STREAMLINING CMMC COMPLIANCE DELIVERABLES WITH OSCAL
KENNY SCOTT, CO-FOUNDER & CEO
Paramify slashes months, even years, of manual effort to hours, for a fraction of the cost. Thank you OSCAL!
KENNY SCOTT

Paramify Co-Founder & CEO

17+ years: Cyber Security & Risk Strategy

Adobe Common Controls Framework Pioneer

https://paramify.com
@kenny-g-scott
@kenny_g_scott

@Paramify
@kenny_g_scott

kenny@paramify.com
Multiple Requirements (Thousands)

SOC2, ISO 27001, HIPAA, FedRAMP, GDPR, Hi-TRUST ...

Distilled Requirements (< 300)

Adobe Common Controls Framework
MY REALIZATION
MY HYPOTHESIS
THE SOLUTION
Our initial prototype streamlined FedRAMP Moderate SSPs for complex packages, proving effective across multiple cases.
Scaling for SOC 2, ISO 27001, FedRAMP High, IL5, and CMMC became challenging, as constant refactoring led to issues.
We faced varying compliance catalogs, diverse report formats, and frequent updates, we realized the need for a universal standard.
OSCAL enabled mapping of security best practices to diverse control catalogs, thus allowing flexible, streamlined compliance reporting.
STANDARDIZATION WITH OSCAL

Requirements
Catalogs & Profiles

Implementation
System Security Plans & Components

Assessment
Assessment Plans, Results & Plan of Action & Milestones

pages.nist.gov/OSCAL

© 2023 Paramify, Inc. All Rights Reserved. Confidential.
# REQUIREMENTS

## CATALOGS & PROFILES

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>METADATA</strong></td>
<td>File title, version, date, defines roles, parties, locations.</td>
</tr>
<tr>
<td><strong>PARAMETERS</strong></td>
<td>Parameters shared by multiple controls defined here.</td>
</tr>
<tr>
<td><strong>CONTROL</strong></td>
<td>Specific parameters, objectives, methods, references.</td>
</tr>
<tr>
<td><strong>GROUP</strong></td>
<td>Group-related controls and parameters defined together.</td>
</tr>
<tr>
<td><strong>BACKMATTER</strong></td>
<td>Identical syntax for attachments, citations, graphics.</td>
</tr>
</tbody>
</table>

© 2023 Paramify, Inc. All Rights Reserved.
REQUIREMENTS

CATALOG
- METADATA
- PARAMETERS
- CONTROL
- GROUP
- BACKMATTER

PROFILE
- METADATA
- PARAMETERS
- CONTROL
- GROUP
- BACKMATTER

CONTROL BASELINE

MODIFY & MERGE

IMPORT

PROFILE
- METADATA
- PARAMETERS
- CONTROL
- GROUP
- BACKMATTER

IMPORT

MODIFY & MERGE

© 2023 Paramify, Inc. All Rights Reserved..
Organizing CMMC Catalogs and Profiles
"catalog": {
"uuid": "b954d3b7-d2c7-453b-8eb2-459e8d3b8462",
"metadata": {
"title": "NIST 800-171 Rev. 2 - Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations",
"last-modified": "2021-06-08T13:57:28.91745-04:00",
"version": "2015-01-22",
"oscal-version": "1.0.0"
},
"groups": [ {
"id": "ac",
"class": "family",
"title": "Access Control",
"controls": [ {
"id": "3.1.1",
"class": "SP800-171",
"title": "Authorized Access Control",
"props": [ {
"name": "label",
"value": "3.1.1"
}, {
"name": "sort-id",
"value": "3.01.01"
} ]
} ]
} ]
}
"id": "3.1.3e",
"class": "SP800-172",
"title": "Secured Information Transfer",
"params": [
  {
    "id": "3.1.3e_odp",
    "props": [
      {
        "name": "alt-identifier",
        "value": "3.1.3e_prm_1"
      }
    ],
    "label": "Secure information transfer solutions",
    "guidelines": [
      {
        "prose": "The organization implementing this requirement must decide on the secure information transfer sc"
      }
    ]
  }
]
Profiles: L1, L2 & L3
Paramify CMMC
CMMC Project (Rev 2)  Level 2

Project Progress

25%

Control Implementation Status

Total 320

Progress Breakdown

Data: 2 of 2

Key Contacts: 6 of 6

Implementation Breakdown

Access Control: 0 of 70
0%

Awareness and Training: 0 of 9
0%
Do I still have to do everything?
STANDARDIZATION WITH OSCAL

Requirements
Catalogs & Profiles

Implementation
System Security Plans & Components

Assessment
Assessment Plans, Results & Plan of Action & Milestones

pages.nist.gov/OSCAL
# Component Definition

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Metadata</td>
<td>File title, version, date, defines roles, parties, locations.</td>
</tr>
<tr>
<td>Import</td>
<td>References component definition from external resource.</td>
</tr>
<tr>
<td>Component</td>
<td>Describes a component within an implemented system.</td>
</tr>
<tr>
<td>Capability</td>
<td>Groups multiple components or capabilities as one.</td>
</tr>
<tr>
<td>Backmatter</td>
<td>Identical syntax for attachments, citations, graphics.</td>
</tr>
</tbody>
</table>
## IMPLEMENTATION

### SYSTEM SECURITY PLAN

<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>METADATA</td>
<td>File title, version, date, defines roles, parties, locations.</td>
</tr>
<tr>
<td>IMPORT PROFILE</td>
<td>Defines system's control baseline as OSCAL profile.</td>
</tr>
<tr>
<td>CHARACTERISTICS</td>
<td>Defines attributes like name, description, models, &amp; info.</td>
</tr>
<tr>
<td>IMPLEMENTATION</td>
<td>Defines info like roles, connections, services, &amp; inventory.</td>
</tr>
<tr>
<td>CONTROL</td>
<td>Describes how each baseline control is implemented.</td>
</tr>
<tr>
<td>BACK MATTER</td>
<td>Identical syntax for attachments, citations, graphics.</td>
</tr>
</tbody>
</table>
Paramify’s Risk Solution Platform
Risk Solutions are the capability inventory of your security program, becoming more robust with time and usage. As your organization grows, your solutions adapt, providing your organization with a tailored security framework for your specific needs, helping you maximize agility.
Components

Components are technical & non-technical tools used to achieve an outcome.

- Agreements (5): Agreements between two or more parties.
- Customer Managed (1): Provided by or configured by the customer.
- IaaS (10): Infrastructure as a Service (IaaS).
- Interconnections (9): Authorized FedRAMP boundary interconnections.
- Plans (10): Official plans for organizational programs.
- Policies (1): What partner must comply with.
- Procedures (1): Step-by-step of how a process is implemented.
- Processes (31): Combines technical and/or non-technical components.
- SaaS (33): Software as a Service (SaaS).
- Services (9): Supports transmission of data over.
# COMPONENT DEFINITION

<table>
<thead>
<tr>
<th>METADATA</th>
<th>File title, version, date, defines roles, parties, locations.</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMPORT</td>
<td>References component definition from external resource.</td>
</tr>
<tr>
<td>COMPONENT</td>
<td>Describes a component within an implemented system.</td>
</tr>
<tr>
<td>CAPABILITY</td>
<td>Groups multiple components or capabilities as one.</td>
</tr>
<tr>
<td>BACKMATTER</td>
<td>Identical syntax for attachments, citations, graphics.</td>
</tr>
</tbody>
</table>
## IMPLEMENTATION

<table>
<thead>
<tr>
<th>COMPONENT DEFINITION</th>
</tr>
</thead>
<tbody>
<tr>
<td>METADATA</td>
</tr>
<tr>
<td>IMPORT</td>
</tr>
<tr>
<td>COMPONENT</td>
</tr>
<tr>
<td>CAPABILITY</td>
</tr>
<tr>
<td>BACKMATTER</td>
</tr>
</tbody>
</table>
3.1.1 Part b

Control Requirement

Processes acting on behalf of authorized users are identified:

Solution Implementation

Service Account Permissions: Amazon Identity

Paramify, Inc. uses IAM, a CMMC-compliant identity and access management tool.

Identity Team

Paramify service account objects are assigned to the Change Management Process.

Activity
STANDARDIZATION WITH OSCAL

Requirements
Catalogs & Profiles

Implementation
System Security Plans & Components

Assessment
Assessment Plans, Results & Plan of Action & Milestones

pages.nist.gov/OSCAL
OSCAL unlocks complete and accurate deliverables with unrivaled speed and ease.
THANK YOU

We'll see you next time!

https://paramify.com
@kenny-g-scott
@kenny_g_scott

@Paramify
@kenny_g_scott
kenny@paramify.com