Level	Definition
1 Ad-hoc	**ISCM program is not formalized and ISCM activities are performed in a reactive manner resulting in an ad-hoc program that does not meet Level 2 requirements for a defined program consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • ISCM activities are performed without the establishment of comprehensive policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • ISCM stakeholders and their responsibilities have not been defined and communicated across the organization. • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • The organization lacks personnel with adequate skills and knowledge to effectively perform ISCM activities. • The organization has not identified and defined the qualitative and quantitative performance measures that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. • The organization has not identified and defined the ISCM technologies needed in one or more of the following automation areas and relies on manual/procedural methods in instances where automation would be more effective: patch management, license management, information management, software assurance, vulnerability management, event management, malware detection, asset management, configuration management, network management, and incident management. • ISCM activities are not integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. • There is no defined process for collecting and considering lessons learned to improve ISCM processes. • The organization has not defined how ISCM information will be shared with individuals with significant security responsibilities and used to make risk-based decisions.
2 Defined	**The organization has formalized its ISCM program through the development of comprehensive ISCM policies, procedures, and strategies consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. However, ISCM policies, procedures, and strategies are not consistently implemented organization-wide.** • ISCM activities are defined and formalized through the establishment of comprehensive ISCM policies, procedures, and strategies developed consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS. • ISCM stakeholders and their responsibilities have been defined and communicated across the organization, but stakeholders may not have adequate resources (people, processes, tools) to consistently implement ISCM activities. • ISCM results vary depending on who performs the activity, when it is performed, and the methods and tools used. • The organization has identified and defined the performance measures and requirements that will be used to assess the effectiveness of its ISCM program, achieve situational awareness, and control ongoing risk. However, these measures are not consistently collected, analyzed, and used across the organization. • The organization has identified and fully defined the ISCM technologies it plans to utilize in the ISCM automation areas. Automated tools are implemented to support some ISCM activities but the tools may not be interoperable. In addition, the organization continues to rely on manual/procedural methods in instances where automation would be more effective. • The organization has defined how ISCM activities will be integrated with respect to organizational risk tolerance, the threat environment, and business/mission requirements. However, the organization does not consistently integrate its ISCM and risk management activities. • The organization has defined its process for collecting and considering lessons learned to make improvements to its ISCM program. Lessons learned are captured but are not shared at an organizational level to make timely improvements. • ISCM information is not always shared with individuals with significant security responsibilities in a timely manner with which to make risk-based decisions.
3 Consistently Implemented	**In addition to the formalization and definition of its ISCM program (Level 2), the organization consistently implements its ISCM program across the agency. However, qualitative and quantitative measures and data on the effectiveness of the ISCM program across the organization are not captured and utilized to make risk-based decisions consistent with NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO ISCM CONOPS.** • The ISCM program is consistently implemented across the organization, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • ISCM stakeholders have adequate resources (people, processes, technologies) to effectively accomplish their duties. • The rigor, intensity, scope, and results of ISCM activities are comparable and predictable across the organization. • The organization has standardized and consistently implemented its defined technologies in all of the ISCM automation areas. ISCM tools are interoperable, to the extent practicable. • ISCM activities are fully integrated with organizational risk tolerance, the threat environment, and business/mission requirements. • The organization is consistently capturing and sharing lessons learned on the effectiveness of ISCM processes and activities. Lessons learned serve as a key input to making regular updates to ISCM processes. • ISCM information is shared with individuals with significant security responsibilities in a consistent and timely manner with which to make risk-based decisions and support ongoing system authorizations.
4 Managed and Measurable	**In addition to being consistently implemented (Level 3), ISCM activities are repeatable and metrics are used to measure and manage the implementation of the ISCM program, achieve situational awareness, control ongoing risk, and perform ongoing system authorizations.** • Qualitative and quantitative measures on the effectiveness of the ISCM program are collected across the organization and used to assess the ISCM program and make necessary changes. • Data supporting ISCM metrics is obtained accurately, consistently, and in a reproducible format, in accordance with the organization's ISCM policies, procedures, and strategies and NIST SP 800-53, SP 800-137, OMB M-14-03, and the CIO CONOPS. • ISCM data is analyzed consistently and collected and presented using standard calculations, comparisons, and presentations. • ISCM metrics are reported to organizational officials charged with correlating and analyzing the metrics in ways that are relevant for risk management activities, including situational awareness and risk response. • ISCM metrics provide persistent situational awareness to stakeholders across the organization, explain the environment from both a threat/vulnerability and risk/impact perspective, and cover mission areas of operations, the organization's infrastructure, and security domains. • ISCM is used to maintain ongoing authorizations of information systems and the environments in which those systems operate, including common controls and keep required system information and data (i.e., System Security Plan Risk Assessment Report, Security Assessment Report, and POA&M) up to date on an ongoing basis
5 Optimized	**In addition to being managed and measurable (Level 4), the organization's ISCM program is institutionalized, repeatable, self-regenerating, and updated in a near real-time basis based on changes in business/mission requirements and a changing threat and technology landscape.** • Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts its ISCM program to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. • The ISCM program is integrated with strategic planning, enterprise architecture, and capital planning and investment control processes. • The ISCM program achieves cost-effective IT security objectives and goals and influences decision making that is based on cost, risk, and mission impact.