Appendix 600B FISCAM Assessment Completion Checklist

Purpose

The *Federal Information System Controls Audit Manual* (FISCAM) assessment completion checklist includes the requirements for conducting an information system (IS) controls assessment based on generally accepted government auditing standards (GAGAS) and requirements prescribed by FISCAM. The FISCAM assessment completion checklist is intended to help auditors determine compliance with FISCAM. It does not include all procedures necessary to achieve the engagement objectives overall.

Instructions

The FISCAM assessment completion checklist contains detailed questions that are organized into four sections: planning, testing, reporting, and conclusions. A response to each question should be documented by either a “Yes,” “No,” or “N/A (not applicable) response in the “Response” column.” For “Yes” responses, a reference to related audit documentation should be noted in the “Explanation and audit documentation reference” column. It is not necessary to create additional documentation to support a “Yes” response. For most questions, “No” responses indicate departures from FISCAM. All departures and their significance, including any effects on the auditor’s report, should be explained in the “Explanation and audit documentation reference” column. An “N/A” response is appropriate when an item does not exist or exists but is considered insignificant to engagement objectives. All “N/A” responses should be explained in the “Explanation and audit documentation reference” column.

The auditor in charge, audit senior, or audit manager prepares and signs this checklist before the assessment completion date, which generally coincides with the date of the auditor’s report. The assistant director and first partner (audit director) review and sign this checklist before the auditor’s report date.

Engagement Information

|  |  |  |  |
| --- | --- | --- | --- |
| Entity name: |  | Job code: |  |

Preparation, Review, and Approval

|  |  |  |  |
| --- | --- | --- | --- |
| Auditor’s report date: |  |  |  |
| Auditor in Charge: |  | Date reviewed: |  |
| Assistant Director: |  | Date reviewed: |  |
| Audit Director: |  | Date reviewed: |  |

Checklist

| **Question** | **Paragraph reference(s) and related GAGAS requirement** | **Response (yes, no, or N/A)** | **Explanation and audit documentation reference** |
| --- | --- | --- | --- |
| Section 1: Planning Phase | | | |
| 1. Did the audit organization assign auditors to conduct the engagement who, before beginning work on the engagement, collectively possessed the competence needed to address the engagement objectives and perform their work? | FISCAM, 220.03  GAGAS (2018), 4.02 |  |  |
| 1. If the auditor used the work of an IT specialist, did the auditor  * determine whether the specialist is competent in their area of specialization; * obtain evidence concerning the specialist’s qualifications and independence; and * evaluate the adequacy of the work for the auditor’s purposes, including   + evaluating the findings and conclusions,   + understanding and evaluating assumptions and methods, and   + evaluating the relevance, completeness, and accuracy of source data that are significant to the work? | FISCAM, 220.06, 220.10  GAGAS (2018), 4.12, 8.82 |  |  |
| 1. Did the auditor determine whether  * other auditors have completed or are completing IS controls work that is relevant to the engagement objectives, and if so * the scope, quality, and timing of the audit work can be relied on in the context of current engagement objectives? | FISCAM, 220.08  GAGAS (2018), 8.80, 8.81 |  |  |
| 1. If the auditor used the work of other auditors, did the auditor  * obtain evidence concerning qualifications and independence of the other auditors and * perform procedures that provided a sufficient basis for using the work? | FISCAM, 220.10  GAGAS (2018), 8.81 |  |  |
| 1. If the auditor determined that the work of the IT specialist was not adequate for the auditor’s purposes, did the auditor ensure additional audit procedures appropriate to the circumstances were performed? | FISCAM, 220.11 |  |  |
| 1. If the engagement is a financial audit and the auditor used the work of an IT specialist or other auditors, did the auditor comply with the requirements in FAM 600? | FISCAM, 220.12 |  |  |
| 1. Did the auditor obtain an understanding of the entity’s IT operations sufficient to plan the engagement? | FISCAM, 230.02 |  |  |
| 1. Did the auditor obtain an understanding of the entity’s information security management program sufficient to   (1) assess the design and implementation of the control environment, entity risk assessment, information and communication, and monitoring components of internal control relevant to the IS controls assessment;  (2) assess IS control risk on a preliminary basis; and  (3) determine the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest? | FISCAM, 240.06 |  |  |
| 1. Did the auditor obtain an understanding of the entity’s information security management program using the FISCAM Framework for Security Management? | FISCAM, 240.08 |  |  |
| 1. Did the auditor identify business processes that are significant to the engagement objectives? | FISCAM, 250.06 |  |  |
| 1. Did the auditor obtain an understanding of significant business processes by performing walk-throughs or alternative audit procedures? | FISCAM, 250.07 |  |  |
| 1. Did the auditor inspect available system documentation that explains the processing and flow of data within the application, as well as interfaces to other information systems and the design of the underlying data management systems? | FISCAM, 250.13 |  |  |
| 1. Did the auditor identify and obtain a sufficient understanding of the business process controls designed to achieve information processing objectives (completeness, accuracy, and validity) based on the auditor’s understanding of the significant business processes? | FISCAM, 250.15 |  |  |
| 1. Did the auditor appropriately identify relevant business process control objectives and the controls intended to achieve those objectives using the FISCAM Framework for Business Process Controls? | FISCAM, 250.16 |  |  |
| 1. If external parties performed any business process controls on behalf of the entity that were intended to achieve the relevant business process control objectives, did the auditor obtain an understanding of such controls sufficient to assess IS control risk on a preliminary basis and design further audit procedures in response to those risks? | FISCAM, 250.19, 250.20 |  |  |
| 1. Did the auditor appropriately identify areas of audit interest at the business process and system levels? | FISCAM, 250.22 |  |  |
| 1. Did the auditor appropriately involve senior members of the engagement team in assessing IS control risk and determining the nature, timing, and extent of IS control tests in response to assessed risks? | FISCAM, 260.05, 260.24 |  |  |
| 1. Did the auditor appropriately obtain an understanding of the inherent risk factors, before consideration of related IS controls, related to information processing objectives relevant to the engagement objectives? | FISCAM, 260.08 |  |  |
| 1. Did the auditor appropriately identify IS risk factors related to information processing objectives relevant to the engagement objectives? | FISCAM, 260.09 |  |  |
| 1. Did the engagement team members adequately discuss fraud risk factors and appropriately assess the risk of fraud occurring that is significant to the engagement objectives? | FISCAM, 260.12  GAGAS (2018), 8.71 |  |  |
| 1. Did the auditor adequately evaluate whether the audited entity has taken appropriate corrective action to address previously reported findings and recommendations that are significant to the engagement objectives, including  * asking management to identify previous engagements or other studies that directly relate to the objectives of the engagement, including whether related recommendations have been implemented, and * using this information to assess risk and determine the nature, timing, and extent of current audit work? | FISCAM, 260.18  GAGAS (2018), 6.11, 7.13, 8.30 |  |  |
| 1. Did the auditor adequately assess the level of IS control risk for each the area of audit interest on a preliminary basis considering  * the auditor’s understanding of inherent risk factors, IS risk factors, fraud risk factors, and results of previous engagements; * the auditor’s determination regarding the likelihood that conditions or events related to the area of audit interest could affect the entity’s ability to achieve the relevant control objectives; and * the impact that such conditions or events (e.g., significance) would have on the entity achieving those objectives? | FISCAM, 260.20, 260.21 |  |  |
| 1. Did the auditor appropriately  * identify relevant general control objectives for each area of audit interest at the system and entity levels and * determine the likelihood that general controls will achieve the relevant general control objectives for each area of audit interest? | FISCAM, 270.04, 270.05 |  |  |
| 1. Did the auditor use the FISCAM Framework (sections 530 through 570) to  * identify general control objectives relevant to the areas of audit interest and * determine the likelihood that general controls applied to the areas of audit interest will achieve the relevant control objectives? | FISCAM, 270.06, 270.09, 270.13, 270.17, 270.21 |  |  |
| 1. Did the auditor determine the likelihood that business process general controls applied to the areas of audit interest will achieve the relevant business process general control objectives for each area of audit interest? | FISCAM, 270.25 |  |  |
| 1. Did the auditor prepare planning phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand the engagement objectives, scope, and approach of the IS controls assessment? | FISCAM, 280.01  GAGAS (2018), 7.34, 8.132 |  |  |
| 1. Did the auditor adequately prepare a written description of each significant business process—including relevant information systems—sufficient to clearly identify the areas of audit interest involved at the business process level, as well as business process controls applied to the significant business processes? | FISCAM, 250.14, 280.02 |  |  |
| 1. Did the auditor adequately prepare a written preliminary assessment of IS control risk for each area of audit interest that identifies the inherent risk factors, IS risk factors, fraud risk factors, and results of previous engagements that significantly increase or decrease the auditor’s assessed level of IS control risk? | FISCAM, 260.06, 280.03 |  |  |
| 1. Did the auditor adequately prepare and update a written planning memo for the IS controls assessment, including  * the identification of significant business processes; * the identification of areas of audit interest at the business process and system levels; * key decisions related to the areas of audit interest; * the identification of relevant user, application, and general control objectives for each area of audit interest, as applicable; and * the auditor’s basis for such scoping decisions? | FISCAM, 280.04 |  |  |
| 1. Did the auditor adequately prepare, update, and complete, as appropriate, a written audit plan, including detailed audit plans, for the IS controls assessment, that describes  * the nature and extent of planned audit procedures for the planning phase; * the nature, timing, and extent of planned audit procedures for relevant control objectives for each area of audit interest; and * other planned audit procedures that are required to be carried out so that the engagement complies with GAGAS? | FISCAM, 280.05, 280.06  GAGAS (2018), 8.03, 8.33 |  |  |
| 1. Did the auditor adequately complete the planning phase portion of this assessment completion checklist? | FISCAM, 280.07 |  |  |
| Section 2: Testing Phase | | | |
| 1. Did the auditor appropriately  * obtain a sufficient understanding of the design of the entity’s IS controls that are likely to achieve the relevant control objectives for each area of audit interest, if implemented and operating effectively, and * identify those controls that achieve the relevant control objectives and improve the efficiency of the auditor’s IS control tests? | FISCAM 320.02, 320.03 |  |  |
| 1. Did the auditor appropriately determine the nature of IS control tests for relevant IS controls? | FISCAM, 330.04, 330.05 |  |  |
| 1. If the auditor used entity-produced information as evidence, did the auditor perform audit procedures to assess the appropriateness of the information prior to performing IS control tests? | FISCAM, 330.07  GAGAS (2018), 8.93 |  |  |
| 1. If the auditor performed inquiries regarding the implementation and operating effectiveness of IS controls, did the auditor appropriately perform other audit procedures in combination with inquiry to obtain sufficient, appropriate evidence? | FISCAM, 330.10  GAGAS (2018), 8.94 |  |  |
| 1. Did the auditor appropriately determine the timing of IS control tests for relevant IS controls? | FISCAM, 330.04, 330.11 |  |  |
| 1. Did the auditor appropriately determine the extent of IS control tests for relevant IS controls, including the use of statistical sampling or nonstatistical selection to identify items for control testing? | FISCAM, 330.04, 330.12, 330.16 |  |  |
| 1. If the auditor used statistical sampling to identify items within a population for control testing, did the auditor appropriately define and determine  * the objectives of the control test (including what constitutes a deviation), * the population (including the sampling unit and time frame), * the method of selecting the sample, and * sample design and resulting sample size? | FISCAM, 330.18, 330.19, 330.20 |  |  |
| 1. If the auditor used statistical sampling to identify items within a population for control testing, did the team appropriately  * use attribute sampling; * determine whether to stratify the population prior to sampling; and * determine a sample size sufficient to obtain sufficient, appropriate audit evidence about the operating effectiveness of relevant IS controls and reduce sampling risk to an acceptably low level? | FISCAM, 330.17, 330.18, 330.21, 330.24 |  |  |
| 1. If the auditor used automated audit tools, did the auditor adequately understand the following for each:  * what are the associated risks, * when to use the tool, * how to operate the tool, * how to analyze the data, and * how to interpret results? | FISCAM, 330.31 |  |  |
| 1. If the auditor used automated audit tools, did the auditor perform a technical review to verify that  * the use and operation of the automated audit tool is appropriate, * the results the tool produces are complete and accurate, and * that the conclusions are supported? | FISCAM, 330.32 |  |  |
| 1. If the auditor used a service organization report as evidence to support the effective design, implementation, and operation of IS controls, did the auditor determine whether the report provides sufficient, appropriate evidence about the design, implementation, and operating effectiveness of IS controls by  * assessing the adequacy of the standards under which the service auditor’s report was issued; * evaluating whether the report is for a period that is appropriate for the auditor's purpose; * evaluating the adequacy of the relevant IS controls that the service organization performed, as described in the service auditor’s report, to achieve relevant control objectives and the relevance and adequacy of the service auditor’s tests of such controls; * evaluating the adequacy of the period covered by the service auditor’s tests of the IS controls the service organization performed and the time elapsed since performance of such tests; * evaluating whether the results of the service auditor’s tests of the IS controls the service organization performed, as described in the service auditor’s report, provide sufficient, appropriate evidence to support the auditor’s conclusions; * determining whether complementary user entity controls that the service organization identified as necessary to support the effectiveness of relevant IS controls the service organization performed are designed, implemented, and operating effectively; and * if applicable, evaluating the adequacy of any IS controls a subservice organization performed that are necessary to support the effectiveness of relevant IS controls that the service organization performed? | FISCAM, 330.36 |  |  |
| 1. If the service organization report excluded the services that a subservice organization performed and those services are relevant to the auditor’s assessment of IS controls, did the auditor adequately apply the same criteria in paragraph 330.36 to the services the subservice organization provided? | FISCAM, 330.40 |  |  |
| 1. If the engagement is a financial audit and the auditor used a service organization report as evidence to support the effective design, implementation, and operation of IS controls, did the auditor comply with the requirements in FAM 640? | FISCAM, 330.37 |  |  |
| 1. Did the auditor use suitable criteria to perform control tests of relevant IS controls? | FISCAM, 340.04  GAGAS 2018, 8.07 |  |  |
| 1. If the engagement is a financial audit, did the auditor comply with requirements for documenting IS controls that are included on the specific control evaluation worksheet as discussed in FAM 390? | FISCAM, 340.05 |  |  |
| 1. Did the auditor adequately evaluate the results of control tests to determine whether IS controls are implemented and operating effectively to achieve the relevant control objectives for each area of audit interest? | FISCAM, 340.06 |  |  |
| 1. Did the auditor appropriately communicate identified control deviations to the entity in sufficient detail for management to consider whether there are additional factors or compensating controls that are relevant to the auditor determining whether  * a control deficiency exists and * the related control objective is achieved? | FISCAM, 340.07 |  |  |
| 1. Did the auditor appropriately determine whether there are specific compensating controls that could mitigate each potential IS control deficiency? | FISCAM, 340.08 |  |  |
| 1. If compensating controls could adequately mitigate a potential IS control deficiency and achieve the related control objective, did the auditor obtain evidence that the compensating controls are designed, implemented, and operating effectively? | FISCAM, 340.08 |  |  |
| 1. Did the auditor appropriately communicate to management the criteria, condition, cause, and effect of the IS control deficiencies identified through the IS controls assessment? | FISCAM, 340.09  GAGAS (2018), 6.17, 7.19, 8.116 |  |  |
| 1. Did the auditor adequately evaluate and sufficiently document the significance of identified IS control deficiencies? | FISCAM, 340.10  GAGAS (2018), 8.54 |  |  |
| 1. Did the auditor adequately reassess, based on the audit procedures performed and the collective evidence obtained, the level of IS control risk for each area of audit interest? | FISCAM, 340.11 |  |  |
| 1. If IS control risk is assessed at moderate or high for one or more of the areas of audit interest, did the auditor appropriately determine the impact of the underlying control deficiencies on the effectiveness of relevant business process controls? | FISCAM, 340.11 |  |  |
| 1. Did the auditor adequately perform and sufficiently document an overall assessment of the collective evidence obtained throughout the IS controls assessment to support the auditor’s findings and conclusions? | FISCAM, 340.15  GAGAS (2018), 8.108 |  |  |
| 1. Did the auditor determine whether the audit procedures performed throughout the IS controls assessment are adequate to reduce audit risk to an acceptably low level? | FISCAM, 340.16  GAGAS (2018), 8.109 |  |  |
| 1. Did the auditor prepare testing phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand from the audit documentation the nature, timing, extent of audit procedures performed and the results of the IS controls assessment, including the significance of any IS control deficiencies identified? | FISCAM, 350.01  GAGAS (2018), 7.34, 8.132 |  |  |
| 1. Before the report was issued, did the auditor adequately prepare audit documentation containing sufficient, appropriate evidence for the auditor’s findings, conclusions, and recommendations, including  * a completed written audit plan reflecting the results of the audit procedures performed, * a written results memo describing the overall assessment of the collective evidence obtained as well as the auditor’s final determinations regarding IS control risk and audit risk, and * detailed audit plans documenting the approach for testing controls for the relevant control objectives for each area of audit interest? | FISCAM, 350.02, 350.03, 350.04, 350.05  GAGAS (2018), 8.133, 8.134, 8.135 |  |  |
| 1. If the auditor used statistical sampling to perform IS control tests, did the auditor prepare written sampling plans that include  * the objectives of each test (including what constitutes a deviation), * the population (including sampling unit and time frame), * the method of selecting the sample, and * the sample design and resulting sample size? | FISCAM, 350.08 |  |  |
| 1. If the auditor used automated audit tools to perform IS control tests, did the auditor prepare relevant audit documentation in sufficient detail to enable a technical review by audit staff independent of the preparer to determine that  * the use and operation of the automated audit tool is appropriate, * the results produced by the automated audit tool are complete and accurate, and * any conclusions are supported? | FISCAM, 350.09 |  |  |
| 1. Did the auditor adequately complete the testing phase portion of this assessment completion checklist? | FISCAM, 350.10 |  |  |
| Section 3: Reporting Phase | | | |
| 1. Did the auditor adequately determine whether they followed the FISCAM methodology? | FISCAM, 420.01 |  |  |
| 1. For financial audit reports, did the overall engagement auditor comply with the reporting requirements, including requirements for classifying control weaknesses, as discussed in FAM 580? | FISCAM, 430.07 |  |  |
| 1. For examination-level attestation engagements, did the overall engagement auditor properly include in the examination report all internal control deficiencies that are considered significant deficiencies or material weaknesses that the auditor identified based on the engagement work performed? | FISCAM, 430.08  GAGAS (2018), 7.42 |  |  |
| 1. For performance audits, did the overall engagement auditor properly include in the audit report any deficiencies in internal control that are significant to the engagement objectives and based upon the audit work performed? | FISCAM, 430.09  GAGAS (2018), 9.29, 9.30 |  |  |
| 1. If the auditor detected deficiencies in internal control that are not significant to the objectives of the performance audit but warrant the attention of those charged with governance, did the team either  * include those deficiencies in the report or * communicate those deficiencies in writing to audited entity officials and refer to that written communication in the audit report? | FISCAM, 430.10  GAGAS (2018), 9.31 |  |  |
| 1. Did the auditor 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? | FISCAM, 430.11  GAGAS (2018), 6.50, 7.48, 9.18 |  |  |
| 1. When presenting findings in the report, did the overall engagement auditor  * place 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; * relate the instances identified to the population or the number of cases examined and quantify the results in terms of dollar value or other measures to give the reader a basis for judging the prevalence and consequences of the findings; and * if the results cannot be projected, limit conclusions appropriately? | FISCAM, 430.13  GAGAS (2018), 6.51, 7.49, 9.21 |  |  |
| 1. For performance audits, did the overall engagement auditor 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? | FISCAM, 430.13  GAGAS (2018), 9.20 |  |  |
| 1. Did the overall engagement auditor  * disclose significant facts relevant to the objectives of the work and known to the team that if not disclosed could mislead knowledgeable users, misrepresent the results, or conceal significant improper or illegal practices; * report conclusions based on the engagement objectives and findings; * provide recommendations for corrective action for any sufficiently developed findings that are significant to the engagement objectives; * make recommendations that flow logically from the findings and conclusions, are directed at resolving the cause of identified deficiencies and findings, and clearly state the actions recommended; and * 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? | FISCAM, 430.14, 430.15, 430.16  GAGAS (2018), 9.19, 9.22, 9.23 |  |  |
| 1. For reports that contain, or may contain, information prohibited from public disclosure because of its confidential or sensitive nature, did the overall engagement auditor appropriately  * request that the source agency perform a classification, security, or sensitivity review of the draft report; * evaluate entity concerns and make appropriate report revisions or redactions, considering legal or regulatory requirements; * if information is excluded from a report, disclose in the report that certain information has been omitted and the circumstances that make the omission necessary; * if information is omitted from the report, 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; and * 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? | FISCAM, 430.17, 430.18, 430.19, 430.20  GAGAS (2018) 6.63, 6.64, 6.65, 7.61, 7.62, 7.63, 9.61, 9.62, 9.63 |  |  |
| 1. Did the auditor prepare reporting phase documentation in sufficient detail to enable an experienced auditor, having no previous connection to the engagement, to understand the conclusions reached, including evidence that supports the auditor’s conclusions? | FISCAM, 440.01  GAGAS (2018), 7.34, 8.132 |  |  |
| 1. Did the engagement team adequately document any departures from the FISCAM requirements and the impact on the engagement and on the auditors’ conclusions? | FISCAM, 440.02 |  |  |
| 1. Did the auditor adequately complete the reporting phase portion of this assessment completion checklist? | FISCAM, 440.03 |  |  |