ACT-IAC  
ATO-AS-CODE

Compliance Automation  
Process Maturity Model  
(CA PMM)

Version 1.0  
June 30, 2023

# **INTRODUCTION**

On June 10, 2021, the National Institute of Standards and Technology (NIST) released the first version of the Open Security Controls Assessment Language (OSCAL) framework. Since then, OSCAL has gained widespread attention from public and private security leaders. OSCAL provides a standard for capturing and sharing security data to support the compliance life cycle. Although early adopters use OSCAL for assessments, the OSCAL standard can profoundly transform an organization by giving them the ability to measure and automate against enterprise initiatives such as CDM, ZTA, and C-ATO. Consequently, The ACT-IAC ATO-AS-CODE initiative created the following process maturity model to assist organizations in adopting and scaling OSCAL. This maturity model requires market advancement of security tools and capabilities.

# **PROCESS MATURITY MODEL**

A process maturity model defines a methodical framework for measuring the effectiveness of an organization’s process, such as cyber operations. Additionally, an organization’s process can be continuously improved through applying a disciplined methodology, leveraging global standards, and adopting emerging technologies. We’re using OSCAL to power more automation.

The Compliance Automation Process Maturity Model (CA PMM) is intended to define a basic model to help organizations safely and rapidly adopt and scale OSCAL. The CA PMM does not prescribe a specific approach to build a fast, high-performing, and security-focused organization, but instead defines the basic principles to measure an organization’s process towards that goal. The CA PPM identifies 5 levels of maturity as defined in the sections below.

## **LEVEL 1: AD HOC**

Level 1 defines the most basic level where processes are ad hoc, manual, and labor-intensive. In this level, the workforce applies a high degree of manual labor to perform their cybersecurity functions. Also, the workforce may not have a Governance, Risk and Compliance (GRC) tool, or rely on custom GRC platforms, to house security artifacts rather than manage the entire cybersecurity experience. Furthermore, delayed insights about cybersecurity risks hamper decision-making.

|  |  |  |
| --- | --- | --- |
| **#** | **METRICS** | **DESCRIPTION** |
| **1** | Manual creation, editing, & verification of security documents | Organization has a developed enterprise control catalog and creates the System Security Plan (SSP), Security Assessment Plan (SAP), and System Assessment Report (SAR) manually. The process of verifying changes to the documents are also conducted manually. |
| **2** | Artifacts are collected in a decentralized manner | Artifacts are collected, edited, and stored in various repositories, tools, or locally. |
| **3** | Plans of Actions & Milestones (POA&Ms) are recorded and tracked manually | POAMs are managed in documents such as a spreadsheet or in a tool that cannot be converted to OSCAL. POAMs are not correlated at the enterprise level. |
| **4** | Wet signatures, manual routing | Authorization documents are routed manually and/or signed with wet signature. |
| **5** | Reporting is conducted manually | Reports and analytics are generated by teams of people who manually consolidate data sources to provide reports into compliance and risk. |

**LEVEL 2: IMPLEMENTED**

Level 2 defines the most basic application of the OSCAL framework. In this level, organizations digitize the System Security Plan (SSP), Security Assessment Plan (SAP), Security Assessment Report (SAR) and supporting artifacts in the OSCAL standard format. Additionally, organizations, in this level, rely on commercial GRC platforms that are capable of using OSCAL input and output to digitize and accelerate the security assessment and authorization process, rather than just a repository for security artifacts. Furthermore, organizations leverage OSCAL to automate compliance checks of the security package. However, integration does not yet exist.

|  |  |  |
| --- | --- | --- |
| **#** | **METRICS** | **DESCRIPTION** |
| **1** | Use OSCAL to digitize the SSP, SAP, and SAR which includes the Organization Baseline and Overlays | Organization stores data in an information system that can ingest the SSP, SAP, and SAR, and export these documents, in OSCAL. Approved leveraged / inherited assets e.g. (Policies, cloud products, other FISMA Systems, etc.) documentation is in OSCAL format. |
| **2** | All artifacts and outputs are stored in OSCAL format | Artifacts (anything that is system-generated that proves the security compliance of a system) are stored in a digital format and in a manner where they can be easily retrieved by an organization / structurally retrieved, taking into account multiple storage methods (E.g., S3 storage, DB, log aggregator). The organization is now accepting digitized versions as part of their OSCAL assessments. |
| **3** | Automated POAM Generation | POAMs are automatically generated based on finding / vulnerability age, and notification of reminders are provided to track and remediate POAMs. |
| **4** | Automated routing of approval & digital signatures | Packages are automatically routed, and digital signatures are applied. Reduce overall approval processing time due to automated routing and convenience of digital signature capability. |
| **5** | Automated reporting and analytics | Reports are generated automatically and enable the organization to trend metrics (e.g., findings, remediation, and risk over time. These metrics are further used to identify aggregated metrics like throughput of findings and remediation coverage.) |
| **6** | Ongoing Authorization with Some Manual Attestation | Systems are mature and undergo check-ins and due diligence on a scheduled basis and are still subject to periodic manual reassessment. |

**LEVEL 3: INTEGRATED**

Level 3 defines the level where the organizational processes are interconnected with external and internal processes. For example, the organization’s security assessment and authorization processes are interconnected with the FedRAMP process. Additionally, control compliance, overlays, and inheritance are seamlessly shared between the organization and governing bodies. Organizations in this level often rely on OSCAL to not only automate security artifact generation, but also transmit security events from CDM platforms. Here, you begin to integrate security management activity that will flow into the compliance process (e.g., patch management, asset tracking and reporting, etc.). These are interconnected and insights from these platforms are displayed in centralized dashboards. Organizations establish Open APIs to interconnect systems and enterprise Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS) to centralize the management of key technologies.

|  |  |  |
| --- | --- | --- |
| **#** | **METRICS** | **DESCRIPTION** |
| **1** | Organization Provides Enterprise Capabilities & Software in Preapproved Format with Leveraged Controls the Software Provides | All templates are in OSCAL format, and the organization can pull information into that template. Implementation statements for enterprise common control catalog are pre-populated in these templates. All inherited assets and artifacts are collected in a OSCAL format and can be leveraged to identify asset-level and leveraged-risk. For example, policies, FedRAMP products, etc. |
| **2** | Security Compliance Baseline Information is Integrated into the Compliance Process | System security posture, compliance scans, and other important information that is used to manage the system life cycle is automatically collected, tagged, and integrated into the compliance process and activities. |
| **3** | Compliance information is automatically published to relying parties | Organization has integration with relying parties to provide compliance information in an automated way, such as DHS, CISA, industry partners, etc. |
| **4** | Alert-Based Ongoing Authorization | Systems are mature based on established enterprise criteria (e.g., integration with CDM) and undergo check-ins and due diligence based on automatically generated alerts. OSCAL-formatted data provides a near real-time assessment of risk posture which is provided in a dashboard view to track and prioritize activities. |

**LEVEL 4: MEASURED**

Level 4 defines the level where cybersecurity risk, budget, and mission alignment are measured, quantified, and embedded into executive decision-making. Here, the business organization, technology organization, and cyber operations are aligned and working in tandem to properly manage risk without impeding the mission. Organizations in this level rely on an enterprise risk framework that strategically embeds cybersecurity into the organization’s scorecard. Enterprise governance is established to manage the business-technology-security alignment. Enterprise management platforms for planning, budget, and acquisitions are more integrated with cybersecurity platforms by using OSCAL.

|  |  |  |
| --- | --- | --- |
| **#** | **METRICS** | **DESCRIPTION** |
| **1** | Integration with the Business and Acquisition Tools | The business, acquisition, budget, cyber, and IT are integrated. POAMs tie in the cost to remediate. |
| **2** | Performance Benchmarking Across Teams & Organizations | Performance is compared across teams to benchmark cybersecurity performance across teams and organizations. Success metrics are collected to track success of the OSCAL program. |
| **3** | Assess risk across all Infrastructure Types | SBOM, Cloud, and Container information is integrated with overall risk to address risk down to the container level. OSCAL tags are applied to data to integrate this data into overall compliance. |
| **4** | Live Dashboards with Risk Information | Reports include business-level risk, in addition to system-level risk, which are updated in real time. |

**LEVEL 5: AUTOMATED AND OPTIMIZED**

Level 5 defines the highest level in the process maturity model where the organizational processes are continuously digitized, integrated, measured, and automated all using OSCAL. Additionally, organizations in this level can use extreme automation to learn, adapt, and optimize business processes. They also leverage a degree of intelligent automation like artificial intelligence to predict risk and protect the organization. This level requires the greatest degree of organizational change. The workforce and culture must appreciate and embrace data to power not only cyber security strategy, but also its operation.

|  |  |  |
| --- | --- | --- |
| **#** | **METRICS** | **DESCRIPTION** |
| **1** | Continuous ATO (C-ATO) | The data arising from changes in your FISMA boundary drives and informs the decision making. Recommendations, stage gates, etc. before going to production to make a risk decision. Auto-approval is possible based on the identified risk and findings. |
| **2** | Intelligently Predict System Risk | The organization is able to predict risk based on past and present data by using AI. |
| **3** | Identify Risk Based on Collective Intelligence Across all Systems | Generate an SSP with the exact posture of that system and calculate the risk based on the aggregation of all of those results. Intelligence is consolidated across all systems and leveraged to detect risk with other systems. |
| **4** | Automated Data Call Responses | Since all data is consolidated in a central repository, data calls can be responded to by selecting the requirements of the requestor. Based on a change in the system reflected in the data, you raise a risk that becomes something you have to address. Leverage information on system behavior. |
| **5** | Policy as Code | Automatically update requirements based on the changes in policy. Automate zero trust checks for system changes. |