400 Reporting Phase

410 Overview of the Reporting Phase

1. The overall objective of the reporting phase is to determine the auditor’s compliance with *Federal Information System Controls Audit Manual* (FISCAM) requirements and to communicate the results of the information system (IS) controls assessment. This section addresses the auditor’s compliance with the FISCAM methodology and the auditor’s responsibilities for communicating the results of the IS controls assessment (see fig. 8).

Figure 8: Reporting Phase Activities

A picture containing shape

Description automatically generated

1. The auditor documents compliance with the FISCAM methodology by completing the FISCAM assessment completion checklist (app. 600B). The checklist lists FISCAM’s requirements for conducting the IS controls assessment based on applicable generally accepted government auditing standards (GAGAS) requirements.
2. Depending on the engagement type and objectives, the results of the IS controls assessment may be incorporated into another engagement (e.g., financial audit report) or issued in a separate report. These results include communicating IS control deficiencies and providing recommendations for corrective action.

420 Determine Compliance with FISCAM

1. The auditor should determine whether the FISCAM methodology was followed. The FISCAM assessment completion checklist (app. 600B) includes FISCAM’s requirements for conducting the IS controls assessment. If the auditor is using a different IS controls assessment methodology, the auditor may use the FISCAM assessment completion checklist to provide a crosswalk between the audit methodology used and FISCAM.

430 Draft Report

1. Reports are issued to communicate the results of the engagement. In the context of the IS controls assessment, this serves several purposes, including

* clearly communicating IS control deficiencies to those charged with governance, appropriate officials of the audited entity, and appropriate oversight officials and
* providing appropriate officials of the audited entity with recommendations for corrective action.

1. The overall engagement auditor considers the engagement objectives, as well as the type of GAGAS engagement (financial audit, attestation engagement, or performance audit) to determine whether to issue a separate report on IS controls is issued or incorporate the results of the IS controls assessment into another engagement. For example, when an assessment is performed as part of a financial audit, the results of the IS controls assessment are incorporated into the auditor’s report on internal control over financial reporting.
2. Report content related to the IS controls assessment generally includes (1) the objectives, scope, and methodology of the engagement; (2) findings, conclusions, and recommendations, as appropriate; and (3) if applicable, the nature of any confidential or sensitive information omitted from the report.[[1]](#footnote-1) Each of these elements, including any differences in requirements based on engagement type, are discussed below.

Objectives, Scope, and Methodology

1. Report users need information regarding the engagement objectives, scope, and methodology to understand the purpose of the engagement; the nature and extent of the work performed; the context and perspective regarding what is reported; and any significant limitations in the engagement objectives, scope, or methodology. Report content relevant to objectives, scope, and methodology differs among engagement types. Depending on the engagement type, the overall engagement auditor addresses the specific requirements established in GAGAS (2018).

Findings, Conclusions, and Recommendations

1. Reporting responsibilities vary depending on the nature of the findings and conclusions. Engagement objectives may or may not require an overall conclusion on the effectiveness of IS controls. For example, when reporting on internal control, the audit report may

* provide an overall conclusion, if appropriate (e.g., the entity’s IS controls are or are not effective in achieving the control objectives relevant to the engagement), and communicate identified deficiencies;
* limit reporting to identified IS control deficiencies without providing an overall conclusion (e.g., “based on our work, we identified the following IS control deficiencies”); or
* report findings within the context of the engagement objectives, such as how they relate to (1) the design, implementation, and operating effectiveness of relevant IS controls or (2) the reliability of data intended to materially support findings, conclusions, or recommendations.

1. Generally, when internal control deficiencies are determined to be significant to the engagement objectives, such deficiencies are reported.[[2]](#footnote-2) Because GAGAS reporting requirements relevant to findings and conclusions vary depending on the engagement type, reporting requirements are discussed below by engagement type.

Financial Audits

1. GAGAS reporting requirements for federal financial audits relevant to internal control are addressed in the *Financial Audit Manual* (FAM), including the reporting of material weaknesses and significant deficiencies.[[3]](#footnote-3) See section 340 for additional information on evaluating the significance of IS control deficiencies. The overall engagement auditor should comply with the reporting requirements, including requirements for classifying control weaknesses, as discussed in FAM 580. See FAM 580 for detailed reporting requirements, including requirements for classifying control weaknesses and reporting weaknesses relevant to the Federal Managers’ Financial Integrity Act of 1982 and the Federal Financial Management Improvement Act of 1996.

Attestation Engagements

1. Under GAGAS (2018), for examination-level attestation engagements, the overall engagement auditor should include in the examination report all internal control deficiencies considered to be significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed.

Performance Audits

1. The overall engagement auditor should include in the audit report (1) the scope of the auditor’s work on internal control and (2) any deficiencies in internal control that are significant within the context of the engagement objectives and based upon the audit work performed.
2. When the auditor detects deficiencies in internal control that are not significant to the engagement objectives but warrant the attention of those charged with governance, the overall engagement auditor should include those deficiencies in the report or communicate those deficiencies in writing to audited entity officials. If the written communication is separate from the audit report, the overall engagement auditor should refer to that written communication in the audit report.

Presentation of Findings, Conclusions, and Recommendations

1. When presenting findings, the auditor should develop the elements of the findings to the extent necessary to assist management or oversight officials of the audited entity in understanding the need for taking corrective action (paragraph 340.08). For performance audits, the extent to which the elements of a finding are developed depends on the engagement objectives.
2. The elements of a finding are criteria, condition, cause, and effect.

* Criteria identify the required or desired state or expectation with respect to the program or operation.
* Condition is a situation that exists.
* Cause is the factor or factors responsible for the difference between the condition and the criteria and may serve as a basis for recommendations.
* Effect or potential effect is the outcome or consequence resulting from the difference between the condition and the criteria.

This information helps senior management understand the significance of the deficiencies and develop appropriate corrective actions.

1. The overall engagement auditor should place audit findings in perspective by describing the nature and extent of the issues being reported and the extent of the work performed that resulted in the findings. As appropriate, the overall engagement auditor should relate the instances identified to the population or the number of cases examined and quantify the results in terms of measures that give the reader a basis for judging the prevalence and consequences of the findings. If the results cannot be projected, the auditor should limit conclusions appropriately. For performance audits, the overall engagement auditor should describe in the report limitations or uncertainties in the reliability or validity of evidence if (1) the evidence is significant to the findings and conclusions within the context of the engagement objectives and (2) such disclosure is necessary to avoid misleading the report users about the findings and conclusions.
2. When reporting on the results of the audit work, the overall engagement auditor should disclose significant facts relevant to the objectives of the work and known to the auditor that if not disclosed, could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices. For example, a limited review of controls over a type of operating system relevant to the areas of audit interest, such as applications that support significant business processes, may not identify any significant weaknesses. However, there may be significant weaknesses in other areas, such as other types of operating systems, that the auditor is unaware of because the scope of the IS controls assessment is limited to areas of audit interest relevant to engagement objectives. As such, the overall engagement auditor evaluates any potential limitations of the work on the auditor’s report and the needs and expectations of users.
3. The overall engagement auditor should report conclusions that are logical inferences based on the auditor’s findings, not merely a summary of the findings. The strength of the auditor’s conclusions depends on the persuasiveness of the evidence supporting the findings and the soundness of the logic used to formulate the conclusions. Conclusions are more compelling if they lead to recommendations and convince a knowledgeable user of the report that action is necessary.
4. The auditor should provide recommendations for corrective action for any sufficiently developed findings that are significant to the engagement objectives. The auditor should make recommendations that flow logically from the findings and conclusions, are directed at resolving the causes of identified deficiencies and findings, and clearly state the actions recommended. When feasible, the auditor should recommend actions to correct deficiencies and other findings identified during the audit and to improve programs and operations when the potential for improvement in programs, operations, and performance is substantiated by the reported findings and conclusions.

Reporting Confidential or Sensitive Information

1. IS controls information may be prohibited from public disclosure because it may be designated as or derived from classified, sensitive but unclassified, or proprietary information.[[4]](#footnote-4) Some audit organizations do not have original or derivative classification authority or the ability to identify unclassified information that may be subject to safeguarding or dissemination controls.[[5]](#footnote-5) Therefore, for reports that contain, or may contain, information prohibited from public disclosure, the overall engagement auditor should request that the source agency perform a classification, security, or sensitivity review of the draft report. The overall engagement auditor should evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements.
2. If certain information is prohibited from public disclosure or is excluded from a report because of its confidential or sensitive nature, the overall engagement auditor should disclose in the report that certain information has been omitted and the circumstances that make the omission necessary.
3. The overall engagement auditor should evaluate whether this omission could distort the results or conceal improper or illegal practices and revise the report language as necessary to avoid report users drawing inappropriate conclusions from the information presented.
4. When the audit organization is subject to public records laws, the overall engagement auditor should determine whether public records laws could affect the availability of classified or limited use reports and determine whether other means of communicating with management and those charged with governance would be more appropriate. Auditors use professional judgment to determine the appropriate means to communicate the omitted information to management and those charged with governance, considering, among other things, whether public records laws could affect the availability of classified or limited use reports.

440 Prepare Reporting Phase Documentation

1. The auditor should prepare reporting phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the audit, to understand conclusions reached, including evidence that supports the auditor’s conclusions.

Departures from FISCAM

1. When auditors do not comply with applicable FISCAM requirements because of statute, regulation, scope limitations, restrictions on access to records, or other issues affecting the audit, the auditor should document the departure from the FISCAM requirements and the effect of the departure on performing the engagement, engagement conclusions, findings, and any related reports. When documenting departures from the FISCAM requirements, the audit documentation requirements apply to departures from unconditional requirements and from presumptively mandatory requirements when alternative procedures performed in the circumstances were not sufficient to achieve the objectives of the requirements. The auditor may document departures in the FISCAM assessment completion checklist (see app. 600B).

FISCAM Assessment Completion Checklist

1. The auditor should complete the reporting phase portion of the FISCAM assessment completion checklist. See appendix 600B.

1. If fraud is discovered as part of the engagement, the auditor addresses reporting requirements established in GAGAS (2018). [↑](#footnote-ref-1)
2. A deficiency in internal control, including IS controls, exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct, misstatements on a timely basis. [↑](#footnote-ref-2)
3. A significant deficiency is a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those charged with governance. A material weakness is a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the entity’s financial statements will not be prevented, or detected and corrected, on a timely basis. [↑](#footnote-ref-3)
4. The federal government is transitioning to the use of the term controlled unclassified information in place of terms such as sensitive but unclassified or for official use only. [↑](#footnote-ref-4)
5. Original classification is the initial determination by a designated classification authority that an item of information requires, in the interest of national security, protection against unauthorized disclosure. Derivative classification means, in part, incorporating, paraphrasing, restating, or generating in new form information that is already classified, and marking the newly developed material consistent with the classification markings that apply to the source information. [↑](#footnote-ref-5)