State of California

Department of Technology

Office of Information Security

Plan of Action and Milestones Instructions

SIMM 5305-B

January 2018

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	**August 2015**	**California Office of Information Security (CISO)**	**New**
Minor Update	**January 2018**	**Office of Information Security (OIS)**	**Office name change**

TABLE OF CONTENTS

Introduction

Each state entity is responsible for establishing an Information Security Program to effectively manage risk. The state entity's information security program shall incorporate an Information Security Program Plan (ISPP) to provide for the proper use and protection of its information assets, including a plan of action and milestones (POAM) process for addressing information security program deficiencies.

POAMs are submitted to the Department of Technology, California Information Security Office to create a statewide perspective and status of a state entity's efforts to achieve full compliance. POAMs are updated throughout program maturation through compliance self-reporting, and in response to risk assessments and audit findings, incidents, and oversight reviews. The standardized format will provide Agencies/state entities with a standardized tool and provide for consistency in reporting to Office of Information Security (OIS).

Procedure

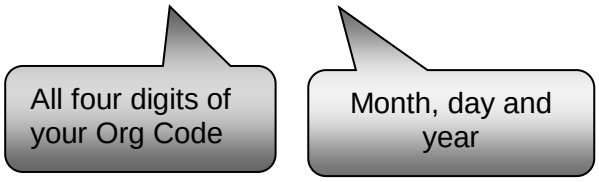
Procedures must be adhered to exactly as specified. The POAM tool is a Microsoft® Excel workbook with several supporting hidden worksheets. The tool was designed to input only the necessary information required to comply with SAM Section 5305.1 and support the OIS's mission. Agencies/state entities may utilize an internal document that captures a more elaborate POAM format; however, please transfer the requested data elements to the OIS's required form.

A working version of the POAM (SIMM 5305-C) is available on the Department of Technology's Office of Information Security website. The Agency/state entity must submit the POAM using the file name format described in step 18 below.

Step-by-Step:

1. Open the Excel workbook.
2. Column A: Do not modify.
3. Column B: Select from drop-down one of the NIST families within the drop down menu that best describes the security audit finding, compliance deficiency, security risk, incident remediation activity, or other gap (henceforth referred to as "risk").
4. Column C: Select from the drop-down one of the SAM sections or Sub-section. Your selection in Column C must align with your section in Column B.
5. Column D: Not available for data entry; internal use only.
6. Column E: Briefly describe the nature and characteristics of the risk.
7. Column F: Briefly describe any short or long-term compensating controls installed.
8. Column G: Select from drop-down the source activity (how the risk was initially identified). There is no "Other" selection as an option.

9. Column H: Briefly describe the information asset(s) that may be impacted by this risk. An information asset can be a system, a data element, a person, a facility, a record, a file, a piece of paper, hardware, software, etc. See the definition for this and other terms in SAM Section 5300.4.
10. Column I: Identify the person(s) responsible for this risk, including name, title and/or classification. By policy, the state entity head (director) is responsible for all risks, but for purposes of the POAM, please indicate who will "own" the risk and secure the necessary resources (persons or funding) to address the risk. This is the person the OIS will contact for more information and expect an informed response.
11. Column J: Briefly describe the high-level steps the Agency/state entity will take to address the risk, including short and longer-term plans. If necessary, a separate attachment may be submitted to the OIS.
12. Column K: Indicate when the risk was first identified. Enter date as MM/DD/YYYY format. Null is acceptable if no date can be identified.
13. Column L: Indicate the start date to address the risk. Enter date as MM/DD/YYYY format.
14. Column M: Indicate the projected completion date. Enter date as MM/DD/YYYY format. NOTE: OIS will know if it's a projected or actual completion date based on the status of the risk.
15. Column N: Select from one of the four (4) status types and use Column O to record the date for the status selected in Column N. NOTE: Once a risk is reported as "Completed" if must remain on the tool until the OIS has acknowledged its "Completed" status. Then, and only then, may it be removed from the tool.
16. Column P: Use the NIST risk categories described in Special Publication 800-30 to identify if the risk is a Very Low, Low, Moderate, High, or Very High value. Select from the drop-down one of the five (5) risk rating options.
17. Column Q: Briefly describe any constraints to remediating this risk. If necessary, a separate attachment may be submitted to the OIS.
18. Prior to sending your completed POAM to the OIS, rename the file using the following format: *ooooPOAMmmddyyyy.xlsx*. Replacing "oooo" with organization code, as identified in Uniform Codes Manual. Example: 0560POAM01312016.xlsx



Securely send the entire form and any attachments (see Steps 11 and 17) to the OIS using the Secure File Transfer (SFT) system. You will receive confirmation of receipt within 24 hours.

Level of Detail and Frequency

This SIMM is to be used to report remediation plan detail related to a security audit finding, compliance deficiency, security risk, incident remediation activity, or other gap.

As configured, the tool has sufficient rows to report 20 risks. Should the Agency/state entity have the need to report more than 20 risks, additional rows can be added (NOTE: unprotect the worksheet first). Wherever possible, aggregate related risks. For example, if an entity is out of compliance with a particular SAM policy requirement that is related to personal computers (PC) and the entity has several dozen PCs that are out of compliance, this risk is reported on only one row. If a state entity expects to report in excess of 40 risks, please contact the OIS for further discussions prior to reporting (security@state.ca.gov).

Unless otherwise directed, each state Agency/entity shall, at a minimum, provide quarterly updates on progress toward completion of the plans.