North Carolina Department of Information Technology

Corrective Action Plan (CAP) Instructions

July 2016

CONTENTS

INTRODUCTION

The CAP document is a key document in the tracking and remediation of risks and vulnerability process for the State Agencies. It describes the specific tasks the AGENCY has planned to correct any weaknesses or deficiencies in the security controls noted during the assessment and to address the residual vulnerabilities in the information system.

AGENCYs develop the CAP document in the CAP Template according to the rules and requirements described in this guide to ensure consistency across providers.

PURPOSE

The purpose of the CAP is to facilitate a disciplined and structured approach to mitigating risks in accordance with the AGENCY's priorities. The CAPs include the findings and recommendations of the security assessment report and the continual security assessments.

ESRMO uses the CAP to monitor progress in correcting weaknesses or deficiencies noted during the security control assessment and throughout the continuous monitoring process.

The CAPs are based on the:

- Security categorization of the cloud information system
- Specific weaknesses or deficiencies in deployed security controls
- Importance of the identified security control weaknesses or deficiencies
- Scope of the weakness in systems within the environment
- Proposed risk mitigation approach to address the identified weaknesses or deficiencies in the security controls (for example, prioritization of risk mitigation actions, allocation of risk mitigation resources)

The CAP identifies: (i) the tasks the AGENCY plans to accomplish with a recommendation for completion either before or after information system implementation; (ii) any milestones the AGENCY has set in place for meeting the tasks; and (iii) the scheduled completion dates the AGENCY has set for the milestones.

OWNER

State Chief Risk Officer

The Department of Information Technology Enterprise Security Risk Management Office (ESRMO)

SCOPE

This policy applies to state agencies, departments and other entities not specifically excluded from Article 14 of N.C. General Statute Chapter 143B

DEFINITIONS

Unless specifically defined in this policy, terms are defined in the Statewide Glossary of Information Technology Terms.

PART 1. CORRECTIVE ACTION PLAN (CAP) TEMPLATE

WORKSHEET 1: CAP TEMPLATE

AGENCYs gather and report basic system and weakness information in the CAP Template. The CAP Template is an Excel Workbook containing three worksheets: The current system CAP worksheet, the closed (mitigated) CAP worksheet, and an up-to-date System Inventory worksheet. AGENCYs should complete the System Inventory worksheet first because the Asset Identifier in the CAP worksheet refers to the inventory items.

The CAP Template worksheet has two sections. The top section of the CAP documents basic system information and tracks the headers described in the table below:

Table 1 - CAP Template Header Information Description

Headers	Details
AGENCY	The Vendor Name as supplied in any of the documents provided to the AO.
System Name	The Information System Name as supplied in any of the documents provided to the Agency CIO or designee.
CAP Date	The date the CAP was created, which is the date the AGENCY committed to in their continuous monitoring plan.

The bottom section of the CAP Template worksheet is the corrective action plan used to track IT security weaknesses. This section of the CAP worksheet has some similarities to the National Institute of Standards and Technology's (NIST) format requirements, but requires additional data and formatting as required by ESRMO.

Table 2 – CAP Template Column Information Description

Column	Details
Column A – CAP ID	Assign a unique identifier to each CAP item. This can be in any format or naming convention that produces uniqueness, but ESRMO recommends the convention V-<incremented number>. (for example, V-123)
Column B – Controls	Specify the ESRMO security control affected by the weakness identified during the security assessment process.
Column C– Weakness Description	Describe the weakness identified during the assessment process. Use the Weakness Description provided by the security assessor or the vulnerability scanner that discovered the weakness. Provide sufficient data to facilitate oversight and tracking. This description should demonstrate awareness of the weakness and facilitate the creation of specific milestones to address the weakness. In cases where it is necessary to provide sensitive information to describe the weakness, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
Column D – Weakness Source Identifier	Often the scanner/assessor will provide an identifier (ID/Reference #) that specifies the weakness in question. This allows further research of the weakness. Provide the identifier, or state that no identifier exists.
Column E – Asset Identifier	List the asset/platform on which the weakness was found. This should correspond to the Asset Identifier for the item provided in Worksheet 3, Inventory List, as well as any applicable network ports and protocols. Include a complete Asset Identifier for each affected asset. Do not use an abbreviation or "shorthand". The AGENCY may obfuscate the asset

	information when it is required by the internal policies of the AGENCY. The Asset Identifier must be unique and consistent across all CAP documents, Security Liaisons, and any vulnerability scanning tools. See Section **Error! Reference source not found.** for formatting requirements.
Column F – Point of Contact	Identify the person/role that the AO holds responsible for resolving the weakness. The AGENCY must identify and document a Point of Contact (POC) for each reported weakness.
Column G – Resources Required	Identify any cost associated with resolving the weakness and provide an estimated staff time in hours.
Column H – Overall Remediation Plan	Provide a high-level summary of the actions required to remediate the plan. In cases where it is necessary to provide sensitive information to describe the remediation plan, italicize the sensitive information to identify it and include a note in the description stating that it is sensitive.
Column I – Original Detection Date	Provide the month, day, and year when the weakness was first detected. This should be consistent with the Security Assessment Report (SAR) and/or any continuous monitoring activities.
Column J – Scheduled Completion Date	The AGENCY must assign a completion date to every weakness that includes the month, day, and year. The Scheduled Completion Date column must not change once it is recorded. See Section **Error! Reference source not found.** for guidance on closing a CAP item.
Column K – Planned Milestones	Each weakness must have a milestone entered with it that identifies specific actions to correct the weakness with an associated completion date. Planned Milestone entries shall not change once they are recorded.
Column L – Milestone Changes	List any changes to existing milestones in Column L, Planned Milestones in this column.
Column M – Status Date	This column should provide the latest date an action was taken to remediate the weakness or some change was made to the CAP item.
Column N – Vendor Dependency	This column should specify whether the remediation of the weakness requires the action of a third party vendor. Should a weakness be vendor dependent, a monthly update with the third party vendor is required. In these cases, the weakness cannot be remediated, and the CAP item cannot be closed, but the completion date may be extended if a monthly update is made. If the completion date is extended, provide an update in Column L, Milestone Changes.
Column O – Last Vendor Check-in Date	If the remediation of the weakness is dependent on a third party vendor's action, as specified in Column N, Vendor Dependency; a monthly update with the third party vendor is required. Provide the date that the latest update was made.
Column P – Vendor Dependent Product Name	If the remediation of the weakness is vendor dependent, provide the name of the product for which the third party vendor has responsibility.
Column Q – Original Risk Rating	Provide the original risk rating of the weakness at the time it was identified as part of an assessment and/or continuous monitoring activities.
Column R – Adjusted Risk Rating	Provide the adjusted risk rating as approved by the Agency CIO or designee. If no risk adjustment is made, state N/A.
Column S – Risk Adjustment	State the status of the risk adjustment request. AGENCY determination of a risk adjustment will cause this column to be set to "pending". The adjustment

	is finalized (setting the Risk Adjustment to "yes") if it is approved by the AO. Approved risk adjustments may alter the scheduled completion date.
Column T – False Positive	State the status of the weakness deviation request for false positive. A false positive means the weakness is determined to be non-existent and is a false positive provided by the vulnerability scanner. A AGENCY determination of a false positive will cause this column to be set to "pending", the deviation is finalized (setting the status to "yes") if it is approved by the Agency CIO or designee. Approved false positives can also be closed, see section **Error! Reference source not found.** for guidance on closing a CAP item.
Column U – Operational Requirement	State the status of the weakness deviation request for operational requirement. An operational requirement means that the weakness cannot be remediated without affecting the operation of the system. A AGENCY determination of an operational requirement will cause this column to be set to "pending", the deviation is finalized (setting the status to "yes") if it is approved by the Agency CIO or designee. Approved operational requirements remain on Worksheet 1, CAP Template, and are to be periodically reassessed by the AGENCY.
Column V – Deviation Rationale	Provide a rationale for the various weakness deviations requested for the item.
Column W – Supporting Documents	List any additional documents that are associated with the CAP item.
Column X – Comments	Provide any additional comments that have not been provided in any of the other columns.

WORKSHEET 2: CLOSED CAP ITEMS

The Closed CAP Items worksheet contains similar basic system information as the top of Worksheet 1, CAP Template. The remainder of the document should contain the CAP items that are completed. The details will reflect almost all of the information provided in the CAP Template worksheet; however, Column O, Status Date, needs to be updated to the date of completion.

To "close" a CAP item, update the date in Column M, Status Date and move the CAP item to Worksheet 2, Closed CAP items.

A CAP item can be moved to the Closed CAP Items when either of the following occurs:

- All corrective actions have been applied and evidence of mitigation has been provided. Evidence of mitigation can be verified by a Security Liaison, a targeted vulnerability scan that covers the weakness domain, the following continuous monitoring scans, etc.
- A false positive request was submitted and approved by the Agency CIO or designee.