FEDERAL MANAGERS'
FINANCIAL INTEGRITY ACT OF 1982

FY 2009
STATEMENT OF ASSURANCE

Defense Commissary Agency

TAB A

DESCRIPTION OF THE CONCEPT OF REASONABLE ASSURANCE AND HOW THE EVALUATION WAS CONDUCTED

The Defense Commissary Agency (DeCA) senior management evaluated the system of internal accounting and administrative controls in effect during the fiscal year as of the date of this memorandum, according to the guidance in Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Internal Control," December 21, 2004. The OMB guidelines were issued in conjunction with the Comptroller General of the United States as required by the Federal Managers' Financial Integrity Act (FMFIA) of 1982. Included is an evaluation of whether the system of internal accounting and administrative control for DeCA is in compliance with standards prescribed by the Comptroller General.

The objectives of the system of internal accounting and administrative control of DeCA are to provide reasonable assurance that:

- The obligations and costs are in compliance with applicable law;

- Funds, property, and other assets are safeguarded against waste, loss, unauthorized use, or misappropriation; and

- Revenues and expenditures applicable to Agency operations are properly recorded and accounted for to permit the preparation of reliable accounting, financial statistical reports, and to maintain accountability over the assets.

The evaluation of internal controls extends to every responsibility and activity undertaken by DeCA and applies to program, administrative, and operational controls. Furthermore, the concept of reasonable assurance recognizes that: (1) the cost of internal controls should not exceed the benefits expected to be derived and (2) the benefits include reducing the risk associated with failing to achieve the stated objectives. Moreover, errors or irregularities may occur and not be detected because of inherent limitations in any system of internal accounting and administrative control, including those limitations resulting from resource constraints, congressional restrictions, and other factors. Finally, projection of any system evaluation to future periods is subject to risk that procedures may be inadequate because of changes in conditions, or that the degree of compliance with procedures may deteriorate. Therefore, this statement of reasonable assurance is provided within the limits of the preceding description.

DeCA evaluated the system of internal management controls in accordance with the guidelines identified above. The results indicate that the system of internal accounting and administrative control of DeCA in effect during the Fiscal Year (FY) 2009 as of the date of this memorandum, taken as a whole, complies with the requirement to provide reasonable assurance that the above mentioned objectives were achieved. This position on reasonable assurance is within the limits described in the preceding paragraph.

For the seventh straight year, DeCA received an unqualified (clean audit) opinion on its financial statements from an independent public accounting (IPA) firm. The consolidated financial statements were, in the auditor's opinion, fairly presented, free of material misstatements, and prepared in accordance with generally accepted accounting principles, consistently applied. In connection with their audit, the IPA considered DeCA's internal control over financial reporting and performance measures and tested DeCA's compliance with certain provisions of applicable laws, regulations, and contracts that could have had a direct and material effect on the financial statements being audited.

DeCA evaluated its system of internal accounting and administrative control using the following process for conducting the evaluation.

Internal Control Program Execution

DeCA's approach is based primarily on our success in the implementation of the OMB A-123, Appendix A requirements. With the advent of Appendix A in FY 2006, we have aligned the financial and non-financial processes to mirror one another. We took advantage of common business process management and maximized the ability of the program to function as a tool for cultural change within the Agency. We adopted the Appendix A deliverable model to fit our overall organizational needs. DeCA will be able to give the same level of reasonable assurance to the Secretary of Defense with greater specificity, management involvement, and accuracy; and with a significant reduction in time and effort to both the financial and non-financial business processes.

Our results continue to be extremely satisfying as we continue to document all of our key business processes. We have fifteen Assessable Unit Managers who have implemented the methodology for their respective business operations.

The continued oversight of the program by our Senior Assessment Team (SAT) ensures the appropriate amount of attention to the program and its goals. The SAT is chaired by the Chief Financial Executive and staffed by functional process owners from each of our directorates and the deputies for each of our three regions.

New Assessable Units

We have defined our Assessable units in correlation to our corporate organization. Since our primary goal has been to emulate the Appendix A process as much as possible, we have had to come up with a system that was more focused on an end product or key output. The Appendix A processes are defined by the lines from our financial statements that exceeded the 1 percent materiality threshold. Assessable Units are identified at Figure 1.

Figure 1: FY 2009 Assessable Units

Acquisition Management/Supplies and Services Contract Management	Human Resources/Position Classification	Resource Management/Productivity Improvement
Acquisition Management/Commercial Activities Contract Management	Human Resources/Training Support	Corporate Planning/Organization & Process Management
Acquisition Management/GPC Program Management	Human Resources/Labor Relations	Corporate Planning/ Strategic Planning & Management
Corporate Communication/Communications	Human Resources/Mentoring	
Corporate Communications/Marketing	Office of Health & Safety/Public Health	
Corporate Communications/Web Site Development	Office of Health & Safety/Safety	
Chief Information Office/IT Planning and Policy	Inspector General/IG Operations	
Chief Information Office/Accreditation and Oversight	Internal Review/Internal Audit Operations	
Chief Information Office/Information Assurance Audits	Program Management/Desktop Support	
Directorate of Operations/Environmental	Program Management/Network Operations Support	
Store Policy/Procedures	Program Management/Program Management Operations (Tech Support)	
Directorate of Operations/Equipment	Product Support/Operational Systems Management	
Directorate of Operations/Facilities	Product Support/Resale Item Management	
Directorate of Operations/Security	Product Support/Resale Item Management	
Equal Employment Opportunity/Equal Opportunity Support	Product Support/Logistics Management	
General Counsel/Legal Support	Resource Management/Manpower Utilization	

<u>Assessment Process/Continuous Process Improvement</u>

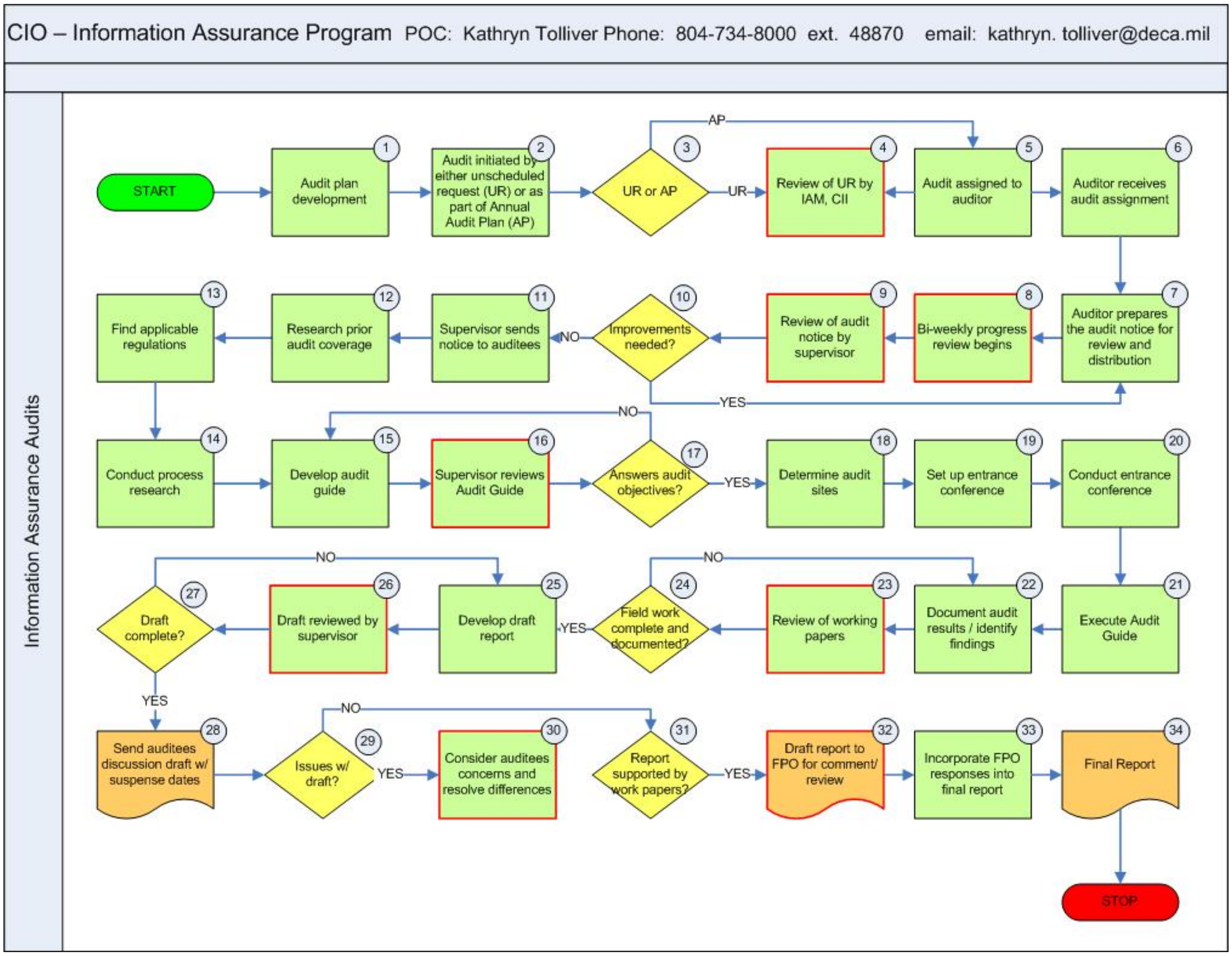
The Internal Control Program (ICP) follows the same methodology as Appendix A with the Flowcharts and Narratives, the Risk Analysis, the Test Plan, the Control Analysis, and the Corrective Action Plans (CAP). The process of producing each of the deliverables is progressive. Each deliverable builds upon the previous one to create one cohesive body of documentation of each process and its controls. We firmly believe that to clearly understand the role and effectiveness of any given internal control, an organization must be able to place those controls in the larger context of the process they are a part. Once a process is defined, our view of what controls are and are not key becomes very different than simply examining those controls in a vacuum of operational risk. Our methodology allows each AUM to look at their controls collectively to assess how they function together to mitigate risk within the larger framework of their business processes, irrespective of what process it is. The Appendix A methodology has been implemented for the fourth year for DeCA process owners. Each year the process is reevaluated to determine if changes have been made to their business processes and if additional clarification or correction needs to be implemented. This methodology is a continuous process improvement for DeCA. DeCA takes the next evolutionary step to expand the program to utilize Lean Six Sigma on all identified deficient controls.

DeCA's Acquisition Management (AM) program manages a worldwide acquisition program in support of the DeCA commissary system. They provide acquisition support for supplies, services and revenue generating agreements, and automation support for all acquisition systems. Further AM program provides guidance and oversight for all DeCA contracting offices using delegated authorities and develops procedures and policy implementation guidance. The AM program utilizes the Appendix A methodology to mitigate risk in its key business processes. The DoD conducted a Procurement Management Review (PMR) of all DeCA contracting offices. The report was issued in November 2008 and determined the contracting processes within DeCA to be compliant. The AM directorate reviewed the Guidance on the Assessment of Acquisition Functions under Office of Management and Budget (OMB) Circular A-123 dated April 6, 2009 to determine how this guidance will be integrated in the internal control review of acquisition with the existing internal control assessment and the annual Statement of Assurance reporting process for FY 2010.

In FY 2008 Information Assurance Program Management Office (IAPMO) under the Chief Information Office (CIO) added the Payment Card Industry (PCI) Data Security Standard (DSS) audit to its annual assessment to be compliant with requirements for cardholder data security. Their tests were not reported complete until 1st quarter FY 2009. The IAPMO began tests for compliance for FY 2009 in the 2nd quarter. Completed test results will not be available until 4th quarter. For DeCA to conduct credit card transactions in our commissaries PCI-DSS compliance must be met annually. The PCI-DSS audit will be reflected further in the Test Plan section of this document.

Flowcharts and Narratives

In order to effectively define the key controls within a process, you must have a clear picture of that process, at least at a high functional level. The flowcharts document the key steps and decisions in each process and clearly define each of the steps that are key control points. Accompanying each flowchart is a process narrative. The narrative process draws a parallel from the bullets contained in the process steps of the flowchart. Taken together, the flowcharts and the narratives give us an unprecedented view not only of the key business processes, but the key controls within those processes that help to ensure the tenants of internal control are adhered to. DeCA asked the process owners to expand their narratives in FY 2009 to include the identification of reference guidance and a strategic link to our strategic goals. It was felt that providing reference guidance would allow for greater clarity for compliance issues and a strategic link would provide a greater focus on mission objectives. Figure 2 below is an example of our flowchart for the business processes for IAMPO under the Chief Information Office (CIO) followed by its accompanying narrative. The Appendix A methodology is the support posture for the Agency compliance for Information Assurance Audits. This is a key process for sustaining compliance and ensuring an acceptable risk posture for the Agency.


CIO – Information Assurance Program POC: Kathryn Tolliver Phone: 804-734-8000 ext. 48870 email: kathryn. tolliver@deca.mil
Information Assurance Audits
START
1 Audit plan development
2 Audit initiated by either unscheduled request (UR) or as part of Annual Audit Plan (AP)
3 UR or AP
AP
UR
4 Review of UR by IAM, CII
5 Audit assigned to auditor
6 Auditor receives audit assignment
7 Auditor prepares the audit notice for review and distribution
8 Bi-weekly progress review begins
9 Review of audit notice by supervisor
10 Improvements needed?
YES
NO
11 Supervisor sends notice to auditees
12 Research prior audit coverage
13 Find applicable regulations
14 Conduct process research
15 Develop audit guide
16 Supervisor reviews Audit Guide
17 Answers audit objectives?
NO
YES
18 Determine audit sites
19 Set up entrance conference
20 Conduct entrance conference
21 Execute Audit Guide
22 Document audit results / identify findings
23 Review of working papers
24 Field work complete and documented?
NO
YES
25 Develop draft report
26 Draft reviewed by supervisor
27 Draft complete?
NO
YES
28 Send auditees discussion draft w/ suspense dates
29 Issues w/ draft?
YES
NO
30 Consider auditees concerns and resolve differences
31 Report supported by work papers?
YES
32 Draft report to FPO for comment/ review
33 Incorporate FPO responses into final report
34 Final Report
STOP

Defense Commissary Agency CIO Narrative

Process. Information Assurance Audits

Assessable Unit Manager. Kathryn Tolliver

References: DoDD 8500.01E, DoDI 8500.2, DoDD 8570.1, DoDD 8570.1-M, DoD 8510.1, and the Federal Information Security Management Act.

Strategic Link: Goal 1 – Preserve and deliver a premier quality-of-life benefit.
Strategy 3 – Continue to optimize store and support operations by implementing process improvements and technological advances.

Date Reviewed. 12.2.2008

STEP 1. Annually, the Information Assurance Manager (IAM), CI creates audit plan based on risk assessments conducted over the course of the previous year.

STEP 2. Audits are assigned. Audits originate from either the Annual Audit Plan (AP) or from unscheduled requests (UR) made by functional managers.

STEP 3. Is the auditor's assignment from the AP or an UR? If from the AP, go to STEP 5.

STEP 4. **Control 1 –** IAM, CI reviews the UR for audit suitability.

STEP 5. Management assigns audit engagement to available auditor.

STEP 6. Auditor receives the assignment.

STEP 7. The auditor prepares an official audit notification for management review.

STEP 8. **Control 2 –** The auditor and managers begin the 'bi-weekly audit status meeting' process in order to provide management guidance, insight and approval of audit methodology.

STEP 9. **Control 3 –** IAM, CI reviews the auditor prepared notification of audit.

STEP 10. If notification requires any revisions, go back to STEP 7, otherwise, go to STEP 11.

STEP 11. The supervisor sends the audit announcement to the auditees and appropriate management officials.

STEP 12. Auditor researches prior audit coverage to include DeCA audits, GAO, DoDIG, KPMG, or other outside audit entities.

STEP 13. Auditor researches and obtains applicable regulatory guidance regarding the audit subject which will serve as the baseline for the ensuing audit.

STEP 14. Auditor obtains an understanding of the processes of the activity under review.

STEP 15. Using information from STEP 12, STEP 13, and STEP 14 the auditor prepares the Audit Guide. The audit guide is the blueprint or plan of action for conducting the engagement.

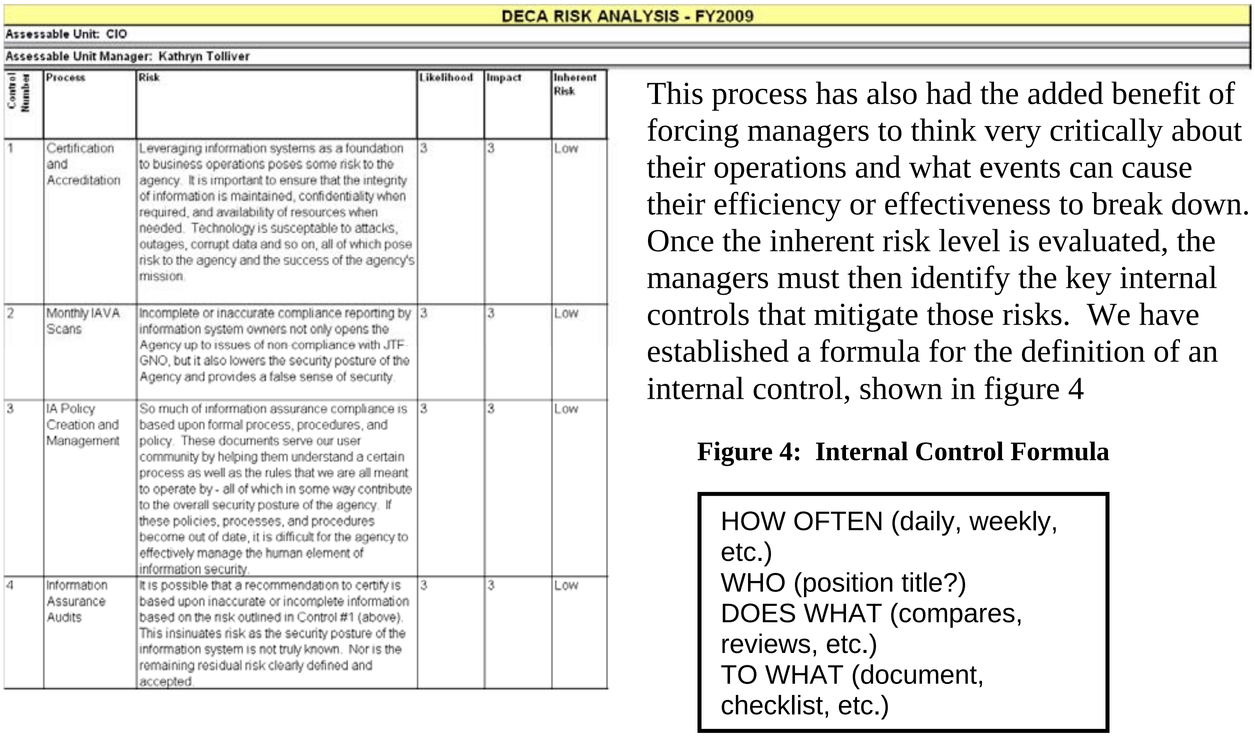
STEP 16. **Control 4 –** Supervisor/Director, IR reviews the Audit Guide.

Risk Analysis

Once the flowcharts and the narratives have been completed, we then begin defining the risks and controls at each of the control points. Figure 3 shows the first part of the analysis, which evaluates the risk absent the controls or inherent risk. This evaluation uses two very distinct measures, likelihood and impact. Both measures are evaluated on a scale of 1 to 5, with 1 being the lowest, 5 the highest. A mathematical combination of these two numbers automatically populates the field defining the inherent risk level. In the DeCA system, we evaluate risk in a purely binary system of either high or low risk. Under the old checklist system, significant time and energy was expended on the evaluation of internal controls that were not central to ensuring the efficiency and effectiveness of DeCA operations and were rarely specific to a business process.

Under the new system, managers must identify the most significant risks to the successful completion of that unit's mission at each of the control points defined on their flowcharts. This has had the effect of both reducing the scope of the activities that had to be investigated and focusing our efforts and resources on the most significant of our operational risks.

Figure 3: Evaluating Inherent Risk



DECA RISK ANALYSIS - FY2009

Assessable Unit: CIO

Assessable Unit Manager: Kathryn Tolliver

Control Number	Process	Risk	Likelihood	Impact	Inherent Risk
1	Certification and Accreditation	Leveraging information systems as a foundation to business operations poses some risk to the agency. It is important to ensure that the integrity of information is maintained, confidentiality when required, and availability of resources when needed. Technology is susceptable to attacks, outages, corrupt data and so on, all of which pose risk to the agency and the success of the agency's mission.	3	3	Low
2	Monthly IAVA Scans	Incomplete or inaccurate compliance reporting by information system owners not only opens the Agency up to issues of non-compliance with JTF-GNO, but it also lowers the security posture of the Agency and provides a false sense of security.	3	3	Low
3	IA Policy Creation and Management	So much of information assurance compliance is based upon formal process, procedures, and policy. These documents serve our user community by helping them understand a certain process as well as the rules that we are all meant to operate by - all of which in some way contribute to the overall security posture of the agency. If these policies, processes, and procedures become out of date, it is difficult for the agency to effectively manage the human element of information security.	3	3	Low
4	Information Assurance Audits	It is possible that a recommendation to certify is based upon inaccurate or incomplete information based on the risk outlined in Control #1 (above). This insinuates risk as the security posture of the information system is not truly known. Nor is the remaining residual risk clearly defined and accepted.	3	3	Low

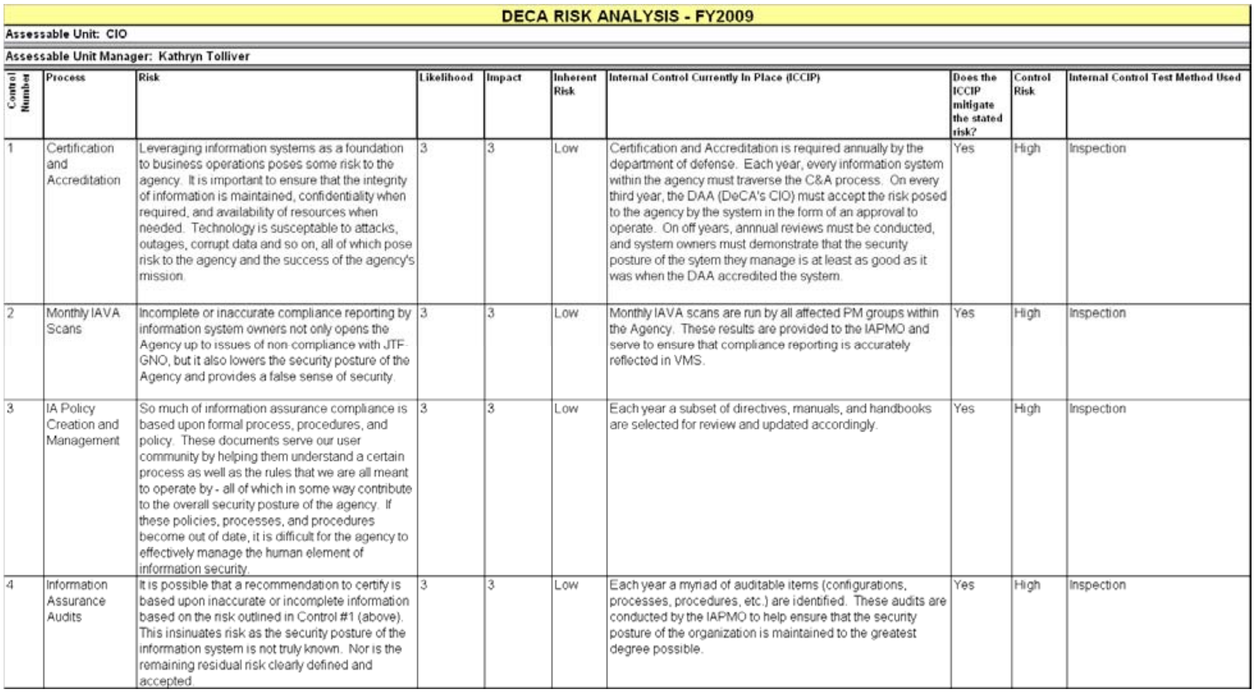
This process has also had the added benefit of forcing managers to think very critically about their operations and what events can cause their efficiency or effectiveness to break down. Once the inherent risk level is evaluated, the managers must then identify the key internal controls that mitigate those risks. We have established a formula for the definition of an internal control, shown in figure 4

Figure 4: Internal Control Formula

HOW OFTEN (daily, weekly, etc.)
WHO (position title?)
DOES WHAT (compares, reviews, etc.)
TO WHAT (document, checklist, etc.)

Defining the internal controls currently in place is one of the most important parts of the evaluation system. In figure 5 you will see several examples of how the internal control template is applied to different controls. The managers then evaluate whether the internal control is adequately designed or adequately mitigates the stated risk, establishing a control risk level (either high or low). If the manager knows that a particular control is not working, the manager will state that the internal control currently in place has a high control risk. If a high control risk is found during the evaluation, the manager will be responsible for initiating a Corrective Action Plan (CAP) (see figure 7) instead of testing the control. This process eliminates the need for excessive testing when the manager already knows there is a control deficiency. For those controls that management rates with a low control risk, they will then identify the test method they will employ to verify that the control is working effectively. A completed risk analysis for the control points listed in the flowchart above can be seen in figure 5 below.

Figure 5: Complete Risk Analysis



DECA RISK ANALYSIS - FY2009

Assessable Unit: CIO

Assessable Unit Manager: Kathryn Tolliver

Control Number	Process	Risk	Likelihood	Impact	Inherent Risk	Internal Control Currently In Place (ICCIP)	Does the ICCIP mitigate the stated risk?	Control Risk	Internal Control Test Method Used
1	Certification and Accreditation	Leveraging information systems as a foundation to business operations poses some risk to the agency. It is important to ensure that the integrity of information is maintained, confidentiality when required, and availability of resources when needed. Technology is susceptable to attacks, outages, corrupt data and so on, all of which pose risk to the agency and the success of the agency's mission.	3	3	Low	Certification and Accreditation is required annually by the department of defense. Each year, every information system within the agency must traverse the C&A process. On every third year, the DAA (DeCA's CIO) must accept the risk posed to the agency by the system in the form of an approval to operate. On off years, annnual reviews must be conducted, and system owners must demonstrate that the security posture of the sytem they manage is at least as good as it was when the DAA accredited the system.	Yes	High	Inspection
2	Monthly IAVA Scans	Incomplete or inaccurate compliance reporting by information system owners not only opens the Agency up to issues of non-compliance with JTF-GNO, but it also lowers the security posture of the Agency and provides a false sense of security.	3	3	Low	Monthly IAVA scans are run by all affected PM groups within the Agency. These results are provided to the IAPMO and serve to ensure that compliance reporting is accurately reflected in VMS.	Yes	High	Inspection
3	IA Policy Creation and Management	So much of information assurance compliance is based upon formal process, procedures, and policy. These documents serve our user community by helping them understand a certain process as well as the rules that we are all meant to operate by - all of which in some way contribute to the overall security posture of the agency. If these policies, processes, and procedures become out of date, it is difficult for the agency to effectively manage the human element of information security.	3	3	Low	Each year a subset of directives, manuals, and handbooks are selected for review and updated accordingly.	Yes	High	Inspection
4	Information Assurance Audits	It is possible that a recommendation to certify is based upon inaccurate or incomplete information based on the risk outlined in Control #1 (above). This insinuates risk as the security posture of the information system is not truly known. Nor is the remaining residual risk clearly defined and accepted.	3	3	Low	Each year a myriad of auditable items (configurations, processes, procedures, etc.) are identified. These audits are conducted by the IAPMO to help ensure that the security posture of the organization is maintained to the greatest degree possible.	Yes	High	Inspection

Test Plan

During the test plan phase a detailed test description is formulated before completing the documentation and testing of controls (Figure 6). Test plans are reviewed and revised as necessary as the testing phase progresses and new information becomes available. Each area tested by IAMPO is summarized below by process.

Certification and Accreditation

Certification and Accreditation (C&A) is mandated by the Department of Defense (DoD) for all information systems and networks that reside on DoD infrastructure. Each year, every information system within the agency must traverse the C&A process, which is comprised of 151 controls, automated vulnerability assessments, and various checklists. On every third year, the Designated Accrediting Authority (DeCA's CIO) must accept the risk posed to the agency by the system in the form of an Approval to Operate. On off years, annual reviews must be conducted, and system owners must demonstrate that the security posture of the system they manage is at least as good as it was when the DAA accredited the system. The internal control established by IAMPO is meant to ensure that each information system or enclave maintains their Approval to Operate by conducting annual reviews and reaccreditations every three years.

Upon completion of certification and accreditation requirements annually, the System Manager of the system is required to update a DoD system, the Defense Information Technology Portfolio Repository (DITPR), and assert applicable completion dates relevant to the certification and accreditation processes (e.g., controls review date, security test date, contingency plan test date, etc.). IAPMO uses a DITPR report quarterly to ensure that annual reviews are being conducted within established timelines and cycles. The DoD also issues quarterly reports on compliance that assert grades for each defense command/service/agency (C/S/A) in how well they meet their certification and accreditation requirements; this report is reviewed by IAPMO as well.

Monthly IAVA Scans

The Department of Defense patch management process is known as the Information Assurance Vulnerability Management (IAVM) program. Whenever software vendors release security patches and hot fixes for their technology, the DoD issues formal requirements for all subordinate C/S/As to acknowledge the requirement and report compliance (i.e., how many systems are affected, and how many have been fixed). IAPMO distributes the requirements to any potentially impacted directorate within the agency and the Information Assurance Officer for that directorate is responsible for submitting a reply to IAMPO. IAMPO then produces a roll-up based on all replies and reports compliance for the agency via the Vulnerability Management System (VMS) operated by the Defense Information Systems Agency (DISA).

The front end of this process relies solely on the reporting of the impacted organizations, that is, certification and accreditation has no way to technically verify the accuracy of the reporting. To address this potential risk, a control was implemented requiring all systems managers to submit monthly IAVM scans for certification and accreditation or review. This review helps to ensure that what is being reported in VMS is accurate as validated by various vulnerability assessment scanning tools. Once scan results are submitted, IAMPO is able to review the scan results to ensure that what is being reported matches the results of the scan. Areas that are inconsistent are addressed and a plan of action and milestones is created to ensure compliance in a timely fashion.

IA Policy Creation and Management

A large portion of governance in the information assurance arena is establishing policies and procedures that help users and technologists understand what the acceptable operating parameters are, define acceptable user behavior, identify approved system architectures, and so on. Since technology changes rapidly, it is easy for the directives, manuals, and handbooks IAMPO writes to become out-dated and obsolete.

The control implemented is meant to track the utility and applicability of established policy and procedures and help ensure that when DoD guidance or technology changes, IAMPO is able to adjust policy and procedures to align appropriately. As such, each year, IAMPO reviews all directives, manuals and handbooks under their purview and works with appropriate stake-holders to ensure that policy/guidance maintained by IAMPO is updated according to the agency's best interests and compliance objectives initiated by DoD.

Information Assurance Audits

Information assurance audits contribute to the overall security posture of the agency and are usually instigated by DoD requirements released over the course of the year. While these audits do relate to the certification and accreditation process, they are usually performed independently of the C&A cycle. Examples of these audits include wireless security audits at stores, Guard/Reserve Sale physical security audits, Computer Network Defense Service Provider audits, external audit reviews (KPMG), and Payment Card Industry (PCI) compliance audits.

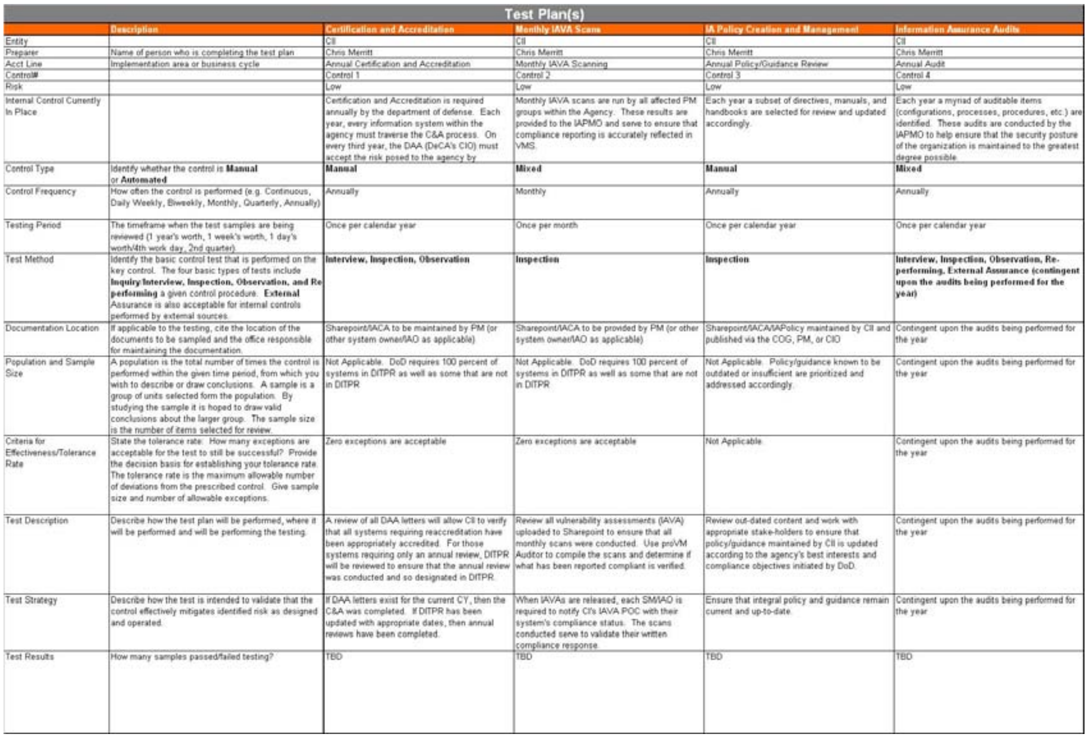
These audits in many ways serve as controls to help validate existing processes and procedures encompassed by other IA and PM processes. The test procedures will vary from audit to audit;

however, each test procedure should ensure the viability and applicability of the audit plan and validate the effectiveness of the process or control being tested.

The Payment Card Industry audit performed annually is more concrete and repeatable because it is specifically governed by the PCI Data Security Standard validation procedures. Upon completion of the audit, each impacted functional area is required to accept/acknowledge the findings, and the Report on Compliance is completed by IAPMO. This report outlines where payment card industry controls are sufficient as well as where deficiencies exist and is coordinated through the Director and eventually submitted to Fifth Third Bank for their review.

A favorable review by Fifth Third Bank demonstrates that this control is effective in helping to maintain the agency's PCI compliance. A negative review would demonstrate the ineffectiveness of this control.

Figure 6



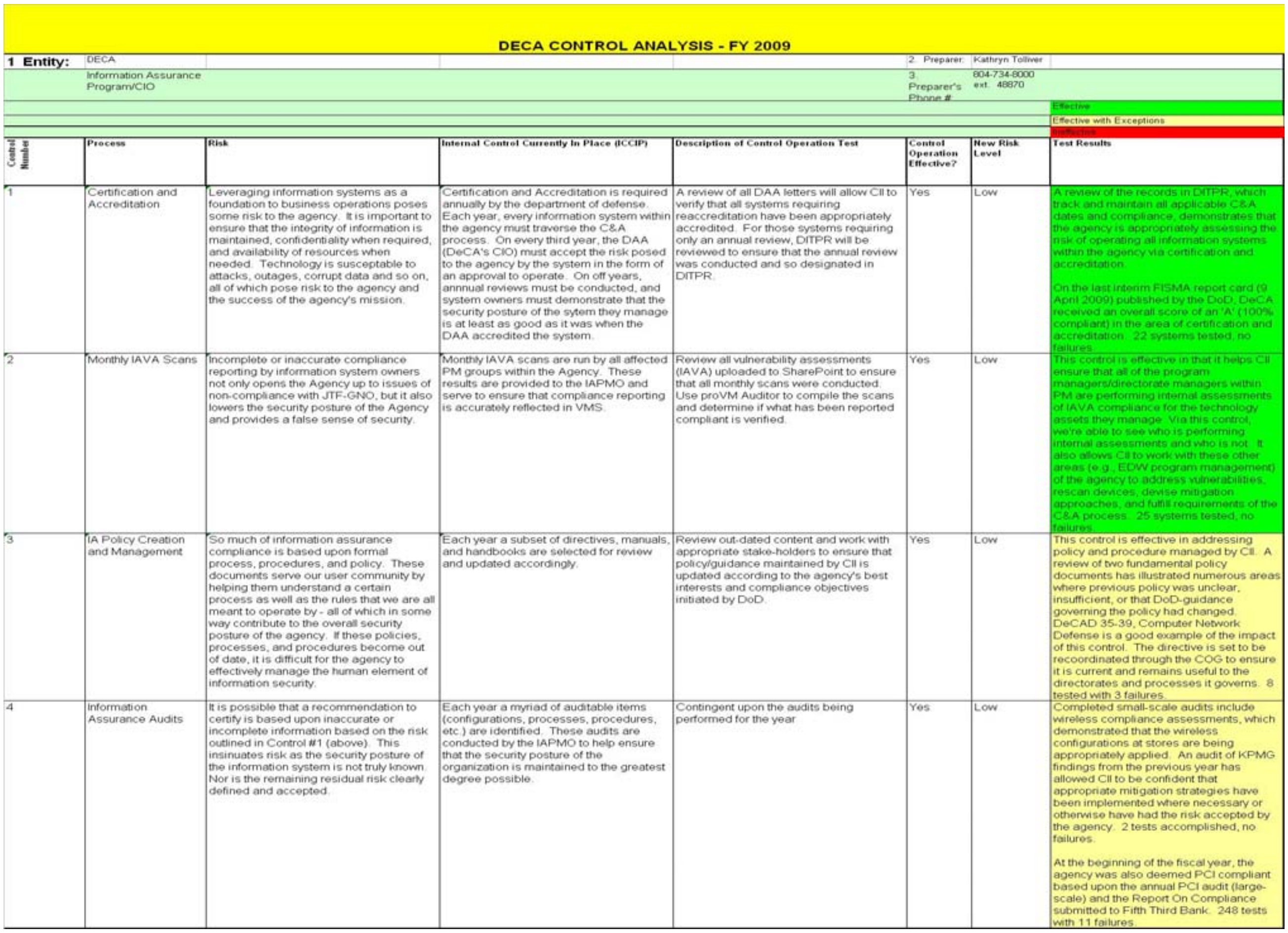
Test Plan(s)

	Description	Certification and Accreditation	Monthly IAVA Scans	IA Policy Creation and Management	Information Assurance Audits
Entity		CII	CII	CII	CII
Preparer	Name of person who is completing the test plan	Chris Merritt	Chris Merritt	Chris Merritt	Chris Merritt
Acct Line	Implementation area or business cycle	Annual Certification and Accreditation	Monthly IAVA Scanning	Annual Policy/Guidance Review	Annual Audit
Control#		Control 1	Control 2	Control 3	Control 4
Risk		Low	Low	Low	Low
Internal Control Currently In Place		Certification and Accreditation is required annually by the department of defense. Each year, every information system within the agency must traverse the C&A process. On every third year, the DAA (DeCA's CIO) must accept the risk posed to the agency by	Monthly IAVA scans are run by all affected PM groups within the Agency. These results are provided to the IAPMO and serve to ensure that compliance reporting is accurately reflected in VMS.	Each year a subset of directives, manuals, and handbooks are selected for review and updated accordingly.	Each year a myriad of auditable items (configurations, processes, procedures, etc.) are identified. These audits are conducted by the IAPMO to help ensure that the security posture of the organization is maintained to the greatest degree possible.
Control Type	Identify whether the control is **Manual** or **Automated**	**Manual**	**Mixed**	**Manual**	**Mixed**
Control Frequency	How often the control is performed (e.g. Continuous, Daily Weekly, Biweekly, Monthly, Quarterly, Annually)	Annually	Monthly	Annually	Annually
Testing Period	The timeframe when the test samples are being reviewed (1 year's worth, 1 week's worth, 1 day's worth/4th work day, 2nd quarter)	Once per calendar year	Once per month	Once per calendar year	Once per calendar year
Test Method	Identify the basic control test that is performed on the key control. The four basic types of tests include **Inquiry/Interview, Inspection, Observation, and Re-performing** a given control procedure. **External** Assurance is also acceptable for internal controls performed by external sources.	**Interview, Inspection, Observation**	**Inspection**	**Inspection**	**Interview, Inspection, Observation, Re-performing, External Assurance (contingent upon the audits being performed for the year)**
Documentation Location	If applicable to the testing, cite the location of the documents to be sampled and the office responsible for maintaining the documentation.	Sharepoint/IACA to be maintained by PM (or other system owner/IAO as applicable)	Sharepoint/IACA to be provided by PM (or other system owner/IAO as applicable)	Sharepoint/IACA/IAPolicy maintained by CII and published via the COG, PM, or CIO	Contingent upon the audits being performed for the year
Population and Sample Size	A population is the total number of times the control is performed within the given time period, from which you wish to describe or draw conclusions. A sample is a group of units selected form the population. By studying the sample it is hoped to draw valid conclusions about the larger group. The sample size is the number of items selected for review.	Not Applicable. DoD requires 100 percent of systems in DITPR as well as some that are not in DITPR	Not Applicable. DoD requires 100 percent of systems in DITPR as well as some that are not in DITPR	Not Applicable. Policy/guidance known to be outdated or insufficient are prioritized and addressed accordingly.	Contingent upon the audits being performed for the year
Criteria for Effectiveness/Tolerance Rate	State the tolerance rate: How many exceptions are acceptable for the test to still be successful? Provide the decision basis for establishing your tolerance rate. The tolerance rate is the maximum allowable number of deviations from the prescribed control. Give sample size and number of allowable exceptions.	Zero exceptions are acceptable	Zero exceptions are acceptable	Not Applicable.	Contingent upon the audits being performed for the year
Test Description	Describe how the test plan will be performed, where it will be performed and will be performing the testing.	A review of all DAA letters will allow CII to verify that all systems requiring reaccreditation have been appropriately accredited. For those systems requiring only an annual review, DITPR will be reviewed to ensure that the annual review was conducted and so designated in DITPR.	Review all vulnerability assessments (IAVA) uploaded to Sharepoint to ensure that all monthly scans were conducted. Use proVM Auditor to compile the scans and determine if what has been reported compliant is verified.	Review out-dated content and work with appropriate stake-holders to ensure that policy/guidance maintained by CII is updated according to the agency's best interests and compliance objectives initiated by DoD.	Contingent upon the audits being performed for the year
Test Strategy	Describe how the test is intended to validate that the control effectively mitigates identified risk as designed and operated.	If DAA letters exist for the current CY, then the C&A was completed. If DITPR has been updated with appropriate dates, then annual reviews have been completed.	When IAVAs are released, each SM/IAO is required to notify CI's IAVA POC with their system's compliance status. The scans conducted serve to validate their written compliance response.	Ensure that integral policy and guidance remain current and up-to-date.	Contingent upon the audits being performed for the year
Test Results	How many samples passed/failed testing?	TBD	TBD	TBD	TBD

Control Analysis

The next step in the ICP is the control analysis, the results from testing of the effectiveness of internal controls. Figure 7 below is an example of a completed Control Analysis by IAMPO/CIO. The risks and controls from the Risk Analysis are mapped to the Control Analysis. In most instances the template provided to the process owners is completed and returned to the MICP for documentation of test results.

Figure 7: Control Analysis



DECA CONTROL ANALYSIS - FY 2009

1 Entity:	DECA Information Assurance Program/CIO	2. Preparer:	Kathryn Tolliver
		3. Preparer's Phone #:	804-734-8000 ext. 48870

🟩 Effective
🟨 Effective with Exceptions
🟥 Ineffective

Control Number	Process	Risk	Internal Control Currently In Place (ICCIP)	Description of Control Operation Test	Control Operation Effective?	New Risk Level	Test Results
1	Certification and Accreditation	Leveraging information systems as a foundation to business operations poses some risk to the agency. It is important to ensure that the integrity of information is maintained, confidentiality when required, and availability of resources when needed. Technology is susceptable to attacks, outages, corrupt data and so on, all of which pose risk to the agency and the success of the agency's mission.	Certification and Accreditation is required annually by the department of defense. Each year, every information system within the agency must traverse the C&A process. On every third year, the DAA (DeCA's CIO) must accept the risk posed to the agency by the system in the form of an approval to operate. On off years, annnual reviews must be conducted, and system owners must demonstrate that the security posture of the sytem they manage is at least as good as it was when the DAA accredited the system.	A review of all DAA letters will allow CII to verify that all systems requiring reaccreditation have been appropriately accredited. For those systems requiring only an annual review, DITPR will be reviewed to ensure that the annual review was conducted and so designated in DITPR.	Yes	Low	A review of the records in DITPR, which track and maintain all applicable C&A dates and compliance, demonstrates that the agency is appropriately assessing the risk of operating all information systems within the agency via certification and accreditation. On the last interim FISMA report card (9 April 2009) published by the DoD, DeCA received an overall score of an 'A' (100% compliant) in the area of certification and accreditation. 22 systems tested, no failures.
2	Monthly IAVA Scans	Incomplete or inaccurate compliance reporting by information system owners not only opens the Agency up to issues of non-compliance with JTF-GNO, but it also lowers the security posture of the Agency and provides a false sense of security.	Monthly IAVA scans are run by all affected PM groups within the Agency. These results are provided to the IAPMO and serve to ensure that compliance reporting is accurately reflected in VMS.	Review all vulnerability assessments (IAVA) uploaded to SharePoint to ensure that all monthly scans were conducted. Use proVM Auditor to compile the scans and determine if what has been reported compliant is verified.	Yes	Low	This control is effective in that it helps CII ensure that all of the program managers/directorate managers within PM are performing internal assessments of IAVA compliance for the technology assets they manage. Via this control, we're able to see who is performing internal assessments and who is not. It also allows CII to work with these other areas (e.g., EDW program management) of the agency to address vulnerabilities, rescan devices, devise mitigation approaches, and fulfill requirements of the C&A process. 25 systems tested, no failures.
3	IA Policy Creation and Management	So much of information assurance compliance is based upon formal process, procedures, and policy. These documents serve our user community by helping them understand a certain process as well as the rules that we are all meant to operate by - all of which in some way contribute to the overall security posture of the agency. If these policies, processes, and procedures become out of date, it is difficult for the agency to effectively manage the human element of information security.	Each year a subset of directives, manuals, and handbooks are selected for review and updated accordingly.	Review out-dated content and work with appropriate stake-holders to ensure that policy/guidance maintained by CII is updated according to the agency's best interests and compliance objectives initiated by DoD.	Yes	Low	This control is effective in addressing policy and procedure managed by CII. A review of two fundamental policy documents has illustrated numerous areas where previous policy was unclear, insufficient, or that DoD-guidance governing the policy had changed. DeCAD 35-39, Computer Network Defense is a good example of the impact of this control. The directive is set to be recoordinated through the COG to ensure it is current and remains useful to the directorates and processes it governs. 8 tested with 3 failures.
4	Information Assurance Audits	It is possible that a recommendation to certify is based upon inaccurate or incomplete information based on the risk outlined in Control #1 (above). This insinuates risk as the security posture of the information system is not truly known. Nor is the remaining residual risk clearly defined and accepted.	Each year a myriad of auditable items (configurations, processes, procedures, etc.) are identified. These audits are conducted by the IAPMO to help ensure that the security posture of the organization is maintained to the greatest degree possible.	Contingent upon the audits being performed for the year	Yes	Low	Completed small-scale audits include wireless compliance assessments, which demonstrated that the wireless configurations at stores are being appropriately applied. An audit of KPMG findings from the previous year has allowed CII to be confident that appropriate mitigation strategies have been implemented where necessary or otherwise have had the risk accepted by the agency. 2 tests accomplished, no failures. At the beginning of the fiscal year, the agency was also deemed PCI compliant based upon the annual PCI audit (large-scale) and the Report On Compliance submitted to Fifth Third Bank. 248 tests with 11 failures.

For controls that have been tested by another DeCA entity, such as the IG, Internal Audit, or our external auditors, the results from those findings may be used instead of having to complete a redundant test. The goal of the templates provided is to integrate all information available from entities conducting testing in the Agency, augmented by the additional tests conducted by management, to give a comprehensive picture of the state of each assessable unit's internal controls.

<u>Corrective Action Plans (CAPS)</u>

Once a control deficiency has been discovered, either in the risk analysis phase or as the result of a control failing its operation test, the implementation of a CAP is mandatory. In our experience, the solution of a problem can often take on a life of its own absent strict standards for resolution. DeCA will be using precisely the same CAP format for our overall program as we use in Appendix A. The example provided (see figure 8) is one of the corrective actions we implemented for PCI-DSS.

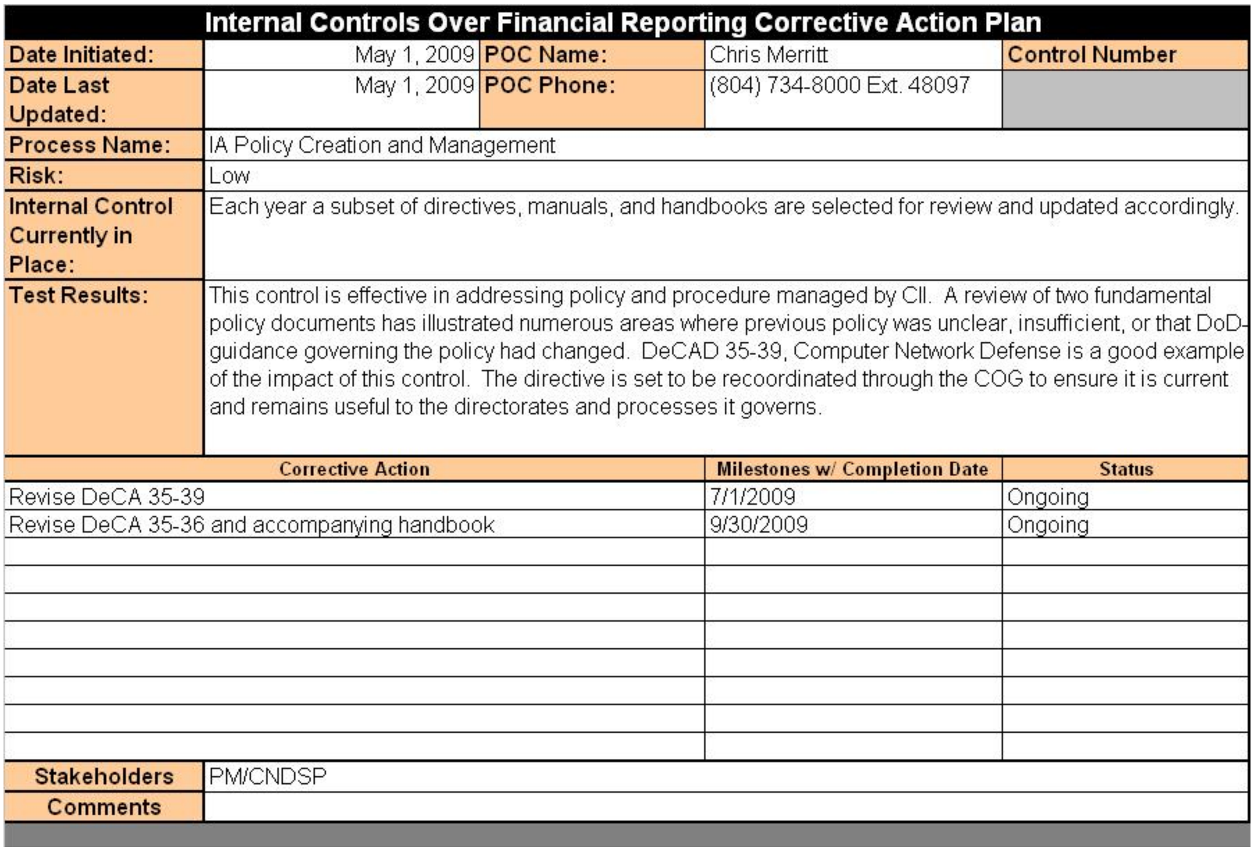
The CAP requires the AUM responsible for the control deficiency to establish:

- An individual responsible for the area where the deficiencies were found;
- A detailed plan to correct the deficiency;
- Milestones and a projected completion date; and

- Status of the solution at each milestone.

The absence of one of these four factors leads to failure when attempting to correct problems. In addition to the responsible manager reporting the status of the solution to the AUM, the AUM must also keep the Senior Assessment Team apprised of their progress. This level of reporting and accountability creates visibility of an issue to our senior managers that was often lacking in the former paradigm.

Figure 8: Corrective Action Plan



Internal Controls Over Financial Reporting Corrective Action Plan

Date Initiated:	May 1, 2009	**POC Name:**	Chris Merritt	**Control Number**
Date Last Updated:	May 1, 2009	**POC Phone:**	(804) 734-8000 Ext. 48097	
Process Name:	IA Policy Creation and Management			
Risk:	Low			
Internal Control Currently in Place:	Each year a subset of directives, manuals, and handbooks are selected for review and updated accordingly.			
Test Results:	This control is effective in addressing policy and procedure managed by CII. A review of two fundamental policy documents has illustrated numerous areas where previous policy was unclear, insufficient, or that DoD-guidance governing the policy had changed. DeCAD 35-39, Computer Network Defense is a good example of the impact of this control. The directive is set to be recoordinated through the COG to ensure it is current and remains useful to the directorates and processes it governs.			

Corrective Action	Milestones w/ Completion Date	Status
Revise DeCA 35-39	7/1/2009	Ongoing
Revise DeCA 35-36 and accompanying handbook	9/30/2009	Ongoing

Stakeholders	PM/CNDSP
Comments	

Internal Control in the Commissaries

In order to improve our control assessments at the store level, beginning in FY 2008, each of DeCA's stores began using a best practice for IG inspection preparation discovered during an internal control evaluation at one of our commissaries. The internal control team evaluated the IG Commissary Compliance Inspection (CCI) checklist and realized that the IG had already well defined the key internal controls at the store level, and that each of our commissaries was required by DeCA policy to systematically prepare for IG inspections. The best practice observed was a simple technique for maintaining all non-sensitive required paperwork that is gathered during the inspection. This technique had the added effect of requiring the department and store managers to constantly review their documentation of their key controls. The stores with this practice in place for FY 2009 have had some of the most effective and efficient processes in the Agency as evidenced by the highest IG scores to date. Recognizing this, the zone managers developed a testing plan similar to the IG CCI checklist and will begin their own structured testing of stores within their zones in FY 2010.

Training

The training of managers and the Agency as a whole is extremely important to the DoD Managers' Internal Control Program. In order to reach all employees, the ICP Manager in coordination with the Corporate Communications Directorate developed a training video that facilitated a greater understanding of the program and led the way for a new culture of thinking**.** The FY 2009 campaign encompassed the Agency's values and promoted a greater understanding on how an employee's knowledge of the internal control process strengthens the performance of their day-to-day business operations. Utilizing the "Check It" message was the starting point for the Agency's campaign. Creating a culture of thinking that emphasizes checking how you do your job and utilizing the tools of the internal control program would assist employees in doing a better job in their daily work.

We challenged the almost 18,000 employees at the Agency to become aware of how their job influences the overall operations of the Commissary. Detailed training was provided on the video that explained the Appendix A methodology and how to implement the methodology in the different business environments of the Agency. We began our video training with a historical background provided by the DoD Managers' Internal Control Program Manager, Peggy Johnson. We asked Peggy to provide our opening comments to reinforce DoD's commitment for the Department's financial improvement and audit readiness through the utilization of the Appendix A methodology. We felt that "Know Your Role In Internal Control" provides a link to not only our Agency strategic plan and values, but to DoD's mission of providing the military forces needed to deter war and to protect the security of our country through good stewardship of tax payer dollars. "Know Your Role In Internal Control" provides us the opportunity to transform our workforce into a more agile, knowledgeable and motivated team who will be aware of how work performance influences the Agency's operational effectiveness and successes. The slogan for the Agency's campaign was "Put the L-I-F-E back in my working day – Know Your Role In Internal Control!" The DeCA values L-I-F-E are the engine behind the vision that highlights the Agency's commitment to the people who deliver and receive the commissary benefit, our military forces.

L-Leadership…We expect passion, courage and excellence!
I-Integrity…….We demand honesty, professionalism and trustworthiness!
F-Flexibility….We cultivate innovation, empowerment and competence!
E-Enjoyment….We foster teamwork, recognition and opportunity!

The video developed for all our employees to view and receive training was placed on DeCA's OneNet. OneNet is our Agency intranet location that unites DeCA's team members online. Further outreach opportunities are available on our SharePoint website, our documentation management location for all Appendix A methodology information. Our sharepoint website gives links to OneNet, Commissaries.com, Office of Personnel Management, OMB Circular A-123, DoD 5010.40 and the former Check It Campaign.

In coordination with DeCA Corporate Communications, Marketing Branch information cards and announcement posters that provide outreach opportunities to our employees to contact our

MICP staff for assistance and to learn more about the Appendix A methodology are under development. These cards and posters will serve as a visual reminder of an employee's role in the internal control process and provide another avenue for learning.

Inspector General

The IG plays a vital role in the validation of the effectiveness of internal controls within the Agency. They are the front line investigators responsible for establishing that the internal controls at the store level are adequately implemented and monitored. There are two types of inspections the IG conducts: the unannounced CCI and the Staff Assistance Compliance Inspection (SACI).

The CCIs are designed for commissaries where risk assessment indicators show that the activity would benefit from an inspection; where a follow-up inspection is needed based on prior inspection results or recent events; or when nominated by the DeCA leadership. The CCI checklist that assesses a commissary's internal controls was updated as of December 12, 2008. The CCI checklist is reviewed and updated annually. Fifteen percent of DeCA commissaries will have a CCI in FY 2009.

The SACI is based on requests from the Director, Chief Executive Officer, Chief Operating Officer, region directors, deputy directors, or zone managers. These inspections are conducted like a CCI but are offered in lieu of a CCI. For example, a SACI may be requested as announced or unannounced when a new store director is scheduled to report or has recently reported to a commissary. The SACI is designed to help the new store director baseline his or her commissary, central distribution center, or Central Meat Processing Plant and establish goals and priorities. Specific or system-wide issues may be analyzed requiring research and site visits to conduct evaluations and collect data. These reviews/evaluations are generally narrower in focus. They are designed to target high risk, known, or suspected problems with processes (e.g., purchase card or inventory accountability) with the final report going to the process owner, Director, Chief Executive Officer, and Chief Operating Officer. Often, these inspections are conducted at the direction or request of the senior leadership.

IG inspectors and evaluators adhere to the Quality Standards for Inspections issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) (formerly President's Council on Integrity and Efficiency and the Executive Council on Integrity and Efficiency) for all inspections and evaluation work.

Internal Audit

The Office of Internal Audit performs a multitude of professional audit services at headquarters, region, and store-level. Their focus is to perform audit services that:

- Improve the commissary benefit;
- Decrease costs without diminishing the benefit; and
- Evaluate the significant, long-term, or systemic issues that are crucial to mission performance or that pose a risk for fraud, waste, or abuse.

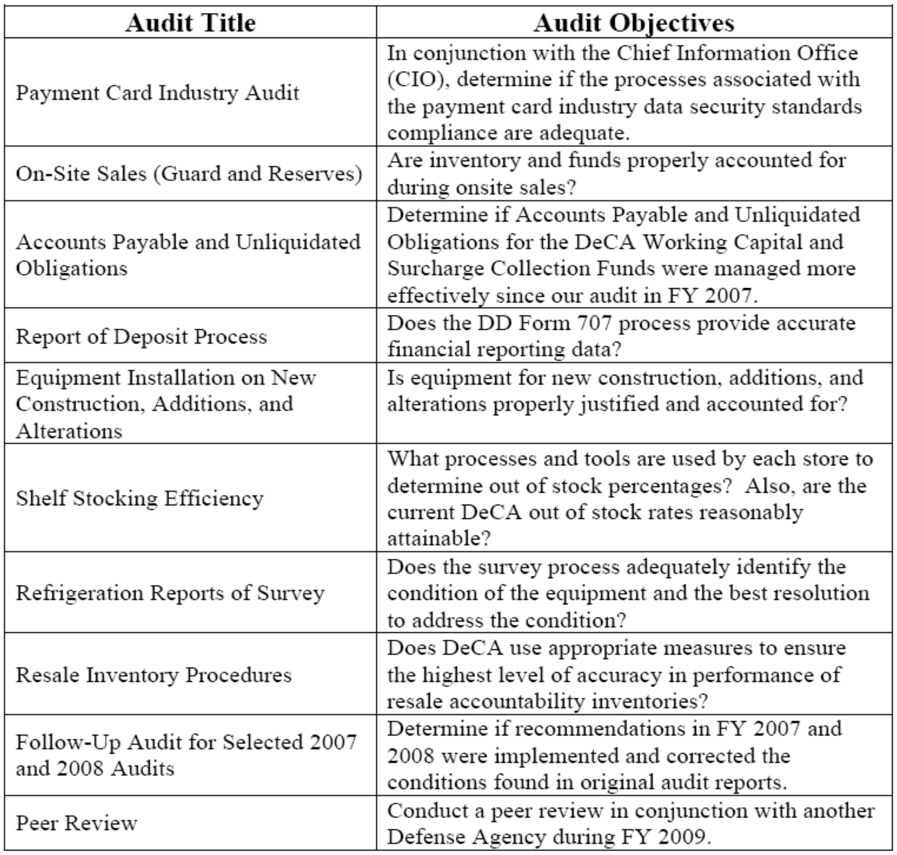
In addition to providing internal audit services, they serve as the primary liaison for all external audits conducted by the Government Accountability Office (GAO) and the Department of Defense Inspector General.

To develop their internal audit plan, they solicited audit topics and suggestions from DeCA directors and staff office chiefs, regions, stores, and the Management Oversight Committee of the Commissary Operating Board. They also generated audits internally based on:

- DeCA's strategic plan and direction;
- Management-identified control risk;
- Emerging issues; and
- Audit entity files.

In addition to the audit suggestions and the internally generated audits, the plan includes follow-up audits which are required by the GAO Comptroller General of the United States.

FY 2009 Audit Plan



Audit Title	Audit Objectives
Payment Card Industry Audit	In conjunction with the Chief Information Office (CIO), determine if the processes associated with the payment card industry data security standards compliance are adequate.
On-Site Sales (Guard and Reserves)	Are inventory and funds properly accounted for during onsite sales?
Accounts Payable and Unliquidated Obligations	Determine if Accounts Payable and Unliquidated Obligations for the DeCA Working Capital and Surcharge Collection Funds were managed more effectively since our audit in FY 2007.
Report of Deposit Process	Does the DD Form 707 process provide accurate financial reporting data?
Equipment Installation on New Construction, Additions, and Alterations	Is equipment for new construction, additions, and alterations properly justified and accounted for?
Shelf Stocking Efficiency	What processes and tools are used by each store to determine out of stock percentages? Also, are the current DeCA out of stock rates reasonably attainable?
Refrigeration Reports of Survey	Does the survey process adequately identify the condition of the equipment and the best resolution to address the condition?
Resale Inventory Procedures	Does DeCA use appropriate measures to ensure the highest level of accuracy in performance of resale accountability inventories?
Follow-Up Audit for Selected 2007 and 2008 Audits	Determine if recommendations in FY 2007 and 2008 were implemented and corrected the conditions found in original audit reports.
Peer Review	Conduct a peer review in conjunction with another Defense Agency during FY 2009.

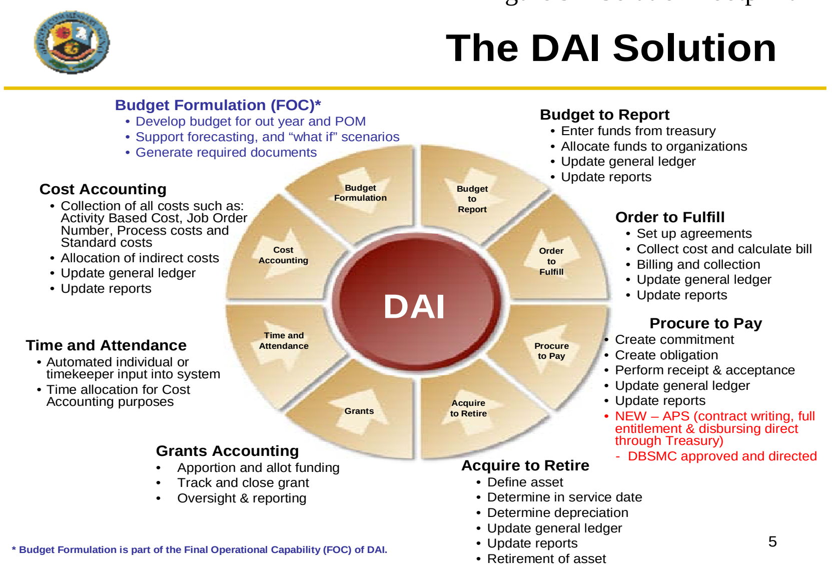
<u>Evidence of Control Issues Discovered or Resolved During Reporting Period</u>

<u>Description of Issue:</u> Integrated financial system conformance with the Federal requirements of the Federal Financial Management Improvement Act (FFMIA) of 1996 and the OMB Circular No. A-127, and as prescribed by DoD 7000.14-R, Volume 1, Chapter 3, “Federal Financial Management Improvement Act of 1996 Compliance, Evaluation and Reporting,” October 2008.

<u>Accomplishments</u>:

DeCA’s legacy financial systems are not compliant with the U.S. Standard General Ledger (USSGL) and fall short of integrated system requirements for FY 2009. As a result the detailed level transactions are not captured at the USSGL level. During the FY 2008 audit KPMG, independent auditor, identified non compliance as a significant deficiency but it was not believed to be a material weakness. The Agency has multiple compensating controls to mitigate these risks. DeCA continually employs a system of processes and detailed reconciliations that adequately address these issues. In addition DeCA, jointly with the DoD, is actively working on improving the business system DoD wide. Illustrated in figure 9 is the DoD business solution footprint. DeCA is projected for implementation of DAI in 4th Quarter FY 2011.

Figure 9 – Solution Footprint



The DAI Solution

Budget Formulation (FOC)*
- Develop budget for out year and POM
- Support forecasting, and “what if” scenarios
- Generate required documents

Budget to Report
- Enter funds from treasury
- Allocate funds to organizations
- Update general ledger
- Update reports

Cost Accounting
- Collection of all costs such as: Activity Based Cost, Job Order Number, Process costs and Standard costs
- Allocation of indirect costs
- Update general ledger
- Update reports

Order to Fulfill
- Set up agreements
- Collect cost and calculate bill
- Billing and collection
- Update general ledger
- Update reports

Time and Attendance
- Automated individual or timekeeper input into system
- Time allocation for Cost Accounting purposes

Procure to Pay
- Create commitment
- Create obligation
- Perform receipt & acceptance
- Update general ledger
- Update reports
- NEW – APS (contract writing, full entitlement & disbursing direct through Treasury)
  - DBSMC approved and directed

Grants Accounting
- Apportion and allot funding
- Track and close grant
- Oversight & reporting

Acquire to Retire
- Define asset
- Determine in service date
- Determine depreciation
- Update general ledger
- Update reports
- Retirement of asset

* Budget Formulation is part of the Final Operational Capability (FOC) of DAI.

5

<u>Description of Issue</u>: Modernize DeCA’s Supply Chain business systems in conjunction with DAI

<u>Accomplishments</u>:

- DeCA approached BTA to share lessons from other DoD business modernization programs as we faced the daunting challenge of replacing our supply chain business systems at the same time as we planned to implement DAI. BTA has agreed to collaborate on identifying our end-to-end business processes and determine commonality between the financial and supply chain systems.

- DeCA is serving as a project model to adopt COTS efficiencies and to minimize the number of modifications and interfaces needed to effectively perform all required Agency business processes.

Description of Issue: Reduction of Aged Accounts Payable and Undelivered Orders

Accomplishments:

- Reduced Agency aged AP and UDO by 50 percent from 10,027 records in September 2007 to 5,010 records in FY 2009 using expected period of performance as a trigger for completing final deliveries and payments. All unliquidated obligations were stratified according to their function within the Agency's mission and an expected period of performance determined. Once that performance period was completed, lists were sent to multi-disciplined task groups to affect final payments and close out the orders.
- This reduction in aged records resulted in 5000 less orders to review each fiscal year during the mandated triannual review of unliquidated obligations, a substantial workload reduction for the Agency.

DeCA's ability to deliver the premiere military benefit depends on our efforts to recognize opportunities for improvement and to implement them as fully as possible, as soon as possible. Our wholehearted commitment to the military community that depends on us demands that we continue to look for new and innovative methods to conduct our business. This program is an acknowledgment that internal controls and our systems for testing their effectiveness will continue to be a top priority for the Agency.