork, reporting, follow-up, communications, resources, quality assurance program, documentation, and ethics.

## **III. Authority**

The Universidad del Sagrado Corazón Internal Audit Charter establishes that the Internal Auditor is authorized to have full and complete access to any of the University's records, systems, physical properties, and personnel relevant to the performance of an audit. The Internal Auditor will have free and unrestricted

access to communicate and interact directly with the members of the Audit Committee, without the presence and intervention of Management<sup>1</sup>.

Internal Audit's independence is supported by its functional reporting to the Board of Trustees ("Board") through the Audit Committee and administrative reporting to senior management.

## **IV. Standards, Ethics, Competency, and Due Professional Care**

The Internal Auditor shall follow GIAS and Internal Audit methodologies. Deviations should be documented with rationale, alternatives considered, and impacts. Disclosures must be made when required.

Integrity, objectivity, due professional care (skepticism), confidentiality and compliance with applicable laws and policies are mandatory for all personnel supporting the Internal Audit function.

The Internal Auditor must remain relevant and competent to deliver the audit plan. To achieve this, the Internal Auditor must comply with at least 40 hours of continued professional education every year.

## **V. Governance of the Internal Audit Function**

### **Internal Audit Charter**

Universidad del Sagrado Corazón has an Internal Audit Charter, which includes the audit function roles and responsibilities and the scope of its activities. This charter is periodically reviewed and approved by the Audit Committee of the Board of Trustees.

### **Independence & Oversight**

In alignment with the requirements set forth in the Global Internal Audit Standards, to fulfill the purpose of internal auditing, the Internal Auditor should report directly to the Board, should be qualified (competent) and placed in a

---

<sup>1</sup> As defined in the *Glossary of Terms of the Internal Audit Charter*, Management is the official or employee in charge a unit, area or activity audited. These individual exercises the highest administrative authority within the units, area or activity audited (for example, President, Vice Presidents, Directors, or their equivalents in the University unit).

position to perform the required duties without interference. To ensure independence and objectivity of the audit function, the Internal Auditor reports directly to the Audit Committee of the Board of Trustees, with a dotted reporting line to the General Counsel and Chief Institutional Integrity Officer for administrative purposes. The Board of Trustees, through the Audit Committee, oversees Internal Audit's effectiveness, resources, plan, and quality of results.

In addition, the Internal Auditor confirms his/her independence annually through the completion of the conflict-of-interest certification, and discusses any impairments and safeguards, as they may exist.

### **Resources & Quality**

Annually, the Internal Auditor identifies the budget needs for the upcoming year, including training, professional licenses and memberships, technology, outsourcing or co-sourcing services, student wages (for audit internship), and any other project planned. Once the budget request is negotiated with Finance, the Internal Auditor shall present it to the Audit Committee (generally with the Internal Audit plan, but timing may vary depending on the meeting date and Management's approval process). The Internal Auditor administers and monitors the use of the budget during the year.

A quality assurance and improvement program (QAIP) should be implemented, including periodic internal assessments and an external quality assurance (EQA) review every five years. The results must be reported to the Audit Committee.

## **VI. Building the Risk-Based Internal Audit Plan**

### **Inputs and Understanding**

The Internal Audit plan is developed annually by the Internal Auditor, listing the different audits and projects to be executed during the fiscal year. These will serve to provide an opinion on the University units' governance, risks and controls. The plan is risk-based and considers factors such as the annual risk assessment, emerging issues in higher education, areas of regulatory focus, prior audit results, operational changes, Management concerns, upcoming projects, and requests from the Board of Trustees, as applicable.

The number of audits and the strategy for coverage should be commensurate with the University's complexity and available resources.

## **Risk Assessment Method**

Every year, the Internal Auditor must complete a comprehensive risk assessment to identify the major risks and prioritize audit coverage. To conduct a proper risk assessment, the Internal Auditor should at least complete the following steps:

- a. Identify the audit universe. The Internal Auditor must have an inventory of the auditable units within the University. This inventory may become more granular year-over-year, as the exercise matures.
- b. Define a worksheet / template to use for the risk assessment exercise to ensure consistency and comparability through the exercise.
- c. Review higher education information to be aware of emerging issues and regulatory requirements.
- d. Interview the unit heads to obtain an understanding of the units' operations and areas of concern.
- e. Using the information obtained as well as prior knowledge on the areas, assess the risk level for the different risk types within a unit as well as its internal controls. At a minimum, assess the following risks:
  - i. Operational – The risk of loss resulting from people, inadequate or failed processes and systems, or from external events.
  - ii. Accounting and financial reporting – Risk that material accounting errors or misstatement of financial statements could occur.
  - iii. Fraud – Risk of fraudulent and other criminal activities perpetrated by employees or external parties against the University, exposing it to financial loss.
  - iv. Legal – Risk derived from the way the University conducts its operations that could result in lawsuits, fines, penalties or imprisonment of officers, which disrupts or otherwise affects the University's financial condition, or risk that contracts are deemed unenforceable.
  - v. Compliance – Risk of an activity not being conducted in conformity with applicable laws, rules, regulations and prescribed practices ("regulatory requirements"), as well as compliance-related internal policies and procedures, and ethical standards expected by regulators, students, employees and others.
  - vi. Information Systems / Technology / Cyber – Risk arising from inadequacy, disruption, destruction, failure, damage

from unauthorized access, modifications, or malicious use of information technology assets, people or processes that enable and support business needs, and can result in financial loss and/or reputational damage.

- vii. *Risk Culture and Conduct* – Risk Culture is the underlying norms, attitudes, and beliefs of individuals and groups that drive their risk management behavior. A strong Risk Culture supports an environment that promotes sound risk-taking behaviors aligned to the University's values and enables employees to identify risk taking activities that are beyond the established risk appetite. Risk Culture is Influenced by the broader culture of an organization, and in turn influences risk management behavior, which is then manifested in employee conduct. The University's Risk Culture program should be based, among others, on tone from the top, accountability, risk management, and people management.
- viii. *Data* (including Privacy)- Risk, whether direct or indirect, to data that is used to support the University's ability to make informed decisions and develop accurate reporting and analytics for the University, including the Board, senior management and regulators. This includes students and employees data gathered by the University. Risks to which the University is exposed include data management, breaches or data that is incomplete, inaccurate, invalid, untimely and/or inaccessible. Data risk applies throughout the data lifecycle as data is originated/ captured, moved/ transformed, stored, consumed, archived or disposed.
- ix. *Environmental / Social / Governance (ESG)* - ESG risk refers to the possibility that environmental, social, and governance concerns related to Sagrado's conduct, business practices, or relationships could result in adverse impacts to the University.
  - 1. *Environmental*: the potential adverse impacts due to the loss of, or damage to the natural environment or biodiversity, such as land, water, plants, animals, natural resources, ecosystems, and the atmosphere. Includes climate change.
  - 2. *Social*: Potential adverse impacts due to the mismanagement of social considerations and actual or

perceived negative impacts on people and communities. Social considerations include human rights; labor standards and working conditions; community health, safety and security; disadvantage and vulnerable groups.

3. *Governance*: The oversight and the way in which the University is governed. It includes the University's processes and policies, how decisions are made, and how it deals with the various interests of, and relationships with its stakeholders, including faculty, administrative staff, students, and the broader university community.
- x. *Reputational* - Risk that negative publicity or public sentiment regarding the University's conduct, business practices or associations, whether true or not, will adversely affect the University's revenues, operations or student base, or require costly litigation or other defensive measures. Includes, indirect reputational risk that might arise from:
  1. Failure under performance or lack of accreditation.
  2. Inaccurate or misleading reporting or insufficient public disclosures.
  3. Inadequate information security leading to hacking or other breaches resulting in student or employee harm.
  4. Poorly implemented initiatives leading to disgruntled employees.
- xi. *Strategic* - Risk that the university, its faculty, and its administrative functions will make strategic choices that are ineffective or insufficiently resilient to changes in the environment it operates. It is the possibility of losses due to high-level decisions associated with the creation of unsustainable competitive advantages.

Aspects such as academics, student's life and well-being, campus and facilities, etc. are covered within the respective auditable unit in charge of managing these topics (e.g. Academic Affairs, Student's Dean Office, Operations Unit, etc.).

- f. Once each individual unit assessment is completed, analyze the overall results and define what the audit plan will be for the year and determine the audit cycle for each unit. Units rated as high risk

should be reviewed for at least one of its key processes annually, moderate risk every 3 years, and low risk every 5 years.

- g. Summarize the analysis of the risk assessment and the proposed plan, and present it to the Audit Committee for approval.

## **Dynamic Updates**

Sagrado's risk assessment should be reviewed and updated at least once every year, before the preparation of the audit plan. It can be updated more frequently, as needed. The annual audit plan is dynamic. While it is prepared once a year, it can be modified throughout the year, to address top and emerging risks, understanding impacts and trade-offs. Audit Committee approval is required for audit plan changes.

## **VII. Engagement Lifecycle and Deliverables**

### **Audit Initiation & Notification**

The Internal Auditor should communicate to Management in advance the intention to audit their unit or processes. The purpose of this communication is to best coordinate the timing and logistics of the work as well as to request information needed to define the scope and plan the execution of the audit work. This includes, but is not limited to, reviewing process documentation and having walkthrough meetings with Management to better understand the current operation.

### **Planning Documents**

All the information gathered during the planning stage of an audit should be documented in a planning memorandum. At a minimum, the planning memorandum should contain the following elements:

- a. Audit objective
- b. High level description of the process to be audited
- c. Organizational structure
- d. Materiality
- e. Proposed audit scope (areas and time period to be reviewed)
- f. Applicable regulations
- g. Applicable policies and procedures
- h. Prior audit findings
- i. Fraud risk analysis

j. Systems to be evaluated

To the extent available, the auditor should also obtain from the units their process narratives, process flowcharts, and their risk and control matrices. The auditor may create an information request list to track and follow-up on documentation requested to the auditee.

### **Fieldwork Documentation**

All audits should have an audit program detailing the procedures required to be performed during the audit. Audit structure will be based on the COSO (or COBIT, when in IT) framework. Length and depth of the audit program will vary, depending on the audit scope. The work done for each audit step tested should be documented in detail, either in the audit system (if available) or in a document (e.g. short memo or workpaper).

All tests and validations performed during the audit must be documented in workpapers. Workpapers can be created by the auditor in different formats and using different tools, including documents, spreadsheets, data analytic tools, presentations, etc. Additional documentation and analyses may be received from the auditee. All documentation should be organized logically in a designated folder or audit system and should be maintained for at least seven (7) years after the completion of the audit (measured from the date of the final audit report), unless a longer period is required by applicable laws, regulations, or institutional policy.

### **Audit Reporting**

At the end of each audit / review, results must be formally discussed with the auditee and should be formally communicated in writing. Results must be transparent and include a description of the strengths observed during the audit and the findings raised for control weaknesses identified.

Draft audit findings, including audit recommendations, will be shared in writing with management. Management will be given a reasonable period of time generally not to exceed ten (10) business days, unless otherwise approved by the Internal Auditor, to provide their proposed action plans along with the expected resolution date. Once the action plans and dates are received, these will be included as part of the draft audit memorandum / report.

Draft audit memorandums or reports will be shared with the auditee to provide them five (5) business days to review its contents and clarify any questions before formally releasing the final version.

## **Findings monitoring and closure**

All audit findings raised will have a Management expected resolution date and an Audit validation date on which the action plans implemented will be tested to ensure they have effectively addressed the risks identified when the finding was raised. Issues not resolved by the committed time and issues that fail audit validation will require an approved extension of time. Refer to **Section VIII** for details on the extension process.

## **VIII. How to Execute an Audit: Detailed Procedures**

### **Engagement Communication and Kickoff**

Once the planning stage of the audit has advanced and the audit scope has been defined, the Internal Auditor should notify the auditee what are the objectives, detailed audit scope, assessment type (review or full audit), criteria, timing, contacts, data needs, and access required for the audit.

While this can be performed through a meeting or call, as the process matures, the Internal Auditor should consider implementing a written commencement advice or an opening meeting presentation for a formal kick-off.

Key points of contact should be defined, and an escalation process should be agreed upon to ensure proper information flow and adequate audit progress throughout the project.

### **Engagement Risk Assessment**

During the planning stage of the audit, the auditor should list the major risks of the unit or process that will be audited and assess their severity (high, moderate, or low). The Internal Auditor should then identify with Management what the controls are, if any, mitigating those risks, to arrive at the residual risk. As part of this exercise, potential fraud risk scenarios should also be identified.

All risks identified as high should be tested. The corresponding audit procedures should be included in the audit program. Level of audit testing for moderate and low risks will vary depending on the availability of resources to test.

### **Audit Program Development**

Once the audit scope has been defined and communicated, and major risks have been identified and assessed, the auditor will develop the audit program to follow. The audit program should address the audit objectives, assertions, risks, and controls involved. Through the definition of the audit steps, the auditor should

consider documenting, to the extent possible, the specific evidence and acceptance criteria. As audit steps are completed, the audit program should be marked as completed and signed off accordingly.

## **Fieldwork – Gathering Evidence**

Before selecting samples to test during the audit, the Internal Auditor must validate population completeness and accuracy. This is mainly achieved with data reconciliations and / or independent reperformance of the activity by the auditor, without Management’s intervention (e.g. data extracts from the system).

The Internal Auditor will execute tests and document all work performed in workpapers, as explained in the section below. Supporting evidence and documentation should be requested to Management and should be properly referenced within the audit file. Copy of supporting documentation must be obtained for all exceptions and linked to the workpaper where it was tested. In big samples of extensive documents where there was no exception, the auditor does not have to retain copies of all documentation reviewed. Rather, the requirement for the Internal Auditor is to register sufficient information in the workpaper so that it is clear what document was reviewed. Once each test is completed, the auditor has to tabulate the exception rate to analyze audit results for conclusion.

Elements to consider for evidence sufficiency when conducting audit tests include the following:

- a. Relevance: Documentation obtained is needed to fulfill the test objective and assertion.
- b. Reliability: Source is authoritative; data is current; integrity verified.
- c. Sufficiency: Samples quantity is aligned to sampling table and is adequate for conclusions, considering risk and materiality.
- d. Corroboration: Information is cross-checked with independent sources, where practicable.
- e. Population Completeness & Accuracy: Procedures to validate completeness should be documented for any sampling/testing.
- f. Traceability: Document is dated, sourced, and cross-referenced to work program steps.
- g. Re-performance: A competent reviewer could replicate and reach similar conclusions.
- h. Confidentiality: Sensitive data is masked or access-controlled.

## **Workpaper Preparation – Required Content**

Workpapers must be properly identified so that they can be considered standalone documents. As such, the documents should include the following elements:

- a. Documentation (evidence) provided by auditee: document name or description, the name of who provided such document, a comment on what it is used for, tickmarks with explanations on what was reviewed about the document, initials and date on when it was reviewed (this can be replaced for electronic sign-off if using an audit system).
- b. Documentation created by auditor: title of audit test, objective and risk / control, population / period, sampling method; source of evidence (including cut-off date), parameters evaluated (generally listed in the columns tested), conclusion, cross-references, sign-off, tickmarks, exception rate, test conclusion (satisfactory, needs improvement, and unsatisfactory). In case the testing was done by an internship student, the workpapers must also be reviewed and signed off by the Internal Auditor. Test results and workpaper conclusion should agree with the grading provided for the area in the audit report.

## **Sampling for Testing**

Sampling is used to evaluate a subset of a larger population—such as financial transactions, student records, grant expenditures, or system access—when reviewing every item is not practical. The purpose is to obtain sufficient and appropriate evidence to form a reliable conclusion about the effectiveness of processes, controls, and compliance across the university.

The Internal Auditor must document the methods used to determine the sample size and the specific sample selection. Samples should be representative of the population and should be independently selected. Where possible, the population of items to be considered for testing should be obtained from a source that is independent of the area audited.

Internal Audit may use one or more of the following methods based on the audit objective and risk profile:

- a. Random Sampling: Every item in the population has an equal chance of selection. This approach is appropriate for most assurance engagements.

- b. Stratified Sampling: The population is divided into risk-based or size-based groups, and selections are made from each group to ensure adequate coverage of higher-risk areas.
- c. Targeted (Judgmental) Sampling: Items are selected based on known risk indicators, such as unusually large transactions, off-cycle adjustments, or items that deviate from standard patterns. Results from targeted sampling provide insight into specific risks but are not used to draw conclusions about the entire population.

While sampling guidance is provided above, the auditor has the authority to use a different sampling method or approach based on judgement, as long as such rationale is properly justified and documented. Workpapers should be clearly documented regarding the following:

- a. The defined population and how it was validated
- b. The sampling approach, rationale, and sample size
- c. The specific items selected and tested
- d. The results of testing, including any exceptions
- e. The overall conclusion and its impact on the audit objectives

Comprehensive documentation ensures transparency and supports the credibility of audit conclusions.

### **Findings – Development and Root Cause**

Upon identifying exceptions during the audit, these should be discussed by the Internal Auditor with the corresponding officer in charge of the activity and subsequently with the unit head, to receive any additional evidence for consideration or to confirm the audit finding. Once the finding is confirmed, the Internal Auditor should document it in the corresponding template and send it to management to obtain a formal action plan and expected resolution date. The elements required in the audit finding template are the following:

- a. Audit name
- b. Issue (finding) name
- c. Issue risk level (high, moderate or low)
- d. Person responsible for resolution
- e. Issue summary
- f. Observation details
- g. Root cause
- h. Risk (impact)

- i. Audit recommendation
- j. Management's action plan and committed dates per action plan
- k. Audit validation date (generally a month, quarter or semester after management's date to test proper resolution and sustainability of actions implemented)

When evaluating the finding, it is important to resolve and address not only the specific instance where the deficiency was noted, but more importantly, to identify and properly address the root cause. Main root causes categories include the following:

- a. Lack of understanding or awareness
- b. Documentation
- c. Process Design
- d. Resources (people, materials, technology)
- e. Systems (system limitations or malfunctions)
- f. Oversight and supervision

Recommendations from Internal Audit as well as the action plans to be developed by management must address the main root cause.

### **Recommendations and Action Plans**

As part of the write-up of the audit findings, the Internal Auditor will provide audit recommendations to be considered by management in their proposed action plan. These recommendations should aim to correct / remediate not only the deficiency identified, but more importantly should address root cause to avoid recurrence. Management's action plan should clearly state the actions and controls to be implemented, the specific owners for each action / control, and expected resolution dates.

Escalation process: Findings not accepted by Management or unresolved disagreements will be elevated by the Internal Auditor to the corresponding EVP or President. Additional escalation forums in case agreement is not possible will be the University's President, and the Audit Committee Chairperson. The Audit Committee Chairperson may take the final decision on the disagreement resolution or may decide to elevate the matter to the full Audit Committee.

### **Audit Conclusions and Ratings**

Audit results will be summarized in the audit report or audit memorandum, as applicable. Such reporting will include the strengths observed in the areas tested, as well as the deficiencies and findings identified, as follows:

# SAGRADO

Universidad del Sagrado Corazón

- a. **Audit memorandum:** A memorandum format may be used when a review of limited scope is performed. In such cases, it is important that the memorandum at least includes background information to provide context to the reader, and a description of the work done, documentation reviewed, and results obtained. It should also include a conclusion and any recommendations provided by the auditor to improve / enhance the process and controls.
- b. **Audit report:** A full detailed report will be prepared for planned audits with an extensive scope reviewed. The audit report will contain the following sections:
  - i. *Dashboard* – This is a summary of results at an executive level and includes a snapshot of the audit coverage, conclusion, findings, and expected resolution.
  - ii. *Detailed results* – This section includes a more detailed narrative on the key strengths observed in the audit and the areas for improvement.
  - iii. *Grading summary* – This area provides a line-by-line detail of the areas in scope and the individual audit grade for each.
  - iv. *Detailed issues and recommendations* – For each audit finding, there is a detailed explanation of the situation observed, what was its root cause, the recommendations from audit and the action plans and dates committed by management for its resolution. These findings are risk rated to reflect their severity for the organization.
  - v. *Unit profile and supplementary information* – This section presents a high-level description of the unit or process audited. Key regulations and systems used are also listed in this section, as applicable.

The following table details the range of audit grades and their definition:

Audit Report Grading	Guidelines for Audit Grades
Satisfactory	No moderate, high, or critical findings or weaknesses in internal controls were noted as a result of the audit procedures.
Satisfactory with Exceptions	Audit report has findings but none that would be considered critical or high priority findings or weaknesses in internal controls identified as a result of the audit procedures.

<b>Needs Improvement</b>	Audit report containing one to three high priority findings or weaknesses in internal controls (or several weaknesses were noted that, when taken collectively, are considered significant). However, if any of the findings taken alone carry a certain risk of a significant negative impact to the University, the report could be classified as Unsatisfactory.
<b>Unsatisfactory</b>	Audit report containing more than four high priority findings and one or more Very High risk finding or weaknesses in internal controls (or very large number of weaknesses were noted that, when taken collectively, are considered significant). Furthermore, a report containing multiple high and/ or moderate priority findings which, individually or collectively, indicate significant weaknesses in the control environment for a particular process or function, could be rated as Unsatisfactory.

Unless a different objective is specified in the report, most of the times the Internal Auditor will opine on the design and operating effectiveness of internal controls on the unit or process evaluated.

The results of each individual audit, combined with continuous monitoring activities and the monitoring and testing of audit findings, will help the Internal Auditor better inform the opinion for the semester and year on the effectiveness of governance, risk management, and controls, which will be provided in the Internal Auditor's quarterly report.

### **Follow-Up and Validation**

The Internal Auditor shall maintain a tracker to monitor the status of open findings against their expected resolution date. Quarterly, status updates will be requested from management and will be reported to the Audit Committee.

Once findings are reported as closed by the respective owners, the Internal Auditor will validate findings closure. The extent of such validation will be risk-based. Workpapers used for the validation testing should follow the same format requirements as those used for the regular audit. Audit validation will be limited to the specific elements raised in the audit finding rather than full scope of testing performed during the audit.

- a. Audit findings monitoring and date extensions: When Management identifies that they will not be able to comply with the committed date to close a finding, the owner of the finding must obtain written approval from their corresponding EVP (or President in case their reporting line is directly to the President) to extend the resolution

date and send the written approval to the Internal Auditor and University President. This will be reported by the Internal Auditor to the Audit Committee. The issue resolution date should not be extended beyond one semester.

- b. Findings that fail audit's retesting: In cases where Management has completed the committed action plans, but audit's validation confirms that the issue remains, the same date extension process applies, whereas Management must obtain EVP approval for an extension to ensure effectiveness of the control implemented.

As an example, if there is a finding for which Management's action plan is to provide training to the staff, but when audit retests still finds the same deficiencies (for example incomplete documentation in student's file), even if Management gave the committed training session, Management will need to seek for an extension approval and the finding would remain open until a new retesting validates the process is being properly executed (e.g. until Audit validates in a new sample that documentation is complete).

As part of the extension request, Management must inform what actions have been taken to date, if the risk has been somewhat mitigated, and what are the pending actions needed to fully close the finding.

- c. Findings closure: Once the auditor validates with satisfactory results that Management has completed the committed action plans and that the findings have been resolved and are not recurrent, the Internal Auditor will close the finding. For the following Audit Committee session, issue would be reported as closed.

## **IX. Data Analytics in Audits**

The Internal Auditor may incorporate the use of data analytics to enhance effectiveness, efficiency, and coverage during audits and monitoring activities (e.g. testing populations instead of samples). Data analytics may support risk assessment, audit planning, testing, and continuous monitoring activities by enabling deeper insights into business processes and controls.

When using data analytics, the Internal Auditor shall request and access data in accordance with the University's policies and controls. All analytics steps, assumptions, and outcomes must be documented and retained as part of the audit working papers. Data obtained for audit purposes must be stored, transmitted, analyzed, and disposed of securely. Internal Audit must maintain confidentiality, integrity, and professional skepticism when handling data.

## **X. Fraud Risk Considerations**

Internal Audit is not responsible for preventing fraud, but plays a critical role by:

- a. Evaluating the design and operating effectiveness of anti-fraud controls.
- b. Considering fraud risk in all audits, risk assessments, and planning processes.
- c. Reporting observations that may indicate potential fraud or control weaknesses.
- d. Supporting fraud investigation activities.

At the planning stage of each audit, the Internal Auditor will brainstorm in the potential fraud risks scenarios in the process or unit that is being audited. These scenarios will be risk-rated based on their likelihood of occurrence and potential loss. The auditor will discuss these scenarios with Management to identify controls in place to mitigate these risks. All residual risks considered high should be tested.

## **XI. Quality Assurance & Improvement Program**

As required by the Global Internal Audit Standards, the Internal Auditor must develop, implement, and maintain a quality assurance and improvement program that covers all aspects of the Internal Audit function. It should consider internal and external assessments. At least once a year, the Internal Auditor must communicate the results of the internal quality assessment to the board or senior management. The results of the external quality assessments must be reported when completed. The results to be reported should include:

- a. The Internal Audit function's conformance with the Global Internal Audit Standards and achievement of objectives.
- b. Compliance with laws and regulations relevant to internal auditing.

- c. Plans to address the Internal Audit function's deficiencies and opportunities for improvement.

If non-conformance with the standards affects the overall scope or operation of the Internal Audit function, the Internal Auditor must disclose to the Audit Committee and the University President the non-conformance and its impact.

## **XII. Third-Party Considerations**

Subject to the procurement and contracting requirements of the University and approval from the Audit Committee, the Internal Auditor may engage external service providers to support the Internal Audit function through outsourcing or co-sourcing arrangements. These are defined as follows:

- a. Outsourcing: The full or partial delegation of Internal Audit activities to an external service provider, while the organization retains responsibility for overseeing the function.
- b. Co-sourcing: A partnership model in which the Internal Auditor is supported with external specialists for specific engagements, technical expertise, or capacity needs.

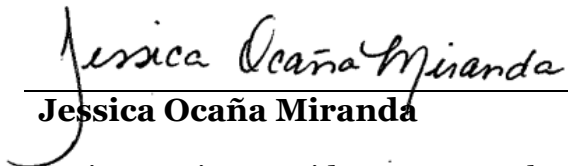
Internal Audit may use outsourcing or co-sourcing to obtain specialized skills or subject-matter expertise, address short-term resource constraints or workload peaks, and enhance coverage of complex, high-risk, or technical audit areas. The use of external resources must comply with the International Standards for the Professional Practice of Internal Auditing (IIA Standards) and preserve the independence and objectivity of the Internal Audit function.

## **XIII. Questions about this manual**

Questions about the scope and interpretation of this Internal Audit Manual should be directed to the Office of Internal Audit at 787.728.1515, ext. 5456, or by email at [auditoriainterna@sagrado.edu](mailto:auditoriainterna@sagrado.edu). If there is any ambiguity in any provision of this Manual, the University reserves the discretion to interpret it in accordance with the purpose for which it was established, the impact to the University's operations and good faith, unless otherwise provided by law.

## **XIV. Reporting Violations**

Violations to this Manual should be directed to the office of President at [presidencia@sagrado.edu](mailto:presidencia@sagrado.edu). Any violations of this Manual will be addressed in accordance with the University's policies and procedures.



---

**Jessica Ocaña Miranda**

Assistant Vice-President & Internal Auditor  
Compliance, Audit & Institutional Integrity