Headquarters
United States Army Europe
Wiesbaden, Germany

Headquarters
United States Army Installation Management Command,
Europe Region
Sembach, Germany

Army in Europe
Pamphlet 11-2*

25 August 2015

Army Programs

Guide to the USAREUR Managers' Internal Control Program

For the Commander:

MARKUS T. LAUBENTHAL
Brigadier General, GS
Chief of Staff

DWAYNE J. VIERGUTZ
Chief, Army in Europe
Document Management

Summary. This pamphlet describes processing procedures for implementing, conducting, and completing requirements for the Managers' Internal Control Program for organizations and personnel assigned to USAREUR as prescribed in AE Regulation 11-2.

Applicability. This pamphlet applies to HQ USAREUR staff offices and USAREUR major subordinate commands.

Records Management. Records created as a result of processes prescribed by this pamphlet must be identified, maintained, and disposed of according to AR 25-400-2. Record titles and descriptions are on the Army Records Information Management System website at *https://www.arims.army.mil*.

Supplementation. Organizations will not supplement this pamphlet without approval of the Manpower and Management Division, Office of the Deputy Chief of Staff, G8, HQ USAREUR.

Suggested Improvements. The proponent of this pamphlet is the Manpower and Management Division, Office of the Deputy Chief of Staff, G8, HQ USAREUR (mil 537-8038). Users may send suggested improvements to this pamphlet by e-mail to the Manpower and Management Division at *USARMY Baden-Wurttemberg USAREUR List G8 Manpower Division*.

Distribution. This pamphlet is available only electronically and is posted in the Army in Europe Library & and Publishing System (AEPUBS) at *https://aepubs.army.mil/*.

CONTENTS

---

1. PURPOSE

This pamphlet provides guidance and procedures—

a. For implementing, evaluating, monitoring, and reporting control activities to support the USAREUR Managers' Internal Control Program (MICP).

b. To help meet responsibilities prescribed in AE Regulation 11-2.

2. REFERENCES

Appendix A lists references.

3. EXPLANATION OF ABBREVIATIONS AND TERMS

The glossary defines abbreviations and terms.

4. STANDARDS FOR INTERNAL CONTROLS

a. Internal control (IC), in the broadest sense, includes management's plan of organization, methods, and procedures to meet the organization's goals. IC is an integral component of an organization's management that provides reasonable assurance that the organization's objectives are being achieved. In its Standards for Internal Control in the Federal Government ("Green Book"), the U.S. Government Accountability Office (GAO) classifies objectives and related risks (glossary) into the following three categories:

(1) Effectiveness and efficiency of operations. Effective operations produce the intended results from operational processes while efficient operations do so in a manner that minimizes the waste of resources.

(2) Reliability of both financial and nonfinancial reporting for internal and external use.

(3) Compliance with applicable laws and regulations.

b. The safeguarding of assets is a subset of all of these objectives. IC should be designed to provide reasonable assurance, not absolute assurance, regarding the prevention or prompt detection of unauthorized acquisition, use, or disposition of assets. An effective IC system increases the likelihood that an entity will achieve its objectives. As part of designing an IC system, management defines the objectives in specific and measurable terms to identify, analyze, and respond to risks related to achieving those objectives (para 6a). IC does not consist of one single event but a series of actions that occur during the operation of an "assessable unit (AU)" (glossary). IC is recognized as an integral part of the operational processes management uses to guide its operations rather than as a separate system within an AU.

c. These standards, however, are not intended to limit or interfere with duly granted authority related to legislation, rulemaking, or other discretionary policymaking in an organization.

d. Management is responsible for developing and maintaining IC activities through a hierarchical structure of five components with their principles and relevant attributes. The five components of IC must be effectively designed, implemented, and operating together in an integrated manner for an IC system to be effective. The five components of IC are the following:

(1) Control Environment.

(a) The control environment is the foundation of an IC system. It provides the discipline and structure to help an entity achieve its control objectives. It influences how objectives are defined and how control activities are structured. The control environment is the organizational structure and culture created by management and employees to sustain organizational support for an effective IC system. When designing, evaluating, or modifying the organizational structure, management must clearly demonstrate its commitment to competence in the workplace. Management must clearly—

1. Set the tone at the top.

2. Set standards of conduct and adhere to those standards.

3. Define areas of authority and responsibility and appropriately delegate authority and responsibility.

4. Establish a suitable hierarchy for reporting.

5. Support appropriate human-capital policies to attract, develop, and retain competent individuals.

6. Evaluate performance and hold individuals accountable for their IC responsibilities.

7. Establish and retain documentation of the IC system.

8. Demonstrate a commitment to integrity and ethical values.

(b) The organizational culture is also crucial within this standard. The culture should be defined by management's leadership in setting values of integrity and ethical behavior but is also affected by the relationship between the organization and central oversight agencies. Management's philosophy and operational style will set the tone within the organization. Management's commitment to establishing and maintaining effective IC should cascade down and permeate the organization's control environment, which will aid in the successful implementation of an effective IC system.

(2) Risk Assessment (para 6b).

(a) A risk assessment or analysis identifies the risks the organization faces as it seeks to achieve its objectives and provides the basis for developing appropriate responses to risks. A precondition for an effective risk assessment is the establishment of clear, consistent agency goals and objectives to enable the identification of risks and define risk tolerances (that is, the acceptable level of variation in performance relative to achieving the objectives) at both the AU and at the activity (program or mission) level. Management should identify, analyze, and respond to risks related to achieving the defined objective; and identify, analyze, and respond to significant changes that could affect the IC system. Management defines an objective in specific and measurable terms to enable the design of control activities for related risks so they are understood at all levels of the AU. Specifically, a risk assessment is conducted by determining the following three estimates of the risk significance:

1. The magnitude or effect of potential loss.

2. The likelihood or probability that a loss will occur.

3. The nature of the deficiency, which involves factors such as the degree of subjectivity involved in the deficiency and whether the deficiency arises from fraud or misconduct.

(b) Management should identify internal and external risks that may prevent the organization from meeting its objectives. When identifying risks, management should also consider previous findings, for example, auditor reviews, internal management reviews, or noncompliance with laws and regulations. In addition, the "key control" (glossary) employed to reduce risk should not exceed the benefits derived.

(c) To identify risks, management considers the types of risks that affect the organization. This includes both inherent and residual risk. Inherent risk is the risk an organization faces if management fails to respond to the risk. Residual risk is the risk that remains after management's response to an inherent risk. Management's lack of response to either risk could cause deficiencies in the IC system. Risk-identification methods may include qualitative and quantitative ranking activities, forecasting and strategic planning, and consideration of deficiencies identified through audits and other assessments. Based on the selected risk response, management designs the specific actions to respond to the analyzed risks. Performance measures are used to assess whether or not risk-response actions enable the organization to operate within the defined risk tolerances.

(d) The risk-assessment phase is the first step in evaluating controls and requires familiarity with both the control process and factors that might lead to deviations in planned control procedures or other ineffective outcomes. This phase determines the ability of the control to prevent or detect material errors in reporting and assesses whether the "control risk" (glossary) is low, moderate, or high. For efficiency reasons, high-risk control processes do not require testing. Instead, these specific processes should be evaluated to identify the deficient controls and determine what corrective actions are needed to improve these processes to establish effective control procedures. Conversely, low- and moderate-risk controls must be tested to determine their effectiveness to meet control objectives. By documenting the specific control-effectiveness test methods, the assessment also serves as a basis for the actual test plan (para 6e).

(3) Control Activities (para 6d).

(a) Control activities or techniques are the policies, procedures, and mechanisms that help mitigate the risks that were identified during the risk-assessment process. Management periodically reviews the policies, procedures, and related control activities for continued relevance and effectiveness to achieving the organization's objectives. The following are examples of common categories of IC activities:

1. Controlling information processing.

2. Physical control over vulnerable assets.

3. Segregation of duties.

4. Accurate and timely recording of transactions and event.

5. Access restriction to and accountability for resources and records.

6. Appropriate documentation of transactions.

(b) Management may design both preventive and detective control activities. A preventive control activity prevents an organization from failing to achieve an objective or address a risk. A detective control activity discovers when an organization is not achieving an objective or addressing a risk before the organization's operation has concluded and corrects the actions so that the organization achieves the objective or addresses the risk. Control activities can be implemented in an either automated or manual manner. Automated control activities tend to be more reliable because they are less susceptible to human error and are typically more efficient. Entity-level controls are controls that have a pervasive effect on an entity's IC system and may pertain to multiple components. Transaction control activities are actions built directly into operational processes to support the entity in achieving its objectives and addressing related risks. To determine the necessary level of precision for a control activity, management evaluates the following:

1. Purpose of the Control Activity. A control activity that is designed to prevent or detect generally is more precise than a control activity that merely identifies and explains differences.

2. Level of Aggregation. A control activity that is performed at a lower level generally is more precise than one performed at a higher level. For example, an analysis of obligations by budget-object class normally is more precise than an analysis of total obligations for the entity.

3. Consistency of Performance. A control activity that is performed routinely and consistently generally is more precise than one performed sporadically.

4. Correlation to Relevant Operational Processes. A control activity that is directly related to an operational process generally is more likely to prevent or detect a risk than a control activity that is only indirectly related to an operational process.

(c) A control activity cannot be effectively implemented if it was not effectively designed. A deficiency in design exists when a control activity necessary to meet a control objective is missing or when a control activity operating as designed does not meet the control objective. Management clearly documents internal control and all transactions and other significant events in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained. Management also evaluates information-processing objectives to meet the defined information requirements. Information-processing objectives may include the following:

1. Completeness. Transactions are recorded and not understated.

2. Accuracy. Transactions are recorded at the correct amount in the right account (and on a timely basis) at each stage of processing.

(d) Control activities also need to be in place for information systems (ISs) as general and application controls. General control applies to all IS components such as the mainframe, network, and end-user equipment and includes agency-wide security-program planning, management, and control of data-center operations, system-software acquisition, and maintenance. Application control should be designed to ensure that transactions are properly authorized and processed accurately and that the data is valid and complete. Controls should be established at an application's interfaces to verify inputs and outputs. General and application control over ISs are interrelated; both are needed to ensure complete and accurate information processing. Due to the rapid changes in information technology, control activities must adjust to remain effective.

(4) Information and Communications. An IS consists of the people, processes, data, and technology that management organizes to obtain, communicate, or dispose of information. Communicating quality information both internally and externally is vital for ensuring AU objectives are achieved. Information should be communicated to relevant personnel at all levels within an organization. The information should be relevant, reliable, current, complete, accurate, accessible, and timely. It is crucial that an agency also communicates with outside organizations, whether providing or receiving information. External parties include suppliers, contractors, service organizations, regulators, external auditors, Government entities, and the general public. High-quality information is communicated down, across, up, and around reporting lines to all levels of the AU. When communicating information, the audience, nature of information, availability, cost, and legal or regulatory requirements should be considered.

(5) Monitoring.

(a) An IC system assesses the quality of performance over time and ensures that the findings of audits and other reviews are promptly resolved. Management should establish and operate activities to monitor the IC system, evaluate results, and correct identified IC deficiencies on a timely basis. Management establishes a baseline for monitoring the IC system. The baseline is the current state of the IC system compared with management's design of the IC system. Once established, management can use the baseline as criteria to evaluate the IC system and make changes to reduce the difference between the criteria and the current condition. As part of monitoring, management determines when to revise the baseline to accommodate changes in the IC system. Management uses the results of ongoing monitoring and separate evaluations to determine the effectiveness of the IC system. The scope and frequency of separate evaluations depend primarily on the assessment of risks, effectiveness of ongoing monitoring, and the rate of change within the entity and its environment.

(b) Monitoring the effectiveness of control activities should occur in the normal course of business. In addition, periodic reviews, reconciliations, or comparisons of data should be included as part of the regular assigned duties of personnel. Periodic assessments should be integrated as part of management's continuous monitoring of the IC system, which should be ingrained in the agency's operations. If an effective continuous monitoring program is in place, it can level the resources needed to maintain effective control activities throughout the year.

(c) Identified deficiencies, whether found through internal review or an external audit, should be reported to the personnel and management responsible for that process and be evaluated and corrected on a timely basis. A systematic process should be in place for addressing deficiencies.

e. An effective IC system provides reasonable assurance that the organization will achieve its objectives. It requires that each of the five components with their principles and relevant attributes of IC (d above) are effectively designed, implemented, and operating together in an integrated manner. To determine if an IC system meets these requirements, management evaluates the effect of IC deficiencies on the IC system. In evaluating operating effectiveness, management determines if controls were applied at relevant times during the evaluation period, the consistency with which they were applied, and by whom or by what means they were applied. A deficiency in operation exists when a properly designed control does not operate as designed, or when the person performing the control does not have the authority or competence necessary to apply the control effectively. Management evaluates the significance of a deficiency by considering the magnitude of effect, likelihood of occurrence, and nature of the deficiency. The nature of the deficiency involves factors such as the degree of subjectivity involved in the deficiency and whether the deficiency arises from fraud or misconduct.

f. The cube in figure 1 illustrates how the five components of IC apply to staff at all organizational levels and to all categories of objectives (Green Book).

5. SEGMENTATION OF THE ORGANIZATION

A precondition for implementing the MICP in an organization is to divide mission areas along organizational lines into AUs. All operations in USAREUR are subject to the requirements of the Federal Managers Financial Integrity Act of 1982 (FMFIA) (Public Law 97-255). The senior responsible official (SRO) of the AU may determine how far the segmentation should progress to achieve adequate oversight of IC responsibilities. Segmentation of AUs should be of appropriate nature and size so that a single manager may be held responsible for the evaluation of the IC system. To the extent practical, AUs should standardize associated IC activities for the operation of common functions and activities throughout the AU. AUs must—

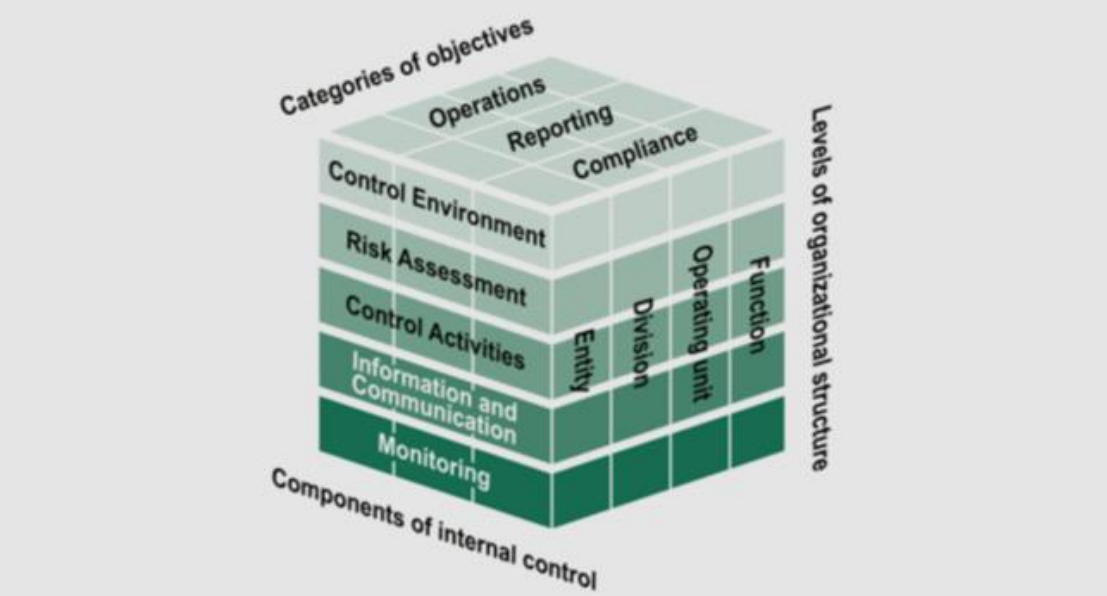


Figure 1. Application of Internal Control Components

a. Have clear limits or boundaries (organizational, functional, programmatic, or a combination of the three) and be identifiable to a specific responsible "assessable unit manager" (AUM) (glossary) or the SRO.

b. Be small enough to allow observations that provide reasonable assurance that control activities are in place and adequate. The AUM or designated representative of the program area should actively participate in the assessment process.

c. Be large enough to identify the effect any detected "material weakness" (glossary) has on the mission.

d. Table 1 illustrates the segmentation of a division as an AU into sub-assessable units.

Table 1 **Segmentation of an Assessable Unit into Sub-assessable Units**	
Assessable Unit: Manpower and Management Division	
Sub-assessable Unit Name	**Sub-assessable Unit Manager**
1. Manpower Analysis and Studies Branch	J. Doe, Chief of Manpower Studies
2. Manpower Analysis and Execution Branch	M. King, Chief of Manpower Execution
3. Business Operation	Y. Smalls, Chief of Business Operations
4. Managers' Internal Control Program	N. Jones, Internal Control Administrator

6. PROCEDURES FOR IMPLEMENTING THE MANAGERS' INTERNAL CONTROL PROGRAM

The MICP is a continuous cycle of actions to be conducted within daily operations and not considered a once-a-year program. Figure 2 is a depiction of that process, explained in paragraphs 6a through h.

Figure 2. Internal Control Process

a. Defining Organizational Objectives.

(1) An organization's objectives are the main reason for its existence. These objectives describe what the organization is trying to achieve. Management defines objectives in specific and measurable terms so they are understood at all levels of the entity. This involves the clear definition of what is to be achieved, who is to achieve it, how it will be achieved, and the timeframe for achievement.

(2) The following are recommended sources to use and steps to take to develop control objectives for an organization:

(a) Reviewing objectives in the USAREUR Campaign Plan and functions described in AE Regulation 10-5 as the key drivers.

(b) Reviewing significant observations and outcomes from recent staff visits, senior management conferences, and other related events that may apply to the area of responsibility.

(c) Soliciting key concerns from counterparts within and outside of the AU or USAREUR.

(d) Reviewing functions being performed throughout the AU to ensure legitimacy and consistency with assigned organizational missions and functions.

(e) Consulting with SROs and AUMs for areas of concern.

b. Conducting a Risk Analysis and Determining the Risk Impact.

(1) Purpose. The purpose of a risk assessment or analysis is to identify, analyze, and respond to "risks" (glossary) in the daily business that could keep the AU from meeting its objectives. Due to their nature, risks cannot be completely eliminated. Risk is not detrimental as long as it is recognized and properly controlled. Identifying, analyzing, and responding to change is similar to, if not part of, the entity's regular risk-assessment process. Management analyzes the effect of identified changes on the IC system and responds by revising the IC system on a timely basis, when necessary, to ensure its effectiveness. Once a risk is identified, a decision should be made on how to manage the risk and what actions should be taken. Primary focus is placed on areas of greatest significance:

(a) Achieving or failing to achieve a program's missions, objectives, or goals.

(b) Producing erroneous reports or data.

(c) Allowing unauthorized uses of resources.

(d) Committing illegal or unethical acts.

(e) Receiving adverse or unfavorable opinions.

(f) Susceptibility to waste, fraud, and mismanagement.

(2) Risk Tolerances. Risk tolerance is the acceptable level of variation in performance relative to the achievement of objectives. Risk tolerances are initially set as part of the objective-setting process. Management evaluates whether risk tolerances enable the appropriate design of control activities by considering whether they are consistent with requirements and expectations for the defined objectives. If risk tolerances for defined objectives are not consistent with these requirements and expectations, management revises the risk tolerances to achieve consistency. Depending on the category of objectives (para 4a), risk tolerances may be expressed as follows:

(a) Operations. For operations, risk tolerance is the level of variation in performance in relation to a risk.

(b) Reporting. For nonfinancial reporting, risk tolerance is the level of precision and accuracy, involving both qualitative and quantitative considerations, that is required to meet the needs of the nonfinancial report user. For financial reporting, risk tolerance is the judgment about materiality that is made in light of surrounding circumstances, involving both qualitative and quantitative considerations, and is affected by the needs of financial report users and the size or nature of a misstatement.

(c) Compliance. The concept of risk tolerance does not apply to this category. An entity is either compliant or not compliant.

(3) Criteria. Before conducting a risk analysis, the following questions needs to be answered:

(a) Has management defined risk tolerances for the defined objectives?

(b) Are clear-cut policies and guidance regarding controls, objectives, and techniques provided to all levels of the organization?

(c) Do repeated audit findings exist or are audits performed only at a minimum?

(d) Are managers open and responsive to recommendations from outside entities?

(e) Does management monitor control activities and provide oversight to identify exceptions from normal program operations?

(f) Is there an active quality internal review staff to periodically ensure that control activities are functioning as intended?

(g) Are IC duties of employees and supervisors properly segregated (for example, timekeeping, certification, payment processing)?

(h) Were audit or review findings corrected in a timely manner?

(i) Does management identify control weaknesses before they are identified by an inspector, auditor, the media, or the public?

(j) Do managers and evaluators also consider factors that would—

1. Prevent management from meeting program objectives?

2. Subject the organization to unwarranted potential loss of assets and revenues?

3. Cause management to provide unreliable information and reports about a mission area?

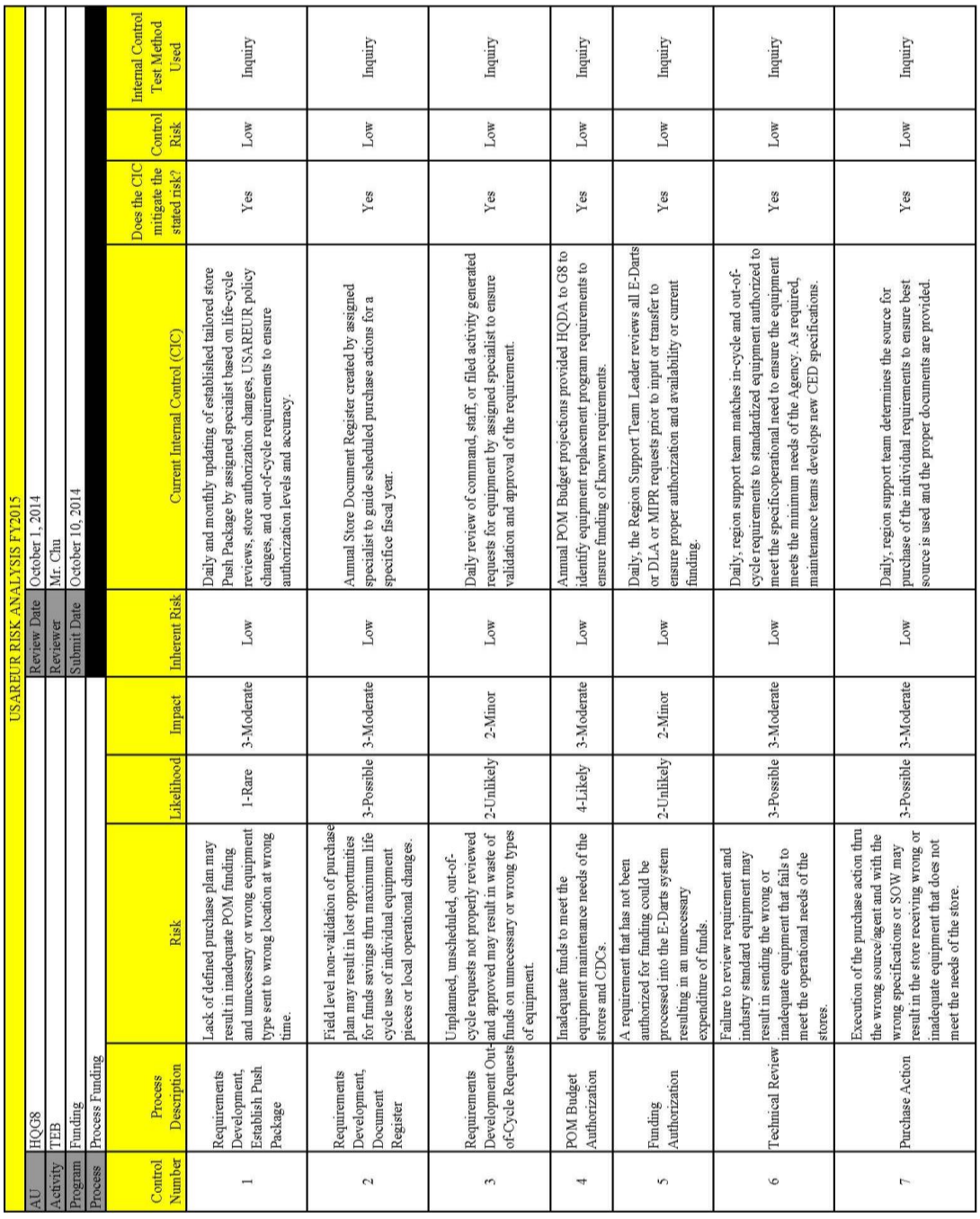
4. Encourage deviations from established procedures?

5. Create an adverse public opinion?

(k) What is the experience of the person who is assigned to perform the IC technique? Less experience usually relates to a higher risk of issues occurring.

(4) Sample Risk Analysis. To conduct a risk analysis, AUs may use the sample risk analysis in figure 3 (available at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx?RootFolder=%2Fhq%2Fg8%2FMMD%2FMASB%2FStewardship%20Team%2FShared%20Documents%2FMICP%20Tools&FolderCTID=0x012000B406588AF6AC12498FF8DADEF954F42A&View={A42FF4DB-D463-4757-81AE-434C494A6DB7}*). Subparagraphs (a) through (j) explain how to complete a risk analysis:

(a) Top rows. These rows are self-explaining. The AU code may be retrieved from appendix B.



USAREUR RISK ANALYSIS FY2015

AU	HQG8	Review Date	October 1, 2014
Activity	TEB	Reviewer	Mr. Chu
Program	Funding	Submit Date	October 10, 2014
Process	Process Funding		

Control Number	Process Description	Risk	Likelihood	Impact	Inherent Risk	Current Internal Control (CIC)	Does the CIC mitigate the stated risk?	Control Risk	Internal Control Test Method Used
1	Requirements Development, Establish Push Package	Lack of defined purchase plan may result in inadequate POM funding and unnecessary or wrong equipment type sent to wrong location at wrong time.	1-Rare	3-Moderate	Low	Daily and monthly updating of established tailored store Push Package by assigned specialist based on life-cycle reviews, store authorization changes, USAREUR policy changes, and out-of-cycle requirements to ensure authorization levels and accuracy.	Yes	Low	Inquiry
2	Requirements Development, Document Register	Field level non-validation of purchase plan may result in lost opportunities for funds savings thru maximum life cycle use of individual equipment pieces or local operational changes.	3-Possible	3-Moderate	Low	Annual Store Document Register created by assigned specialist to guide scheduled purchase actions for a specifice fiscal year.	Yes	Low	Inquiry
3	Requirements Development Out-of-Cycle Requests	Unplanned, unscheduled, out-of-cycle requests not properly reviewed and approved may result in waste of funds on unnecessary or wrong types of equipment.	2-Unlikely	2-Minor	Low	Daily review of command, staff, or filed activity generated requests for equipment by assigned specialist to ensure validation and approval of the requirement.	Yes	Low	Inquiry
4	POM Budget Authorization	Inadequate funds to meet the equipment maintenance needs of the stores and CDCs.	4-Likely	3-Moderate	Low	Annual POM Budget projections provided HQDA to G8 to identify equipment replacement program requirements to ensure funding of known requirements.	Yes	Low	Inquiry
5	Funding Authorization	A requirement that has not been authorized for funding could be processed into the E-Darts system resulting in an unnecessary expenditure of funds.	2-Unlikely	2-Minor	Low	Daily, the Region Support Team Leader reviews all E-Darts or DLA or MIPR requests prior to input or transfer to ensure proper authorization and availability or current funding.	Yes	Low	Inquiry
6	Technical Review	Failure to review requirement and industry standard equipment may result in sending the wrong or inadequate equipment that fails to meet the operational needs of the stores.	3-Possible	3-Moderate	Low	Daily, region support team matches in-cycle and out-of-cycle requirements to standardized equipment authorized to meet the specificoperational need to ensure the equipment meets the minimum needs of the Agency. As required, maintenance teams develops new CED specifications.	Yes	Low	Inquiry
7	Purchase Action	Execution of the purchase action thru the wrong source/agent and with the wrong specifications or SOW may result in the store receiving wrong or inadequate equipment that does not meet the needs of the store.	3-Possible	3-Moderate	Low	Daily, region support team determines the source for purchase of the individual requirements to ensure best source is used and the proper documents are provided.	Yes	Low	Inquiry

Figure 3. Sample Risk Analysis

(b) Column 1 (Control Number). This column shows the numerical control number for each risk and associated control activity. If a risk has more than one control, a lower case letter is added in parenthesis after the first number to account for the controls.

(c) Column 2 (Process Description). This is a short description of the specific key process within the AU that is being evaluated. Each AU will define the key processes within that unit. Within each process, separate risks and controls will be identified. It is not necessary to account for every process within the AU, only those processes that define the primary "key" tasks within the AU.

(d) Column 3 (Risk). This column describes the risk that could occur if key steps within a key process are not occurring at all, not occurring on time, or not being performed accurately. Once the key steps have been identified in the key processes, identifying the risks is very easy. Special attention should be paid to ensuring that the risks are stated clearly and accurately. All of the remaining analysis flows from the proper definition of the risk.

(e) Column 4 (Likelihood) and Column 5 (Impact). These two factors are used to quantify management's judgment as to the severity of each risk. Each factor is measured on a scale from 1 to 5, with 1 being the lowest and 5 being the highest level. The assessment of likelihood and impact constitutes the analysis of the inherent-risk level. Inherent risk is the level of risk present in a situation before the situation is controlled with risk-mitigating actions.

1. Likelihood. The likelihood of occurrence is the probability that an unfavorable event would occur if there were no control activities or limited control activities. The existence of a design weakness is sufficient to conclude that there is more than a rare likelihood that the control activity would not have been effective. For each risk, simply ask how often the situation arises and make a determination. Use the definitions of likelihood levels in table 2 to assist in the rating.

2. Impact. This factor is a measure of how severe the consequences would be if this risk did occur. Use the definitions of the impact levels in table 2 to assist in the rating.

(f) Column 6 (Inherent Risk). Based on the likelihood and impact levels identified in columns 4 and 5, the inherent risk will be designated as either "high," "moderate," or "low." Certain combinations of impact and likelihood will add up to different risk levels as identified in the risk matrix (table 2). All controls will be listed irrespective of the risk level they mitigate; however, resources are only expended on testing key controls.

(g) Column 7 (Current Internal Control (CIC)). This column describes the actions managers and their employees actually take to mitigate the risk. Sometimes, directives and manuals will direct a certain action, when, in fact, the action taken is different or no action is taken at all. There may be instances where a control does not fit easily into a format. In these cases, the best effort should be made to provide as much detail about what is being done to mitigate the risk. Detail is important because how we define our controls leads directly to defining how we test their effectiveness (para 6e).

(h) Column 8 (Does the CIC mitigate the stated risk?). This question asks the manager to make a judgment as to whether a control is working effectively. For many processes in the AU, managers know that a particular control is not catching mistakes because they waste inordinate amounts of time fixing the mistakes the control should have caught the first time. Answering "yes" to all of the questions would be a mistake and an even greater waste of time if the manager knows that a control is not working. Each of these control activities that mitigate a high risk must then be evaluated to identify the deficient control activity and determine what "corrective actions" (glossary) are needed to establish effective control procedures. If the control activity is working, it must be tested and proven to be working effectively. Verifiable proof must be available for the USAREUR Managers' Internal Control Program Administrator (MICPA) to review or assess the control activity. If a control activity is not working, and it was known not to be working, all the testing time was wasted. The bottom line is that the evaluation of the effectiveness of control activities will no longer be a subjective, but a quantifiably objective.

Table 2
Risk Matrix

Likelihood	Impact				
	Insignificant (no impact on program objectives; very low impact on financial information)	**Minor** (potential impact on program objectives)	**Moderate** (some impact on program objectives)	**Major** (high impact on program objectives)	**Catastrophic** (failure to meet program objectives; significant human, equipment, or financial loss)
Almost certain (event is expected to occur in most circumstances, the chance is higher than 90%)	Moderate	Moderate	High	High	High
Likely (event will probably occur in most circumstances, the chance is between 50% and 90%)	Moderate	Moderate	High	High	High
Possible (event could occur sometime, the chance is between 10% and 50%)	Low	Moderate	Moderate	High	High
Unlikely (event could occur in remote circumstances, the chance is between 3% and 10%)	Low	Low	Moderate	Moderate	High
Rare (event may only occur in exceptional circumstances, the chance is less than 3%)	Low	Low	Low	Moderate	High

(i) Column 9 ("Control Risk" glossary)). The assigned inherent risk and the determination whether the CIC mitigates the risk will define the control-risk level. Both the AU "process owner" (glossary) and the AUM should agree on the risk level. If the inherent risk is assessed as "high" or "moderate," and the CIC does not mitigate the risk, the control risk must be assessed as "high" and the CIC must be redesigned to mitigate the risk. If the inherent risk is assessed as "high" or "moderate," and the CIC does mitigate the risk, the control risk will be assessed as "moderate" or "low," respectively. The importance of the rating distinction is that only control activities that mitigate low and moderate risks will be tested to determine their effectiveness in meeting their control objectives. For efficiency reasons, high-risk control processes are not required to be tested. Instead, these specific processes should be evaluated to identify the deficient controls and determine what corrective actions are needed to improve these processes to establish effective control procedures.

(j) Column 10 (Internal Control Test Method Used). The last column is for identifying how to test the effectiveness of each control activity. The test that will most accurately reveal the effectiveness of the control activity should be selected. (Paragraph 6e provides more details on testing control activities.)

(5) Risk Impact. Each risk should be assessed for the impact on the objective, mission, and goal accomplishment if the risk occurs. Use the risk matrix in table 2 to assign either the "high," "moderate," or "low" risk label by identifying the highest likelihood of occurrence and matching it with the level of impact if the risk identified does occur.

(6) Responses to Risk. Management designs responses to the analyzed risks so that risks are within the defined risk tolerance for the defined objective. Management designs overall risk responses for the analyzed risks based on the significance of the risk and defined risk tolerance. These risk responses may include the following:

(a) Acceptance. No action is taken to respond to the risk.

(b) Avoidance. Action is taken to stop the operational process or the part of the operational process causing the risk.

(c) Reduction. Action is taken to reduce the likelihood or magnitude of the risk.

(d) Sharing. Action is taken to transfer or share risks across the entity or with external parties, such as insuring against losses.

c. Determining Internal Control Objectives.

(1) After identifying the most significant risks, IC objectives need to be developed. The objective should be the statement of management's commitment to implement techniques that will ensure the goal or the positive outcome management wants to achieve. The IC objective should start with words such as "ensure," "make sure," "make certain," "guarantee," or similar. The following are recommended sources you should review and steps you need to take to develop control objectives for your organization.

(a) Reviewing objectives in the USAREUR Campaign Plan and functions described in AE Regulation 10-5 as the key drivers.

(b) Examine your programs and procedures in relation to the GAO internal control standards (para 4).

(c) Review current plans of your unit's internal review element, the inspector general, and the organization inspection program for areas of concern that are not included in the USAREUR Campaign Plan or AE Regulation 10-5.

(d) Identify high-risk areas found through external audits, internal reviews, and GAO reports that may have implications for your AU.

(e) Review significant observations and outcomes from recent staff visits, senior management conferences, and other related events that may apply to your area.

(f) Review functional regulations, directives, and policies.

(g) Review functions being performed throughout the AU to ensure legitimacy and consistency with assigned organizational missions and functions.

(h) Review performance plans, reports, systems, applications, financial statements and systems, and daily operational information to identify possible concerns and deficiencies.

(i) Solicit SRO and AUM input on areas of concern.

(2) The following are examples of IC objectives:

(a) Ensure all employees complete mandatory training and that the training is documented.

(b) Make sure that at least 95 percent of time and attendance is accurately reported in accordance with USAREUR policies and directives.

(c) Ensure that USAREUR personnel safely collect, record, store, and dispose of property items in accordance with guidance from the property book officer and regulations.

(d) Ensure the proper handling and storage of all classified materials according to DOD, HQDA, and USAREUR policies and procedures.

d. Developing Internal Control Techniques.

(1) IC techniques are significant activities, processes, procedures, and tasks implemented or needed to provide "reasonable assurance" that the IC objective will be met. The need for techniques is dynamic. As situations change, the types and numbers of techniques may also change. The techniques should be updated as needed based on changes in regulations, directives, and policies. Techniques must also be cost-effective. The cost of performing a technique should not outweigh its benefit or control. For example, does the AUM or SRO need to sign a purchase request for a box of pens? Is the signature of the manager directly above the requester sufficient? The following should be considered when developing IC techniques:

(a) Determine the appropriate number of techniques to mitigate your risk.

(b) Is there a process to designate an employee to be responsible for the objective?

(c) Is that designation in writing? If not, put it in writing with responsibilities listed.

(d) Is there a procedure, desktop instruction, or process involved in achieving the objective?

(e) Is the procedure in writing? If not, document the steps of the procedure.

(f) How often should the written procedure be reviewed and updated? At least annually?

(g) Has the person responsible for performing the procedure or process been adequately trained on the procedure or process? Is the training documented?

(h) Is an alternate person required or trained in case the primary person is unavailable?

(i) What are the foundations of the work required (for example, databases, lists, formal records or files)? Who is responsible for maintaining or updating them?

(j) Is the data-entry process checked for accuracy? Is there a required accuracy level for data input?

(k) What are the inputs or documents required (for example, filled out checklists or forms, reviews, or analyses)?

(l) What are the outputs of the work (for example, periodic reports, briefings, memorandums)? How often are they produced? Are the outputs required to be entered into a database (for example, General Fund Enterprise Business System, Automated Time Attendance and Production System (ATAAPS), Property Book Unit Supply Enhanced)?

(m) Do different levels of authority see different outputs? What are those levels and outputs?

(2) Once a technique is designed, the technique will be assigned to a technique process owner (TPO) to ensure that the technique is applied to achieve the desired control objective. The TPO may be the branch chief or the employee who is responsible for the specific task or function. The TPO must not be a contractor.

(3) The TPO is also responsible for documenting corrective actions that are required based on the assessment results. The TPO is responsible for maintaining the "assessment documentation" (glossary) and reporting the results to the AU "internal control administrator" (ICA) (glossary) or AUM. If the TPO is not the person performing the assessment on the technique, the TPO will be the point of contact for the assessment and responsible for providing any required information and documentation.

(4) Once you have determined the technique and TPO, a reviewing cycle for the technique needs to be determined. This reviewing cycle needs to be based on the risk level assigned to the technique as follows:

(a) Quarterly (at a minimum) for high-risk-level techniques.

(b) Semiannually for moderate-risk-level techniques.

(c) Annually for low-risk level-techniques.

e. Conducting Internal Control Assessments through Testing.

(1) The Office of Management and Budget (OMB) Circular A-123 and the Green Book require an assessment of IC techniques to be documented on a test plan to ensure that the assessment was completed, properly reviewed, and that the testing process was valid. The assessment of IC techniques has to be based on actually testing the IC activities, processes, and procedures to ensure that IC systems exist, are implemented, and working effectively. A determination of the effectiveness of an IC system is obtained during the testing process. Corrective actions are required if testing determines a control to be moderately effective or ineffective.

(2) An individual assessment of the potential effectiveness of each technique should be made considering the risk of something going wrong and the controls that are designed, working, and in place to prevent or detect such problems. Procedures required to perform the assessment include inquiries of appropriate personnel; inspection of documents, reports, or electronic files; observation of the application of specific controls; and re-performance to ensure the control design is correct and the assessor is able to reach the same results as the previous tester. This is sometimes referred to as a "walk-through" and help assessors ensure their understanding of the controls. Assessments should identify controls as effective, moderately effective, or not effective.

(3) The frequency of assessing IC techniques should be based on the risk level assigned to a technique. The higher the risk of something going wrong with the control activity, the more important it is to ensure that the activity is working the way it is supposed to work and at the quality level that is required for that activity. There may be activities that management may consider at "very high" risk. In this case, assessments should be performed on a monthly basis.

(4) The assessment schedule should be listed in the internal control evaluation plan (ICEP) (para 6h(1)). The ICA or AUM will maintain and report the schedule to the MICPA quarterly and send out reminders to TPOs to ensure assessments are being performed as scheduled.

(5) The performance plan of the TPO, ICA, and SRO or AUM should include IC responsibilities and the requirement of performing the assessments.

(6) Alternative reviews may be used for a portion of an assessment. For example, purchase-card reviews are performed by the 409th Support Brigade. While these reviews may assess a portion of the activities performed in the AU area of responsibility, not all of the details and activities associated with the technique will be assessed. It is important that the AUM assess the activities that he or she is responsible for to ensure the effectiveness of a control.

(7) Assessments must be based on testing to ensure that a process is assessed in an unbiased manner and that a sufficient number of samples are reviewed to form an opinion on the effectiveness of the control and build a reasonable basis for conclusion. There are multiple types of testing methods available that a TPO can use to assess ICs:

(a) Inquiry. Conducting inquiries through discussions, interviews, or meetings with process owners, process staff, and key stakeholders is one testing method. Inquiry is seldom used alone. Inquiry serves for preparing identifying controls and designing tests. By gathering information from the people who exercise the controls, management can gain a better understanding of what is being done. For controls for which no other logic method for testing exists, the inquiry must be documented.

(b) Observation. Observation involves simply watching a control while it is being exercised from the start to the end. Managers must be careful when using this method as it is universally understood that people will not do precisely the same things when they know they are not being watched. This method will, however, uncover whether employees being observed know that what they are doing is the wrong thing. All observation tests must be documented, including information about the person observing; the person observed; and the time, date, and location of the test.

(c) Examination. Examination is the best method to determine the effectiveness of a control. This method is especially good for control activities that involve documentation based on which the exercise of the control can be confirmed. Signed documents, entry logs, control logs, checklists, or similar are perfect candidates for examination. Examination tests will involve determining how many instances of a control occur in a testing period and deciding what percentage of that total will give an accurate look at the control's effectiveness (typically 10 to 15 percent). Any documents that are inspected should be listed on DA Form 11-2. The MICPA will conduct random spot checks of the testing documents to ensure accurate testing.

(d) Re-performance. Repeating the performance of an IC activity by using different sources and samples to ensure that same conclusions are reached is the appropriate testing method to be used when earlier test controls were not documented. For example, reviews of contract requirements and compliance with Federal regulations would require a re-performance of the control to discover whether or not it was employed correctly the first time. For example, when reviewing contract requirements, simply pull a certain number of contracts and review them in the same way they would have been reviewed the first time to try and find any mistakes if possible. To perform this test, the tester must not be the person who inspected the documents the first time.

(8) The TPO should communicate the completion of an assessment to the AUM or ICA. The AUM or ICA should review and approve the assessment in the ICEP or test plan (subpara (11) below). If the assessment is not sufficient, it should be rejected and the TPO should make the required corrections. The AUM is responsible for ensuring that all assessments are performed as scheduled.

(9) The AUM is also responsible for ensuring that the access to supporting documentation containing sensitive information or personally identifiable information is restricted to key personnel with a need to know to prevent unauthorized personnel access to such data. The documents may be maintained electronically, must be password-controlled, and a signed nondisclosure agreement must be on file.

(10) Before testing an IC techniques, the documentation of the previous assessment of that technique should be reviewed to ensure that the same process and verification steps are being followed. The assessor should review the issues identified in the previous assessment to verify that they have been corrected or corrective actions are taking place. The documentation of the assessment should be sufficient enough so that another manager could look at the documentation, replicate the assessment, and come to the same conclusion.

(11) To ensure consistency in conducting IC assessments, AUs should use a test plan. A test-plan format has been developed to help with the overall assessment process (fig 4). The test plan is available on the USAREUR SharePoint site at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx* under the MICP Tools Folder. If no other process is in place or being used, USAREUR TPOs will use this test-plan format to ensure consistency. A test plan should be created for each test to be performed. One plan, however, may cover the testing of multiple controls, especially if the frequency of the controls or the control objectives are the same or similar.

(12) The test plan must list how often a control is performed (for example, annually, quarterly, monthly, biweekly, weekly, daily) to determine the number of samples to select. For example, a vendor pay report is generated weekly to identify late payments. Using the numbers in table 3, a weekly report would require 10 (out of 52) samples to be selected. Once the frequency is determined, each report will be reviewed to determine the number of transaction samples to select. The table outlines the minimum sample size. Management, however, must exercise judgment and consider additional factors such as the significance of a control and whether or not the control is automated when developing the sample size. Guidance from the United States Chief Financial Officers Council (CFO Council) Implementation Guide for OMB Circular A-123 has been included in table 3 along with an acceptable number of deviations that AUs may use only for audit readiness purposes (last column). Organizations must document the justification of the sample size used for testing if it differs from table 3.

TEST PLAN FY 15	
AU	XYZ WCF
Program	Civilian Pay
Process	Payroll
TPO or Tester	John Smith E-mail: john.smith.mil@mail.mil Telephone: 537-5555
Control #	1a
Risk	Time and attendance omitted (for example, sick, annual, overtime/comp time worked)
Current Internal Control	Supervisor verfies timesheet with supporting documentation
Control Type (manual/automated)	Manual
Control Risk	High
Testing Period	Q1-2015 through Q4-2015
Test Method	Inspection
Control Frequency	Biweekly
Population and Sample size	Population: 1,128 (47 employees; biweekly), Sample Size: 45
Criteria for Effectiveness/Tolerance Rate	For sample size of 9 and below, no exceptions allowed; (10 to 29, 1 exception allowed; samples of 30 to 44, 3 exceptions allowed; samples of 45 and above, 5 exceptions allowed)
Test Description	DCPS T&A printouts will be verified against supporting documentation to determine if T&A has been correctly captured and approved. Someone other than timekeeper or supervisor will examine DCPS T&A printouts from two predetermined pay periods to verify that (1) leave, comp time/overtime hours and night differential hours ("labor exceptions") are the same as on the timesheet signed by the employee; (2) that printouts have the supervisor's signature; (3) that the labor exceptions are supported by some kind of documentation such as leave requests or overtime schedules.
Test Strategy	• Identify the individuals who will be involved in the testing • Identify the where and when for the testing • Identify the documents, systems, or evidentiary business papers to be examined • Prepare detailed instructions for conducting the test • Instructions on how to conduct the test and record the results will be provided by e-mail on the day of the test • Test results will be sent by e-mail to Jane Doe • Copies of supporting documentation will be mailed to Jim Jones
Test Results	Test work resulted in 6 exceptions, which exceeds the criteria for effectiveness noted above. Preliminary control risk must be reassessed from Moderate to High, and the control is deemed ineffective. Development of a corrective action plan (CAP) is required and must be approved by the AUM.
Assessment Completion Date	January 5, 2015
AUM (or ICA) Review Date	January 12, 2015
AUM (or ICA) Comments	Process owner has been directed to complete a CAP and guidance has been provided on how to bring the program back within standards.

Figure 4. Sample Test Plan

Table 3
Determining the Sample Size for Testing Control Techniques

Frequency	Population size	Total Sample size	Acceptable Number of Deviations/ Tolerable Misstatement (by CFO Council)	Acceptable Number of Deviations/Tolerable Misstatement (for Audit Readiness)
Annually	1	1	0	0
Quarterly	4	2	0	0
Monthly	12	3	0	0
Weekly	52	10	0	1
Daily	250	30	0	3
Multiple times a day	More than 250	45	0	5

(13) Once the control frequency has been determined, management must determine the number of transactions to test within each report. When developing the test plan, populations may have to be determined for testing. Once the sample size has been determined, the AU should identify a sampling technique to select the items to be tested. The Financial Improvement and Audit Readiness Guidance recommends the following two sampling techniques:

(a) Random Sample Selection. This method ensures that all items in the population have an equal chance of being selected. Organizations should make every effort to use random sampling. To select a random sample, the AU can use random number tables, random numbers generated in software such as Microsoft Excel, or random selection offered by sampling software.

(b) Haphazard Sample Selection. This method provides for selecting a representative sample without relying on a truly random process. Sample items should be selected without any conscious bias. When using haphazard selection, be careful to avoid distorting the group of transactions picked for testing by purposely selecting certain types of transactions, such as unusual or large dollar transactions.

(14) When testing a technique, the following should be considered:

(a) Are controls in place?

(b) Are the controls, procedures, or processes in writing? Are they up to date?

(c) Have personnel been trained on the controls, procedures, or processes? Has the training been documented?

(d) Request a walk-through of the process with the personnel performing the technique.

(e) Can personnel walk through the process or procedure completely?

(f) Does the demonstrated process match the documentation of the process or procedure?

(g) Does the personnel provide examples of exceptions or when they do not follow the process or procedure?

(h) Is the present control working? Is it weak, working well, or excessive for what is required?

(i) What is the review or approval process in place and is it at the correct level?

(j) Were changes or corrections made after approvals?

(k) Is the information accurate and correct?

(l) Was all of the information required on forms or other documentation (for example, boxes to be checked on leave requests)?

(m) Is there a time requirement for the document to be completed (for example, sick leave requests should be filled out within 48 hours after return of an employee; travel authorization needs to be approved before the travel)?

(n) Is the document properly authorized? (Were all of the approvals and certifications performed to ensure segregation of duties? Were the authorizations granted? Did the supervisor approve the leave request in ATAAPS timely or did it take 3-4 weeks before it was signed? Was the travel authorization or voucher approved and certified timely?)

(o) Is supporting documentation (for example, emergency leave orders, invoice for payment of vendors, copies of quotes for supplies to validate prices) available and attached?

(15) The determination of the risk level of objectives, missions, and goals is based on the number of deviations found during the testing.

(a) If the number of deviations found during the IC techniques assessment does not exceed the acceptable number of deviations in the CFO Council column of table 3, the control risk should be considered "low."

(b) The control risk is "moderate" if deviations exceed the acceptable number prescribed in the CFO Council column in table 3, but not exceed the number of acceptable deviations prescribed in the Audit Readiness column in table 3. For example, if the original sample was 10 items, the manager may reassess the control risk as "moderate" if there is no more than 1 deviation.

(c) If the number of deviations exceeds the acceptable number of deviations in the Audit Readiness column in table 3, management must conclude that the control risk is "high," which would require immediate development of a "corrective action plan" (CAP) (glossary) (subpara g).

f. Documenting Results of Internal Control Assessments.

(1) Effective documentation helps management design IC techniques by establishing and communicating the who, what, when, where, and why of IC responsibilities to personnel. Documentation also provides a means to retain organizational knowledge and mitigate the risk of having that knowledge limited to a few personnel, as well as a means to communicate that knowledge as needed to external parties, such as external auditors. Management documents IC to meet operational needs. Documentation of controls, including changes to controls, is evidence that controls are identified, being communicated to those responsible for their performance, and being monitored and evaluated by the entity. The extent of documentation needed to support the design, implementation, and operating effectiveness of the five components of IC (para 4) is a matter of judgment for management. Management considers the cost benefit of documentation requirements for the entity as well as the size, nature, and complexity of the entity and its objectives. Some level of documentation, however, is necessary so that the components of IC can be designed, implemented, tested, and operated effectively. Any paperwork, copies of forms, screen prints, and other documentation may be attached to the assessment.

(2) Results of IC technique assessments must be reported to appropriate levels within the organization. The reporting AU should list the number of effective, moderately effective, and ineffective IC techniques. Corrective actions taken or to be taken must also be reported. The TPO should report the results of scheduled or performed assessments to the AU ICA on a monthly basis. The AU ICA, in turn, will report the results to the AU SRO or AUM on a monthly basis (quarterly at a minimum). CAPs should be reported and status reports given as required for any deficiencies identified during testing.

(3) Apart from the test plan (subpara e), documentation should include the following:

(a) Process Narrative and Process Flowchart. Preparing process narratives and process flowcharts that describe and illustrate major and essential operations can assist in identifying risks and "control deficiencies" (glossary). Process narratives are written descriptions of the flowcharts, explaining what actions are being taken in each step. The process flowchart and controls should complement the process narrative and summarize the significant steps in major and essential operations. Additionally, the methods of communication used to share the status of steps throughout the process can be documented. The flowchart will identify key processes and their related control activities such as control over information processing and physical control over vulnerable assets.

(b) Standing Operating Procedure (SOP). An SOP is a set of instructions covering those features of operations used to establish a definite or standardized procedure without losing effectiveness. An SOP is both standing and standard; it instructs how to perform a prescribed and accepted process established for completing a task. Features of operations that lead to standardization are common and usually detailed processes performed often and requiring minimal variation each time. The benefits of SOPs are numerous. SOPs reduce training time, the loss of unwritten information, the commission of errors, the omission of essential steps or processes, and the time required for the completion of tasks. This does not mean that carrying out SOPs never requires thought or that SOPs should never change. SOPs should be reviewed annually and updated as needed.

(c) CAP (subpara g). If the assessment of a process determines that an IC technique is moderately effective or ineffective, corrective actions are required to correct the deficiencies. USAREUR is required to track corrective actions taken to expedite prompt resolution of "reportable conditions" (glossary) found during the assessment or inspection of a program.

g. Monitoring CAPs.

(1) It is the responsibility of the AUM to develop a CAP and ensure that the corrective actions are taken. CAPs will be used to document who, when, and how an ineffective control will be brought back to the level of effectiveness that is required. Once the CAP is developed and reviewed, it must be certified and approved by the AUM or SRO.

(2) The status of CAPs should be reported to the ICA on a monthly basis to be included in the monthly assessment status report (subpara f(2)). The CAP will target milestone dates and ICAs must continuously monitor the progress to ensure the target completion dates are met. If the deficiency results in USAREUR having to report a material weakness in the USAREUR "Annual Statement of Assurance" (ASOA) (glossary), updates must be submitted quarterly through the MICPA to HQDA.

(3) Once all of the corrective actions have been completed, an assessment should be performed again on the IC technique to validate that the corrective actions remediated the deficiency. The result should be part of the ICA monthly report to the SRO or AUM. Documentation on the completion of the corrective actions must be maintained along with a copy of the CAP.

(4) Figure 5 is a sample CAP. The format for the CAP and instructions for completing the CAP are available at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx?RootFolder=%2Fhq%2Fg8%2FMMD%2FMASB%2FStewardship%20Team%2FShared%20Documents%2FMICP%20Tools&FolderCTID=0x012000B406588AF6AC12498FF8DADEF954F42A&View={A42FF4DB-D463-4757-81AE-434C494A6DB7}*.

Internal Controls Over Operations or Financial Reporting Corrective Action Plan				
1. Date Initiated:	October 1, 2013	**2. POC Name:**	Robert Hughes	**3. Control Number**
4. Date Last Updated:	June 9, 2014	**5. POC Phone:**	314-337-5555	CAP-HQG8-0001
6. Process Name:	Payroll			
7. Description of material weakness		**8. IC Reporting Category**	Comptroller	**9. Target Correction Date: 1 Nov 13**
10. Risk:	Entries on DCPS printout are not the same as regular hours worked, leave taken or comp time/OT worked			
11. Current Internal Control:	Biweekly, supervisor compares DCPS printout to source documents and to personal knowledge of leave taken and/or comp time/OT worked to ensure that time and attendance is correct on DCPS printout			
12. Test Results:	Test work resulted in 13 (out of 136 sampled) exceptions. Eight supervisors (Kaneohe Bay, Seymour Johnson, Holloman, Monmouth, Eglin, Moody, Taegu, and Iwakuni) were missing leave documentation and 5 supervisors (Kaneohe Bay-2 supervisors, Bangor-1 supervisor, and Nellis-2 supervisors) were missing OT authorizations			
13. Corrective Action		**14. Milestones w/Completion Date**		**15. Status**
Send notices to timekeepers and supervisors to remind them that approved OT request is mandatory for all OT/comp time worked as certified on DCPS printout.		Quarterly or when an exception is found in testing		Ongoing
Sample activities and request DCPS printouts and OT requests. Since 1 September 2012, records of 53 supervisors were tested internally; 2 did not properly approve OT/comp time worked.		May 8, 2014		Complete
External auditors will perform timekeeping test February-May 2014. 24 AUs will be tested.		May 31, 2014		Complete
For OT requests, 2/53 supervisors failed to document approval of OT/comp time worked. Also, KPMG found 4/24 activities did not have the proper approvals for OT/comp time worked.		May 31, 2014		Complete
For leave taken, 5/53 supervisors failed to provide approved leave requests for all leave taken. Also, KPMG found 1/24 activities where this occurred. KPMG limited testing to at least 8 hours of leave taken.		May 31, 2014		Complete
Progress was not sufficient for SAT to approve closing of CAP		June 9, 2014		Complete
CAP will be split into two for FY 14. One CAP will be for OT requests and second CAP will be for leave requests.		June 9, 2014		Complete
16. Comments:				
17. Stakeholders	All USAREUR timekeepers and certifiers			

Figure 5. Sample Corrective Action Plan

h. Annual Reporting of Internal Control Status. The MICP has the following two annual reporting requirements:

(1) ICEP. The AUM develops an ICEP to establish control objectives for areas most critical to mission accomplishment and susceptible to fraud, waste, and mismanagement. Based on the risk associated with an objective, the AUM will determine assessment dates. The ICEP can be used to monitor progress and ensure that planned actions are completed. The ICEP will be updated when a new issue has been identified for IC. Each AU is required to annually create and maintain an ICEP or to develop a 5-year plan like the USAREUR ICEP. Each major subordinate command (MSC) and HQ USAREUR staff office is required to submit a signed paper copy and an electronic copy of their ICEP to the MICPA by the last workday in June. Figure 6 shows a sample ICEP. The AUM may also use the USAREUR ICEP at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx* for guidance. The USAREUR ICEP is a summary of the USAREUR MICP activity for the current year and is prepared by the USAREUR MICPA with inputs from the "Internal Control Council" (ICC) (glossary), MSC commanders, and HQ USAREUR staff principals. The USAREUR ICEP, which is updated annually and covers 5 years, indicates the program areas of scheduled assessments, the identity of USAREUR AUs, governing regulations, directives, and dates of last assessments. The data contained in or summarized by the plan must be consistent with information reported in the USAREUR ASOA. The plan should address IC assessments throughout the command and convey with a reasonable amount of certainty the knowledge that the objective has been accomplished.

21st TSC Fiscal Years 2016-2020 Internal Control Evaluation Plan												
Functional Proponent	Function	Description	Regulation/ Directive	Risk Level (L,M,H)	AR Required Frequency	Organization Required Frequency	2016	2017	2018	2019	2020	Last Evaluation
All	Procurement Policy and Procedures	Government Purchase Card Program	Army GPC Operating Procedures, Appendix D	H	Annually	Annually	X	X	X	X	X	FY 15
All	Financial Administration	Government Travel Charge Card Program	DOD 7000.14-R, Volume 9, Chapter 3, Annex 9	H	Annually	Annually	X	X	X	X	X	FY 15
All	Time and Attendance	Army Time and Attendance (ATAA)	DOD 7000.14-R, Volume 8, Chapter 2	H	Annually	Annually	X	X	X	X	X	New FY 16
All (as required)	Financial Administration	Commanders Audit Readiness Checklist	FIAR Guidance	H	Annually	Annually	X	X	X	X	X	FY 15
S1	Personnel	Local National Time & Attendance Data	AE Reg 690-99, Appendix B	M	2 Years	2 Years	X		X		X	FY 14
S1	Time and Attendance	Overtime/ Compensatory Time	AE Reg 690-58	H	Annually	Annually	X	X	X	X	X	New FY 16
S3	Security	Physical Security	AR 190-13	M	5 Years	3 Years		X			X	FY 15
S4	Supply	Physical Inventory Control	AR 740-26, Appendix I	H	Per MCP	Annually	X	X	X	X	X	FY 15
S8	Financial Management	Budget Execution	DFAS-IN 37-1, Appendix W	H	5 Years	Annually	X	X	X	X	X	FY 15
S8	Travel	Defense Travel System	DODFMR Volume 9, Chapter 3, and Volume 5, Chapter 33	H	Annually	Annually	X	X	X	X	X	New FY 16

Figure 6. Sample Internal Control Evaluation Plan

(2) Feeder ASOA and USAREUR ASOA.

(a) The feeder ASOA is a statement of assurance representing the AU SRO informed decision as to the overall adequacy and effectiveness of the IC system within the AU. AE Regulation 11-2 requires MSC commanders and HQ USAREUR staff principals to submit a feeder ASOA to be used as the basis for the USAREUR ASOA. The feeder ASOA and supporting documentation must be kept for 3 years or until 3 years after the remediation of any reported material weaknesses. Each feeder ASOA will consist of a cover memorandum addressed to the CG, USAREUR, signed by the AU SRO providing an assessment as to whether there is "reasonable assurance" that ICs employed in the AU are in place, operating effectively, and being monitored. The assessment should be based on the testing of IC processes. These processes must be identified in the ASOA. OMB Circular A-123 states the ASOA must take one of the following forms:

1. An unqualified statement of assurance provides reasonable assurance that the IC system is operating as required by the FMFIA. Each unqualified statement must summarize the basis for making that designation citing the specific control processes in effect throughout the AU and the method employed to reach this conclusion. Details supporting the designation of an unqualified statement will be identified in TAB A of the ASOA. Specific external reviews, IC objective-plan assessments, or other activities documenting effective control should be used to support an unqualified statement of assurance.

2. A qualified statement of assurance provides reasonable assurance. There are significant deficiencies or material weaknesses noted. The statement must cite the deficiencies or material weaknesses that preclude an unqualified statement. A CAP must be prepared and submitted with the ASOA (subpara g). The deficiencies will be identified in TAB B.

3. A statement of no assurance provides no reasonable assurance. The statement must provide the reason for this designation and should be used when no IC processes are employed in the specific AU. A CAP must be submitted with the statement of no assurance. (AU SROs are asked to contact the MICPA before submitting a statement of no assurance).

(b) The MICPA will initiate a task management tool (TMT) tasker to all MSCs and staff offices providing detailed ASOA reporting guidance by 30 November each year. All MSCs and staff offices will provide their signed feeder ASOA to the MICPA by the last workday in February. The MICPA will review all feeder ASOAs to ensure compliance with reporting requirements or return noncompliant ASOAs for corrective actions. The MICPA will evaluate the submitted ASOAs using scores. Table D-1 shows how the scores are distributed. The feeder ASOA will also include TAB G "Army Commander's Audit Readiness Checklist for Statement of Budgetary Resources (SBR) and Existence and Completeness (E&C)." The TMT task will provide details for completing this TAB.

(c) The MICPA will prepare the USAREUR ASOA for CG signature according to instructions received annually from HQDA. The report will be based on the feeder ASOAs provided by the MSC and staff offices and include an assessment of the effectiveness of the USAREUR MICP. Additional assurances as designated by HQDA are required to be made by the USAREUR G8 and included in the USAREUR ASOA. A draft version of the USAREUR ASOA is prepared and forwarded to the USAREUR SRO and, if required, presented to the ICC for further discussion. Once the CG signs the USAREUR ASOA, the MICPA will transmit the USAREUR ASOA to the Assistant Secretary of the Army (Financial Management and Comptroller) to complete the annual reporting requirement.

(d) Formats for all parts of the ASOA are available at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx?RootFolder=%2Fhq%2Fg8%2FMMD%2FMASB%2FStewardship%20Team%2FShared%20Documents%2FAnnual%20Statement%20of%20Assurance%20%28ASOA%29%20Preparation%20Guidance&FolderCTID=0x012000B406588AF6AC12498FF8DADEF954F42A&View={A42FF4DB-D463-4757-81AE-434C494A6DB7}*.

7. TRAINING

All USAREUR employees directly involved in the MICP will be trained in their duties. Several training courses are available online through the Army Learning Management System (ALMS) at *https:www.lms.army.mil/*. AU ICAs and the MICPA should provide additional training to TPOs and inspection personnel on how to properly perform the assessments. All training classes should be documented and all training certifications retained. The AUM is responsible for ensuring that AU staff is properly trained on their responsibilities. Personnel with MICP responsibilities will complete initial and refresher training as prescribed in AE Regulation 11-2, appendix D.

8. ADDITIONAL INFORMATION

a. The United States Army Audit Agency and commercial auditing firms may provide advice to USAREUR and its AU on establishing IC techniques for the organization. The MICPA may review audits and other reports issued by these agencies and provide a summary to USAREUR AUMs to use in evaluating whether similar issues exist in their AU.

b. Automation processes used in information technology (IT) introduce new or different elements of risk into systems. Ensuring that proper controls, manual or automated, are in place in automated systems and managing the IT function is an important aspect of the MICP. Both the control over the operation of each application system and the control over the management of the IT function should be in place and reviewed.

(1) Application controls are unique to each application system. Proper controls assure that an application system does exactly what it is intended to do and nothing else. AUs need to establish controls that are commensurate with the risk or magnitude of loss or harm that could result from improperly working automated systems.

(2) General controls apply to the overall management of the IT function. They have a direct effect on the resources being expended for automation and should assure the effective and efficient use of those resources as well as the quality of service to IT users. General controls include the following:

(a) Organizational controls for the IT unit.

(b) Systems design, development, and modification controls.

(c) Installation security controls.

(d) System hardware and software contracts.

9. HELPFUL HINTS FOR PROGRAM MANAGEMENT

The following are helpful hints for conducting an effective MICP:

a. Maintain objectivity throughout the assessment process.

b. Maintain organized files of your IC documents. You must keep MICP supporting documentation for 3 years at a minimum.

c. Start the feeder ASOA as early as possible after submission of the previous statement in the form of a perpetual ASOA. Working the feeder ASOA throughout the year versus attempting to pull it all together during January and February makes the task much more manageable and a lot less stressful. Activities for audits, program reviews, and assessments performed outside of the ICEP review process can be used to support the ASOA.

d. Enter summaries of audits as they occur during the year; document corrective actions for material weaknesses, control deficiencies, and concerns as they are initiated.

e. Make sure everyone knows what is expected of them.

f. Always keep your eyes open. When you are least expecting a problem, that is when it will occur.

g. Communication is a key element to the success of the program. Keep your commanders informed at all times.

h. When it comes to the IC reporting process, do your best to simplify it for your AUMs. Provide them with samples and formats. Most importantly, ask them if they were the SRO reading the report, would they feel “reasonably sure” that the objective is being met and that adequate controls are in place and working.

i. Remind your AUM that this is a self-assessment and that they must use their own judgment as to whether they should conduct an IC review or rely on alternate IC reviews, audits, or other to support their conclusions regarding adequacy of controls for their objectives. A combination of these methods will often provide the best information to back up their conclusions and recommendations.

j. Continuous monitoring is essential to improving the effectiveness of IC associated with USAREUR programs. This continuous monitoring and other periodic evaluations provide the basis for the ASOA, as required by the FMFIA.

k. Use the Program Compliance Review Checklist in appendix C as a tool to assess your MICP. The USAREUR MICPA uses this checklist to review HQ USAREUR staff offices and MSCs for their compliance with MICP requirements.

l. Use this guide and the tools on the MICP website at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx* to manage your program. Remember that IC is a "common sense program."

m. Reporting on ICs is required by law, and controls make sense. They protect us, help ensure mission accomplishment, and let taxpayers know we are making every effort to spend their money wisely.

APPENDIX A
REFERENCES

SECTION I
PUBLICATIONS

Public Law 97-255, Federal Managers Financial Integrity Act of 1982
http://www.whitehouse.gov/omb/financial_fmfia1982

Public Law 101-576, Chief Financial Officers Act of 1990
http://www.gao.gov/special.pubs/af12194.pdf

GAO-14-704G, Standards for Internal Control in the Federal Government ("Green Book")
http://www.gao.gov/assets/670/665712.pdf

OMB Circular A-123, Management's Responsibility for Internal Control
http://www.whitehouse.gov/omb/circulars_a123_rev

United States Chief Financial Officers Council, Implementation Guide for OMB Circular A-123, Management's Responsibility for Internal Control Appendix A, Internal Control over Financial Reporting
https://www.whitehouse.gov/sites/default/files/omb/assets/OMB/circulars/a123/a123_appx_a_implementation_guide.pdf

Office of the Under Secretary of Defense (Comptroller)/Chief Financial Officer, Financial Improvement and Audit Readiness (FIAR) Guidance
http://comptroller.defense.gov/Portals/45/documents/fiar/FIAR_Guidance.pdf

AE Regulation 10-5, Headquarters, United States Army Europe

AE Regulation 11-2, USAREUR Manager's Internal Control Program

SECTION II
FORMS

DA Form 11-2, Internal Control Evaluation Certification

DA Form 2028, Recommended Changes to Publications and Blank Forms

SECTION III
ADDITIONAL SOURCES

Army Managers' Internal Control Program (Assistant Secretary of the Army for Financial Management & Comptroller)
http://asafm.army.mil/offices/FO/IntControl.aspx?OfficeCode=1500

GAO-01-1008G, Internal Control Management and Evaluation Tool
http://www.gao.gov/new.items/d011008g.pdf

OMB Circular A-127, Financial Management Systems
https://www.whitehouse.gov/omb/circulars_a127

OMB Circular A-130, Management of Federal Information Resources
https://www.whitehouse.gov/omb/circulars_a130

Government Performance and Results Act of 1993
https://www.whitehouse.gov/omb/mgmt-gpra/gplaw2m

Information on reporting potential fraud, waste, or abuse of GAO property, assets, and resources
http://www.gao.gov/fraudnet/fraudnet.htm

Government Management Reform Act of 1994
http://thomas.loc.gov/cgi-bin/bdquery/z?d103:SN02170:|TOM:/bss/d103query.html

The Institute of Internal Auditors
https://na.theiia.org/Pages/IIAHome.aspx

American Institute of Certified Public Accountants
http://www.aicpa.org/Pages/default.aspx

U.S. Government business news
www.govexec.com

Information on new laws and regulations to key court decisions
www.fedmanager.com

Gateway to Government information
http://fedworld.ntis.gov/

APPENDIX B
ASSESSABLE UNIT CODES

The following table lists assessable unit codes for HQ USAREUR staff offices and major subordinate commands to be used when completing the risk analysis:

Table B-1
Assessable Unit Codes

Assessable Unit	AU Code
Headquarters and Headquarters Battalion	HHBN
Office of the Deputy Chief of Staff, G1	HQG1
Office of the Deputy Chief of Staff, G2	HQG2
Office of the Deputy Chief of Staff, G3/5/7	HQG3
Office of the Deputy Chief of Staff, G4	HQG4
Office of the Deputy Chief of Staff, Engineer	OENG
Office of the Deputy Chief of Staff, G6	HQG6
Office of the Deputy Chief of Staff, G8	HQG8
Office of the Chaplain	CHAP
Office of the Inspector General	HQIG
Office of the Judge Advocate	OJAG
Office of the Chief of Public Affairs	OCPA
Office of the Command Surgeon	SURG
Command Resource Management Office	RMO
21st Theater Sustainment Command	21TSC
Seventh Army Joint Multinational Training Command	JMTC
2d Cavalry Regiment	2CR
12th Combat Aviation Brigade	12CAB
173d Airborne Brigade Combat Team	173IBCT
19th Battlefield Coordination Detachment	19BCD
10th Army Air and Missile Defense Command	10AAMDC
Area Support Team Balkans	ASTB

APPENDIX C
PROGRAM COMPLIANCE REVIEW CHECKLIST

This checklist is also available at *https://intranet.eur.army.mil/hq/g8/MMD/MASB/Stewardship%20Team/SitePages/Managers%27%20Internal%20Control%20Program.aspx*.

Program Compliance Review			
Review Date		Reviewer	
AU		Activity	
Process		Pass/Fail	
		Y/N/NA	Comments (Required for No or NA answers)
1	Is local internal control guidance available that defines internal control responsibilities and required actions?		
2	Are MICP documents centrally located?		
3	Does the organization have a current ICEP?		
4	How are objectives communicated throughout the agency, and does management obtain feedback on the effectiveness of the communication?		
5	Have risk assessements been completed? If so, how?		
6	Have AUMs and ICAs been designated in writing, and have personnel completed MICP training?		
7	Are explicit statements of internal control responsibility included in performance agreements (AUMs,ICAs, etc.)?		
8	Has a material weakness been reported in the past 5 years, or an area of concern within the past 3 years? If so, how are they tracked?		
9	What are the AU critical functions? How are they managed? Is there a mission essential task list?		
10	Does the ICA maintain the ASOAs from the last 3 years?		
11	How are AU objectives established and how often are they reviewed?		
12	Does management monitor controls, provide oversight, identify exceptions from normal operations? Is it in writing?		
13	Are employee and supervisor IC duties properly segregated (for example, timekeeping,certification,payment)?		
14	Does the AU have a copy of the current-year USAREUR ICEP?		
15	Risk management evaluation criteria include—		
	o Identification of risks.		
	o Assessment of risks.		
	o Making risk decisions and developing controls.		
	o Implementing controls.		
	o Monitoring and evaluating controls.		
	o Providing feedback.		
16	Can personnel walk through the process or procedure completely?		
17	Does their process match the documentation of the process or procedure?		
18	Have personnel been trained on the controls, procedures, and processes?		
19	How are risks handled as a result of findings from audits, evaluations, inspection, OIP review, and other reviews?		
20	Is there a system to monitor problems until they are solved?		
21	What review or approval process is in place? Are the reviews or approvals at the correct level?		
22	Were changes or corrections made after approvals?		
23	Was all of the required information filled out on forms or documentation? Did they have the proper authorization?		
24	Does personnel provide examples of exceptions or an explanation why they do not follow the process or procedure?		
25	Is the AUM certification of IC evaluations documented on DA Form 11-2 and is supporting documentation attached?		

Figure C-1. Program Compliance Review Checklist

APPENDIX D
ASSESSMENT SCORE CARD

The following table shows how the Managers Internal Control Program Administrator distributes the scores for the evaluation of feeder annual statements of assurance.

Table D-1
Distribution of Assessment Scores

Timeliness		
Received on or before the due date (that is, the last workday in February)		+ 10 points
Up to 5 days late (received until 5 March)		0 points
More than 5 days late (received on 6 March or later)		- 5 points
Format		
Does the ASOA follow guidance?		
No revision required, acceptable in all aspects		+ 5 points
Returned for correction, unsatisfactory in at least one aspect		+ 2 points
Extensive formatting changes required, incorrectly stated opinion, statement is noncompliant in more than one aspect		0 points
Program Execution		
How well does the organization execute and explain how it conducts its MICP in Tab A?		
The ASOA clearly indicates that the MICP is executed at all levels of the organization (ICEP developed and submitted, evaluations completed as required, AU submitted accomplishments).		+ 55 points
The ASOA has limited evidence of organization-wide execution (all of the identified inspections were not completed, no accomplishments identified).		+ 30 points
There is no evidence of organization-wide program execution in the ASOA.		0 points
Training		
Evidence of attendance and completion is specifically mentioned (training certificates submitted with feeder ASOA).		+ 10 points
There is evidence of attendance and completion of training, but training is not mentioned in the feeder ASOA (certificates not provided).		+ 7 points
There is no evidence of attendance and completion of training and no evidence of organization-wide program execution in the feeder ASOA.		0 points
Material Weakness Reporting Activity		
Any of the following applies:		
Correction of earlier reported MW or quarterly update with CAP for current MW		+ 20 points
New MW is reported with a plan or schedule for remediation		
No MW due for correction in FY with projected milestones completed as due		
MW reported and strong evidence addressing the consideration of reporting MW (areas of concerns and controlled deficiencies identified)		
Delay in remediating existing MW with progress shown		+15 points
Any of the following applies:		
MWs reported without a plan or schedule for remediation		+ 10 points
No MWs reported and limited evidence addressing the consideration of reporting MW		
Any of the following applies:		
MWs reported, not providing adequate evidence that consideration was given to reporting MWs and using statements identical to the prior year's ASOA, giving the impression that dates were simply changed when compared to prior years' ASOA		0 points
Delay in remediating existing MWs without progress shown		
No MWs reported and no evidence addressing the consideration of reporting MWs		
Bonus Points		
ASOA mentions the tone at the top or uses language suggesting support of MICP by management.		+ 5 points
SCORE CATEGORIES		
90 to 105 points	Requirements are met or exceeded	**GREEN**
60 to 89 points	Some requirement deficiencies are noted, improvement needed	**YELLOW**
0 to 59 points	Failure to meet requirements, significant improvement needed	**RED**

GLOSSARY

SECTION I
ABBREVIATIONS

AR	Army regulation
ATAAPS	Automated Time Attendance and Production System
AE	Army in Europe
ALMS	Army Learning Management System
ASOA	annual statement of assurance
AU	assessable unit
AUM	assessable unit manager
CAP	corrective action plan
CFO	chief financial officer
CIC	current internal control
DA	Department of the Army
FMFIA	Federal Managers Financial Integrity Act
GAO	United States Government Accountability Office
IC	internal control
ICA	internal control administrator
ICC	internal control council
ICEP	internal control evaluation plan
IS	information system
IT	information technology
MICP	Managers' Internal Control Program
MICPA	Managers' Internal Control Program Administrator
MSC	major subordinate command
OMB	Office of Management and Budget
SOP	standing operating procedure
SRO	senior responsible official
TMT	task management tool
TPO	technique process owner
HQ USAREUR	Headquarters, United States Army Europe
USAREUR	United States Army Europe
USAREUR G8	Deputy Chief of Staff, G8, United States Army Europe

SECTION II
TERMS

annual statement of assurance
A statement representing an agency head's informed decision as to the overall adequacy and effectiveness of internal controls within the agency

assessable unit
The basic organizational segment that has one or more internal control systems on which periodic risk assessments must be performed

assessable unit manager
The military or civilian head of an assessable unit, preferably at the general-officer or Senior Executive Service level, but not below the grade of an O6, GS-15, or equivalent

control deficiency
The insufficient design or operation of a control that does not allow management or employees, in the normal course of performing their assigned functions, to satisfactorily accomplish their assigned functions or inhibits the prevention or detection of misstatements on a timely basis

control objective
A point of reference against which the effectiveness of internal controls can be evaluated

control risk
The risk of a control failing to prevent or detect an identified inherent risk

control standard
A program requirement prescribed by a policy or procedure; basis for developing control objectives

corrective action
Actions taken to remediate or correct issues or problems identified during an internal control assessment or audit that caused an internal control to be moderately effective or ineffective

corrective action plan
A plan that identifies the actions required to mitigate a risk and correct a weakness or control deficiency identified during an internal-control assessment or audit that caused an internal control to be moderately effective or ineffective

documentation
Documents showing the type and scope of review, the responsible official, the pertinent dates and facts, the key findings, and the recommended corrective actions; include policies and procedures, organizational charts, manuals, flow charts, and related written and graphic materials necessary to describe organizational structure, operating procedures, and administrative practices; and communicate responsibilities and authorities for accomplishing programs and activities

internal control
The rules, procedures, techniques, and devices employed by managers to ensure what should occur in their daily operations does occur on a continuing basis

internal control administrator
A U.S. military, Department of the Army civilian, or local national employee designated to serve as the focal point for internal control activities in his or her organization

Internal Control Council
A senior management council that comprises senior management officials from all USAREUR functional offices and assesses and monitors internal-control deficiencies

key control
An absolutely essential control for ensuring that key processes operate as intended and that resources are safeguarded from fraud, waste, and misuse; failure would “break” or seriously impair the system

material weakness
A significant deficiency or a combination of significant deficiencies that result in a reasonable possibility that a material misstatement will not be prevented or detected

process owner
A manager or employee who is responsible for developing, completing, and reporting a specific corrective action plan to the senior responsible official or assessable-unit manager

program compliance review
A review of staff offices and reporting commands conducted by the USAREUR Managers' Internal Control Program (MICP) Administrator to determine compliance with MICP guidance

reportable condition
A control deficiency or combination of control deficiencies that in management's judgment should be communicated because they represent significant weaknesses in the design or operation of internal controls that could adversely affect the organization's ability to meet its internal-control objectives

risk
The probability of inadequate internal controls leading to adverse effects that may result in the loss of Government resources through abuse, fraud, loss, mismanagement, or waste