COURSE SYLLABUS

Army Managers' Internal Control Administrators' Course

This two-day seminar provides the detailed guidance you need to carry out your roles and responsibilities as an Army Internal Control Administrator. It covers the current statutory and regulatory requirements of the Army's Internal Control Program as well as other pertinent guidance. You will fully grasp the underlying Army philosophy on internal controls, the major elements of the Army Manager's Internal Control Program, basic responsibilities of key players in the process, and GAO Internal Control Standards, as well as Enterprise Risk Management. By completing practical exercises, you will gain experience in conducting internal control evaluations and identifying control weaknesses. This course is part of the Certified Government Auditor (CGA) program, Level 1.

Group classes (Live Online) and onsite training are available for this course. For more information, email onsite@graduateschool.edu or visit: https://sdfm.graduateschool.edu/courses/army-managers-internal-control-administrators-course



CustomerRelations@graduateschool.edu • (888) 744-4723

Course Outline

Module 1: Expectations and Responsibilities of Army Managers

- Understand accountability for stewardship (funds, assets) and performance (results, quality, timeliness, cost).
- Relate GPRA/GPRMA requirements and quarterly performance reviews to Army management expectations.
- Connect “tone at the top,” FIAR, and leadership roles to effective internal control.
- Link planning, organizing, staffing, directing, and controlling to a robust control environment.

Module 2: Statutory and Regulatory Framework

- Review FMFIA, OMB Circular A-123 (and Appendices A–D), GAO “Green Book,” DoD 5118.03/DoDI 5010.40, and AR 11-2.
- Explain Statements of Assurance (ICONO/ICOFR/ICOFS), material weakness reporting, and annual timelines.
- Summarize requirements for charge card controls and improper payments reduction.
- Clarify roles and responsibilities across DoD and Army for internal control governance.

Module 3: Definition and Benefits of Effective Internal Controls

- Define risk and “reasonable assurance” in the context of mission accomplishment.
- Distinguish preventive, detective, and corrective controls with common examples.
- Weigh cost–benefit of controls and recognize inherent risk in programs and processes.
- Use key questions to judge whether controls are in place, used as intended, and effective.

Module 4: The GAO Standards for Internal Control

- Apply the five components: Control Environment, Risk Assessment, Control Activities, Information & Communication, Monitoring.
- Identify common control activities (reviews, segregation of duties, documentation, access restrictions).
- Differentiate general vs. application IT controls and their impact on reliability.
- Ensure timely, useful information flows vertically and horizontally to support decisions.

Module 5: When Internal Controls Fail

- Recognize patterns of breakdown leading to waste, fraud, abuse, and mission risk.
- Analyze causes linked to weak control environments, poor risk assessment, or process gaps.
- Review illustrative cases (e.g., property accountability, purchase cards) and remediation steps.
- Quantify impacts to resources, public trust, and operational outcomes.

Module 6: The Army Managers' Internal Control Program

- Describe AMICP structure in alignment with OMB A-123, DoDI 5010.40, and AR 11-2.
- Integrate risk assessment, AU inventories, ICEPs, and corrective action tracking.
- Explain material weakness identification, prioritization, and governance (councils/leadership).
- Connect AMICP to FIAR and audit readiness objectives.

Module 7: Designating Assessable Units & AU Commanders/Managers

- Establish criteria and boundaries for assessable units; maintain a current AU inventory.
- Assign AUM responsibilities and reporting lines for accountability.
- Prioritize AUs by risk and mission significance to focus evaluations.
- Update AU designations as missions, structures, or risks change.

Module 8: Responsibilities of the Internal Control Administrator

- Coordinate policy, training, templates, and program communications.
- Monitor evaluation quality, corrective actions, and documentation completeness.
- Consolidate reports and brief leadership on status, risks, and trends.
- Interface with auditors/inspectors and facilitate data calls.

Module 9: Developing Effective Internal Control Evaluation Plans

- Build a multi-year ICEP that schedules evaluations of key controls across AUs.
- Align plan scope and timing with risk assessments and mission priorities.
- Specify evaluators, methods, criteria, and evidence requirements (e.g., DA Form 11-2).
- Review and update the ICEP annually to reflect evolving risk.

Module 10: Conducting Internal Control Evaluations

- Plan and perform testing for design and operating effectiveness using sufficient, appropriate evidence.
- Apply sampling, tracing, reconciliations, and walkthroughs; document procedures and results.
- Record findings and recommended improvements; communicate results to stakeholders.
- Link evaluation outcomes to corrective action planning and follow-up.

Module 11: Identifying, Reporting, and Correcting Material Weaknesses

- Differentiate control deficiencies, significant deficiencies, and material weaknesses.
- Develop CAPs with milestones, owners, resources, and performance measures.
- Track, validate, and close weaknesses; escalate issues when milestones slip.
- Prepare required reports and updates for leadership and Statements of Assurance.

Module 12: The Annual Statement of Assurance

- Compile ICONO/ICOFR/ICOFS assessments and summarize material weaknesses and status.
- Ensure alignment with OMB A-123 guidance and DoD/Army submission requirements.
- Document supporting subordinate statements and evidence.
- Meet timelines for endorsement and transmittal to higher headquarters.