Standard DE.CM: Ongoing Assessment & Authorization

Approval Date:

2/10/2021

U.S. Department of Education (ED)

Office of the Chief Information Officer (OCIO)

Information Assurance Services (IAS)

Revision History

The table below identifies all changes that have been incorporated into this document.

Version	Draft Date	Summary of Changes
1.0	05/31/2019	Initial draft
1.1	4/10/2020	Reviewed for accuracy
1.2	4/17/20	Added new table for criteria
1.3	4/24/20	Added additional ISO responsibilities
1.4	5/4/2020	Added additional ISO responsibilities
1.5	5/21/2020	Incorporated OCIO stakeholder comments
1.6	5/21/2020	CISO Review
1.7	1/13/2021	Reviewed for accuracy and timeliness. Standardized Risk Acceptance/Policy exception verbiage. Update references in Appendix A.

APPROVAL

Steven Hernandez

Digitally signed by Steven Hernandez
Date: 2021.02.10 19:04:53 -05'00'

Steven Hernandez **Date**
Director, IAS/Chief Information Security Officer (CISO)

Table of Contents

Table of Contents

1. INTRODUCTION 1

1.1 Purpose 1

1.2 Scope 1

2. STANDARDS 2

2.1 Information System Continuous Monitoring (ISCM) 2

2.2 Ongoing Security Authorization 2

3. RISK ACCEPTANCE/POLICY EXCEPTIONS 4

APPENDIX A: RESOURCES AND REFERENCES 4

1. INTRODUCTION

1.1 Purpose

The Office of Management and Budget (OMB) Circular A-130, *Managing Information as a Strategic Resource*, addresses responsibilities for protecting federal information resources and for managing personally identifiable information (PII). It requires agencies to implement the Risk Management Framework (RMF) processes which are contained within the current version of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37. An important aspect of risk management is the ability to monitor and maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. Initial Authorization to Operate (ATO) is based on evidence available at a static point in time, but systems and environments of operation can change over time. Through Information System Continuous Monitoring (ISCM), new threat or vulnerability information is evaluated as it becomes available, permitting the Department to better perform risk response actions. The continuous monitoring of security and privacy control effectiveness facilitates Ongoing Security Authorization (OSA) after the initial authorization is granted. In September 2011, OMB memorandum M-11-33 approved the transition from a static every-three-year security authorization process to an ongoing authorization process via ISCM. The OSA program supports improved near real time risk reporting in accordance with updated NIST guidelines while serving to mature department cybersecurity culture, posture, and improving the overall cyber hygiene for Department information systems and data When a system is operating under ongoing authorization, the Authorizing Official (AO) continues to be responsible and accountable for explicitly understanding and accepting the risk of continued operations, use of the information system, or continuing to provide common controls for inheritance.

This document establishes the Department standards for implementing and maintaining an OSA program for common controls providers, cloud service providers, and FISMA reportable information systems across ED. This document aligns to and supports Department standard, *ID.RM Cyber Risk Management Framework*.

1.2 Scope

All Department FISMA reportable systems must be authorized for operation. The OSA policy within this standard pertains to all Common Control Providers (CCP) as well as all ED information systems and Cloud Service Providers (CSP) operated by, funded by or on behalf of ED, including contractor owned, grantee owned, and ED-owned information systems regardless of current lifecycle phase or location with the exception of FSA systems.

All employees, contract personnel (including grantees) consultants, licensees, and any person or entity providing, operating, maintaining, or supporting any common control provider, cloud service provider or information system that processes ED information are required to comply with this standard.

2. STANDARDS

2.1 Information System Continuous Monitoring (ISCM)

Mature ISCM capabilities support effective security assessment outcomes and OSA decisions. The continuous evaluation of the effectiveness of security and privacy control implementation; it is not separate from ISCM but in fact is a subset of ISCM activities. As such, Information System Owners (ISOs) and Information System Security Officers (ISSOs) are responsible for the continuous monitoring of the effectiveness of security controls employed within, offered by, or inherited by the system[1], and monitoring the impact of any proposed or actual changes to the system and its operational environment. ISOs and ISSOs make recommendations through continuous monitoring reporting to inform the AO of system risks for the purpose of making system authorization decisions. ISCM does not replace the security authorization requirement; rather, it supports the OSA decisions.

All Principal Offices and information systems, cloud service providers, and common controls providers are required to comply with the guidance specified in (1) the current version of NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*; 2) the current version of NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*.

2.2 Ongoing Security Authorization

OSA consists of operations and maintenance activities, security control assessments, and remediation actions at a frequency sufficient to support AO risk-based security decisions to adequately protect organization information. The goal of these activities is to ensure that control implementations documented in the system security plans in the initial security authorization process remain in place, operate effectively, and are updated when threats, vulnerabilities, or environmental changes cause controls to be ineffective.

2.2.1 Entrance Criteria

The conditions in Table 1 must be satisfied to enter into the Department's OSA program.

Criteria	Description
ATO Granted	• A Full Scope security assessment has been completed, the Initial Authorization granted, and the ATO date is at least 3 months in the past OR • A system with an existing ATO must have more than 18 months remaining on its current ATO.

Table 1: OSA Entrance Criteria

[1] CCP continuous monitoring outcomes and security posture communicated through the ED CSF Risk Scorecard.

2.2.2 Maintaining OSA Status

Systems that have been evaluated by the Office of the Chief Information Officer (OCIO) as having met the criteria in Section 2.2.1 and provide sufficient combined manual and automated system-level continuous monitoring in place and adhere to the control assessment schedules, delivery of control artifacts, and requirements detailed within the Department's Ongoing Security Authorization Guidance are required to enroll and operate under OSA. If a system fails to enroll within 90 days of meeting the criteria, the system's ATO will be re-evaluated for revocation in six (6) months. Eligible systems which are not enrolled within 90 days will also receive a POA&M to track the non-compliance with the Department Assessment & Authorization standard.

ISOs are required to manage the schedule of activities related to all system operations, including assessment and authorization actions. Under the delegation of the ISO, the ISSO ensures the appropriate system security documentation is in place and evaluates impacts of system modifications or architecture decisions. Systems authorized under OSA must be assessed based on predetermined frequency and selection of the technical, management, and operational security controls employed within and inherited by the information system. The selection of appropriate security controls to monitor and the frequency of monitoring are based on an OSA testing schedule developed by the ISSO or Common Control Provider and approved by the AO and CISO. The ISO must make appropriate resources available to support periodic security assessments as defined in the system OSA testing schedule. The ISO and ISSO must monitor all OSA, continuous monitoring, and assessment activities in accordance with related guidance and/or procedures.

The ISO, in coordination with the AO, must ensure that unacceptable security risks identified throughout the OSA assessments and continuous monitoring period are remediated in accordance with established Department frequencies and in consultation with Information Assurance Services (IAS). When security controls are identified as being ineffective, either before or during OSA must be remediated. Remediation is tracked by establishing Plan of Action and Milestones (POA&M) and re-testing remediation actions throughout the OSA process. This includes evaluating and updating the selection of security controls for the information system when events occur that indicate the baseline set of security controls is no longer accurate or adequate for protection of the information system. ISOs, with assistance from appropriate system technical support personnel, must also review controls selected for inheritance to ensure common and hybrid controls are accurately identified and selected.

2.2.3 OSA Exit Criteria

Systems which are impacted by the event triggers below or fail to maintain the required enrollment criteria may result in the system, cloud service provider, or common control provider being exited from the OSA program and ATO status revaluated for revocation unless remediation actions are completed prior to the next scheduled assessment conducted in accordance with the system's OSA assessment schedule. Systems impacted by the event triggers below may be removed from the program unless remediation actions are taken. In the event remediation does not occur, the AO will re-evaluate the ATO status and mandate the system undergo a full scope ATO within six months. However, the following event triggers may result in re-evaluating the status of a system's ATO and the potential issuance of a Denial of Authorization, per *ID.RM Cyber Risk Management Framework* if the AO has determined the risk to Department operations (including image & reputation) and assets, individuals, and other organization is at an unacceptable level after reviewing risk assessment results and authorization package and any additional inputs provided.

Event	Description
Past Due POA&Ms	Past Due POA&M risk factor score is less than a three (3) in the system level CSF Scorecard
CSF Risk Scorecard Overall Score	Overall Score < 2, which is below the established Department Risk Appetite as documented in standard *ID.RM Cyber Risk Management Framework*.
Secure Baseline Configuration (STIG) Compliance	Remediation of non-compliant secure baseline configuration findings not completed within two weeks of OSA entrance or OSA assessment remediation period.
Critical and High Vulnerabilities	All identified critical and high vulnerabilities have not been remediated within the Department's established timelines in accordance with OCIO-STND-01.
Significant System Change	If significant system changes occurs, including planned or unplanned major upgrades or system migration.
System information is inaccurate and/or outdated in CSAM	System is identified on the CSAM Data Discrepancies report for inaccuracies or missing infomation.

3. RISK ACCEPTANCE/POLICY EXCEPTIONS

Deviations from the Department policies, Instructions, Standards, Procedures or Memos must be approved and documented through the Department's Risk Acceptance process. Deviations that introduce additional risks to the enterprise must be submitted through the Department Risk Acceptance Form (RAF) and must be approved by the ED CISO (as delegated). Requests must justify the reason for the deviation(s)/exception(s) as well as the compensating security controls implemented to secure the device or information, if applicable. Policy deviations that do not introduce additional risks do not need to be submitted through the Department RAF but will need to be approved by the Department CISO (as delegated).

APPENDIX A: RESOURCES AND REFERENCES

- NIST Special Publication (SP) 800-137: *Information Security Continuous Monitoring (ISCM) for Federal Information*
- NIST Special Publication (SP) 800- 37 (as amended): *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*
- NIST Special Publication (SP) 800-137
- NIST Special Publication (SP) 800-53, (as amended): *Security and Privacy Controls for Federal Information Systems and Organizations*

- Federal Information Security Modernization Act of 2014 (FISMA 2014)
- NIST Privacy Framework: *A Tool for Improving Privacy through Enterprise Risk Management*, 2020