ARMICS Review Checklist

DOA reviews ARMICS documentation to determine if the minimum requirements according to the Agency Risk Management and Internal Control Standards have been met. These requirements can be found on pages 18, 21, 27, 31, and 35 of the standards. http://www.doa.virginia.gov/Admin_Services/ARMICS/ARMICS_Standards.pdf

MR = Minimum Requirement

Agency-level review

1 Does the agency documentation contain a list and description of agency-level controls (policies and procedures, code of ethics, background checks on employees, access controls – physical and system, etc.)? There needs to be a document that spells out "these are our agency-level controls" and indicates which ones were tested.	
2 Description of how the agency assessed (tested) the agency-level controls. (Surveys? Who was surveyed? Interviews, and what controls were tested, how they were tested and the results of those tests.) **Note: Surveys are NOT a test of control. Surveys can help an agency identify problem areas. They can be part of an assessment, but not THE assessment.** **Note: Surveys are not required by ARMICS.**	
3 Did the agency provide a Summary and Analysis of the agency-level assessment?	
4 Did the agency provide copies of all documentation to include surveys, testing sheets, summaries?	
5 **MR -** Agency-level risk assessment – review and describe. Was it adequate? Standard says: "Conduct and document an agency-wide risk assessment. This risk assessment should be coordinated with the strategic planning process overseen by the Department of Planning and Budget." This is where the Agency takes a good look at itself – purpose, core functions, etc. The risk of fraud must be considered.	

6 **DPB requirement** - SWOT analysis – is it current? Did management review and use the information? (Even if DPB doesn't require a SWOT anymore, agencies should use it as part of their risk assessment.)	
7 **MR** – Did the agency create a code of ethics?	
7A **MR –** Does the agency actively promote the code of ethics (COE)? Is the COE displayed? Is it on the website for the public to see? Do employees acknowledge receipt of the COE? Does the agency perform training on ethics?	
8 **MR** – Did the agency **document and assess key elements** of the control **environment** including, but not limited to: Management philosophy Management's attitude towards risk Oversight by the agency's governing board Integrity and ethical values Promotion of ethics and appropriate conduct Organizational structure Workforce competence and human resource development Assignment of authority and responsibility ***Note: Assess means TEST.***	
9 Give brief description of ***Management philosophy*** and how they documented it and tested it for ARMICS	
10 Give brief description of ***Management's attitude towards risk*** and how they documented it and tested it for ARMICS	
11 Give brief description of ***Oversight by the agency's governing board*** and how they documented it and tested it for ARMICS	
12 Give brief description of ***Integrity and ethical values*** and how they documented it and tested it for ARMICS	
13 Give brief description of ***Promotion of ethics and appropriate conduct*** and how they documented it and tested it for ARMICS	
14 Give brief description of ***Organizational structure*** and how they documented it and tested it for ARMICS	

15 Give brief description of ***Workforce competence and human resource development*** and how they documented it and tested it for ARMICS	
16 Give brief description of ***Assignment of authority and responsibility*** and how they documented it and tested it for ARMICS	
17 **MR –** did the agency **document and assess agency-level control activities** applicable to: o All significant fiscal processes o Accounting administration o The general ledger o Information systems *Does the agency have sufficient documentation showing they identified and tested the agency-level controls for the above? Note: Information Systems may have been tested by an IT expert – not necessarily the finance department. Ask to see if the IT department at the agency gave assurance to management for ARMICS.*	
18 When was the agency-level evaluation completed? Has the agency undergone any organizational changes that suggest that the agency-level evaluation (assessment) should be performed again? Note: Agency-level evaluation should be redone when executive management turn-over occurs, or every three years as a best practice.	
19 Has the agency updated or retested areas of internal control that needed improvement? Have they revisited the key controls in the Agency-level assessment?	
20 **MR: Information and communication internal control component –** Did the agency document and assess how the agency gathers, uses and disseminates information?	
21 “Information and Communication” involves identifying, capturing and communicating relevant information in a form and timeframe that enables people to carry out their responsibilities. Effective communication occurs down, across and up the agency. An effective information and communication	

process will assure that all personnel receive a clear message from top management that internal control responsibilities must be taken seriously. See page 29 and 30 of the standards. External communication is also critical – citizens, stakeholders, other agencies. How does the agency communicate? Do they have meetings, intranet? Internet? Memos? Training? Town hall type meetings with staff and citizens?	
22 **MR: Monitoring internal control component –** Did the agency document and assess the effectiveness of the agency's monitoring activities?	
23 "Monitoring" is the process of assessing the presence, functioning, and continuous improvement of internal control components. Monitoring is accomplished through ongoing management activities, separate evaluations, or both. • Managers reviewing operating reports and performance measures. • Internal auditors, external auditors, and advisors regularly providing recommendations. • Training seminars, planning sessions and other meetings giving feedback to management. • Management reviews reports of key activity indicators, including financial and operating statistics. • Management reviews error rates, items in suspense, or reconciling items. • Management reviews key performance indicators such as trends in direction and magnitude of risks, status of strategic and tactical initiatives, or trends in actual results compared to budget or prior periods. Describe the agency's monitoring. **Did the agency follow up on and monitor necessary internal control improvements? Did they take action on APA items? Did they temporarily or permanently fix the problem?**	

Transaction-level review (Processes)

24 Obtain a list of all significant fiscal processes and how the list was created. The agency should explain the criteria for including or not including a process for assessment and testing. Is it a complete listing based on the agency's function and purpose? Note: Financial reporting and monthly reconciliations should always be considered a significant fiscal process by the Agency.	
25 **MR –** Was a risk assessment performed on each of the significant processes? (The MR states "Conduct and document risk assessments of each agency fiscal process as part of the documentation and assessment of control activities.") The risk of fraud must be considered.	
26 **MR -** Were the key controls identified and tested? Was the testing adequate? Is there sufficient documentation of completed test work and the results of those tests? (MR states: "Document all significant agency fiscal processes and assess the operation of their associated control activities.") Note: The process, risk and control matrix is a good way of documenting.	
27 **MR –** was each significant process tested as required? If not, was a plan or schedule provided for testing? What is their testing schedule going forward? (After the initial testing, each process should be tested at least every third year. This does not mean they can wait and test everything every third year – it should be done on a rolling basis. Many processes require annual testing due to significance.)	
28 Please indicate whether each significant process has current and accurate written procedures.	
29 Is there a summary and analysis of the	

transaction-level assessment by the agency?	
30 Were significant weaknesses identified? If, so does the corrective action plan **(required if significant weaknesses)** seem appropriate for the significant weaknesses identified? Were they corrected? Were they retested?	
31 Did the agency certify ARMICS? What type of certification? (See CAPP – Cardinal Topic No. 10305)	
32 Was there sufficient supporting documentation in order to certify?	

Notes:

Agency-level controls – These include controls such as: policies and procedures, code of ethics, background checks on employees, access controls – physical and system, etc. - anything that affects the whole agency.

Surveys - Doing a survey does not mean that the agency has assessed controls or performed ARMICS. The surveys in the ARMICS manual are meant to be a tool for helping an agency identify areas that should be targeted for further investigation, but they do not identify specific agency-level controls that exist at an agency. The surveys do not identify key internal controls for the agency and the surveys are not a test of control. The surveys are just a tool to help agencies identify higher risk areas they need to focus on for further analysis. The surveys are not a requirement of ARMICS. The surveys are a generic tool that can assist agencies in getting started and identifying risk areas.

Testing – Do agencies follow their own policies? – they say they do background checks – well, did they pull a sample of HR files? Was everyone checked? They say they do training for employees – did they offer any training in the last 2 years? Was attendance mandatory? Proof of completion? They say they have access controls – Are they tested? Are the policies followed? (Look at the onboarding and offboarding policies and processes.) They say they do timely employee reviews and have management feedback for employees – did someone interview employees for testing? Did they meet timely? Did employees get feedback? Did someone pull HR files to see if EWPs were updated, filed timely? Did HR review to ensure KSA's matched the job description?

Note/tip: A good way to ensure policies and procedures are kept up to date is to have section managers certify to the agency that their procedures and policies are current and up to date. As part of ARMICS testing, the agency should sample some procedures and do a walk through or the process or interview staff to see if up to date and current. What was sampled and the results of those tests should be documented.

Management philosophy – Does management communicate their tone at the top? How?
Management's attitude towards risk – What evidence do you have of management's attitude toward risk? Were the SWOT and Risk Assessment completed? Were they acted on? Does management have Security Policies and Policies dealing with safety and information security? Do they have committees formed? IT Steering?
Oversight by the agency's governing board - Depends on the agency – Where do they get their direction from?
Integrity and ethical values – Do they communicate this? Code of ethics? Do they follow their own policies? Are wrong doers corrected?
Promotion of ethics and appropriate conduct - Training offered, requirements, policies, do they have a hotline? Policies for reporting fraud and misconduct?
Organizational structure – Is this documented? Why are they set up the way they are? Do they review? Is there a better way? Are there clear communication channels? Do they have meetings regularly?
Workforce competence and human resource development – See paragraph on testing above for ideas on assessment and what to expect.
Assignment of authority and responsibility – Usually this is done through EWPs, policies and procedures and these should all match. If a secretary is doing high-level work – most likely the EWP isn't going to match daily activities.

The ARMICS Agency-level Assessment should be repeated at least every three years as a best practice. If there is a change in leadership, a change in policies, processes, or procedures or any other significant change that affects the agency, then the Agency-level Assessment should be repeated sooner. Per the CAPP Manual Topic No. 10305, *Internal Control*:

> Once the [Agency-level assessment] has been successfully implemented, the agency does not have to repeat this process each year. However, the agency should refresh and refine the agency-level control evaluation every year considering:
>
> • Any changes to the organization, its management, or functions from prior implementations of ARMICS;
>
> • Enhancements identified internally from prior ARMICS experiences, DOA Quality Assurance Reviews (QARs), APA audits, or other sources;
>
> • Information from the most recent S.W.O.T. (Strengths, Weaknesses, Opportunities, and Threats) analysis; and,

- Best internal control practices from industry, governments, and other agencies.

Continuity of Operations Plan (COOP) – DOA does not review COOP plans as that is done by VDEM, but as a critical agency-level control, the ARMICS process should ensure that COOP is up to date and tested.

Agencies should include written summaries of both the Agency-level and the Transaction-level assessments with their ARMICS documentation.

Agency-level risk assessment – This is no one page document – this should be every division and unit describing what they do and the risks they face – what could happen to keep them from doing their job. Input should be received from each division or unit. This is a big and important undertaking. Risks include – outside forces – weather, disasters, aging workforce, loss of knowledge, and changing technologies. This cannot be one person writing something in a vacuum – even in a five person agency – there needs to be input from all departments and sections.

Significant Processes:

- consumes a proportionally large share of agency resources;
- has a high-degree of public visibility;
- represents areas of concern and high risk to mission-critical business processes for agency managers and stakeholders, or;
- has a significant affect on general ledger account balances.

Decisions about significance should take into account not only quantitative, but also qualitative factors.

When identifying significant fiscal processes, ***financial reporting*** and ***reconciliations*** should be documented processes with testing performed annually.

Types of Control Activities include preventive, detective, manual, computer, and management controls. Control activities can correspond to specified control objectives, such as ensuring completeness and accuracy of data processing. Control activities can be classified in the following eight broad categories:

- **Authorization –** Control activities in this category are designed to provide reasonable assurance that all transactions are within the limits set by policy or that exceptions to policy have been granted by the appropriate officials.

- **Review and Approval –** Control activities in this category are designed to provide reasonable assurance that transactions have been reviewed for accuracy and completeness by appropriate personnel.

- **Verification –** Control activities in this category could encompass a variety of computer and manual controls that are designed to provide reasonable assurance that all accounting information has been correctly captured.

- **Reconciliation –** Control activities in this category are designed to provide reasonable assurance of the accuracy of financial records through the periodic comparison of source documents to data recorded in accounting information systems.

- **Physical Security over Assets –** Control activities in this category are designed to provide reasonable assurance that assets are safeguarded and protected from loss or damage due to accident, natural disaster, negligence or intentional acts of fraud, theft or abuse.

- **Segregation of Duties –** Control activities in this category reduce the risk of error and fraud by requiring that more than one person complete a particular fiscal process.

- **Education, Training and Coaching –** Control activities in this category reduce the risk of error and inefficiency in operations by ensuring that personnel have the proper education and training to perform their duties effectively. Education and training programs should be periodically reviewed and updated to conform to any changes in the agency environment or fiscal processing procedures.

- **Performance Planning and Evaluation –** Control activities in this category establish key performance indicators for the agency that may be used to identify unexpected results or unusual trends in data which could indicate situations that require further investigation and/or corrective action.

Information Systems General Controls include controls over information technology management, infrastructure, security management, and software acquisition, development, and maintenance. For example:

- **Information Technology Management** – A steering committee oversees, monitors, and reports on information technology activities and improvement initiatives.

- **Information Technology Infrastructure** – Controls apply to system definition, acquisition, installation, configuration, integration, operation, and maintenance. Controls include continuity of operations (COOP) planning, scheduling of computer operations, restricting access to system configuration and operating system software, incident tracking, system logging, and monitoring use of data-altering utilities.

- **Security Management** – Secure passwords restrict internal access to the network, database, and applications. Firewalls and virtual private networks protect data from unauthorized external access.

- **Software Acquisition, Development, and Maintenance** – Software acquisition and implementation controls are incorporated into a formal change management process. One control over development is allowing software developers to work only in segregated development environments with no access to the production environment. System change controls include authorizations, reviews, approvals, documentation, and testing.

ARMICS will have to be redone with respect to processes impacted by Cardinal. Agencies will have to write new procedures and re-evaluate risks and controls over significant processes.