
State of California
Department of Technology
Office of Information Security

Plan of Action and Milestones Instructions

SIMM 5305-B

March 2019

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
Minor Update	March 2019	OIS	Instruction clarification; Added confidential statement

TABLE OF CONTENTS

INTRODUCTION	4
INSTRUCTIONS.....	4
LEVEL OF DETAIL AND FREQUENCY	6

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 California Department of Technology, Office of Information Security (OIS) 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 OIS. Per [State Administrative Manual \(SAM\) 5300.2](#), the updated POAM is due on the last business day of January, April, July, and October.

Instructions

Instructions 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.

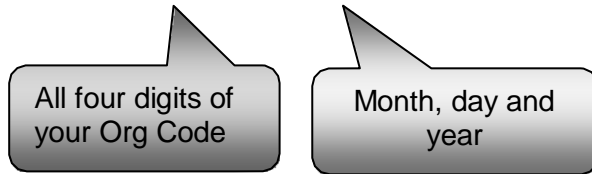
A working version of the POAM (SIMM 5305-C) is available on the Department of Technology's Office of Information Security website within the [Statewide Information Management Manual \(SIMM\) Forms](#) page. The Agency/state entity must submit the POAM using the file name format described in step 20 below.

Step-by-Step Instructions:

1. Open the Excel workbook.
2. **Row 3:** Enter the complete name of your state entity in box 3C, the organization code for your state entity in box 3F, and the Agency that your entity reports to in box 3H.
3. **Row 4:** Check the box that best describes the program deficiency status for your state entity.
4. **Row 7:** Provides a sample of how to properly complete the POAM.
5. **Column B:** Select 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").
6. **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.

7. **Column D:** Not available for data entry; internal use only.
8. **Column E:** Briefly describe the nature and characteristics of the risk.
9. **Column F:** Briefly describe any short or long-term compensating controls installed.
10. **Column G:** Select from drop-down the source activity (how the risk was initially identified). There is no "Other" selection as an option.
11. **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](#).
12. **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.
13. **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.
14. **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.
15. **Column L:** Indicate the start date to address the risk. Enter date as MM/DD/YYYY format.
16. **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.
17. **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" it must remain on the tool. At this time the row may be hidden, but never deleted.
18. **Column P:** Use the NIST risk categories described in [NIST 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.
19. **Column Q:** Briefly describe any constraints to remediating this risk. If necessary, a separate attachment may be submitted to the OIS.

20. **File Name:** 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**



Information contained in the POAM is confidential, securely send the entire form and any attachments (as referenced in Steps 13 and 19 above) to OIS using the Secure Automated File Exchange (SAFE) system. If you are in need of assistance obtaining a SAFE account for your state entity, please contact our office for assistance at security@state.ca.gov.

Level of Detail and Frequency

The POAM 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. 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 at security@state.ca.gov.

Unless otherwise directed, each state entity shall, at a minimum, provide quarterly updates on progress toward completion of the plans. Quarterly submissions are due on the last business day of the following months; January, April, July, and October. The quarterly due dates for all OIS compliance documents are outlined in the [Information Security Compliance Reporting Schedule \(SIMM 5330-C\)](#).