## Machine-readable format for EUCS (Proof of Concept)

In order to enable the usage of automation in compliance assessment policies as envisioned by the EUCS, we saw the need of leveraging standardized machine-readable languages able to represent the different elements of this certification scheme (e.g., controls, requirements, assessments, etc.). To the best of our knowledge, NIST OSCAL[[1]](#footnote-1) is probably the most mature candidate in this specific field. The rest of this section further elaborates on the initial POC we developed to represent the EUCS catalogue of requirements in OSCAL format.

This part of the ENISA POC was developed with the JSON scheme of OSCAL, although other available possibilities to develop the OSCAL scheme were XML and yaml. Our choice of JSON purely obeyed the expertise of the available team.

The EUCS requirements are modelled as a hierarchy comprising the following eight levels:

1. Domain
2. Category
3. Objective
4. Control ID
5. Control
6. Control Objective
7. Requirement ID
8. Requirement

The OSCAL scheme is implemented within a catalog element, which contains an UUID and other applicable metadata.

{  
 "catalog": {  
 "uuid":"93a38765-4930-451a-9b74-9dba729bea84",  
 "metadata":{  
 "title":"OSCAL TEST",  
 "last-modified":"2021-06-10T08:18:37.432+02:00",  
 "version":"FPD",  
 "oscal-version":"1.0.0"  
 },

In the next step the Domain and Category is created with the attribute “title”. With usage of “parts” and “prose” the Objective can be added into OSCAL.

"groups": [  
 {  
 "id":"a7",  
 "title":"A7 Operational Security",

"parts":[  
 {  
 "name":"objective",  
 "prose": "Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity, protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures"

}  
 ],

The Control is specified with “title” and Control ID with “id” and “properties”.

"controls": [  
 {  
 "id":"ops-02",  
 "title": "CAPACITY MANAGEMENT - MONITORING",

"properties":[  
 {  
 "name":"label",  
 "value":"OPS-02"  
 }  
 ],

To complete the Control, the Control Objective must been added within “parts” and is displayed in “prose”. Requirements and Control IDs are implemented with “parts” within the upper “parts” of Control. Requirement ID is specified with “properties” and the requirement itself with “prose”.

"parts": [  
 {  
 "id":"ops\_02\_obj",  
 "name":"control-objective",  
 "prose": "The capacities of critical resources such as personnel and IT resources are monitored."  
 },  
 {  
 "id":"ops-02\_smt",  
 "name":"statement",  
 "parts": [  
 {  
 "id":"ops-02\_smt.3",  
 "name":"item",  
 "properties": [  
 {  
 "name":"label",  
 "value":"OPS-02.3"  
 }  
 ],  
 "prose": "The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee fulfilment of OPS-02.1"

}  
 ]  
 }  
 ]  
 },

The proposed mapping from EUCS to OSCAL is shown in the following table:

Table 5. Proposed EUCS to OSCAL mapping

| **OSCAL** | **EUCS** | **Examples** |
| --- | --- | --- |
| Groups/ID | Domain | A7 |
| Groups/title | Category | A7 Operational Security |
| Groups/parts/prose(objective) | Objective | Ensure proper and regular operation, including appropriate measures for planning and monitoring capacity,  protection against malware, logging and monitoring events, and dealing with vulnerabilities, malfunctions and failures |
| Groups/Controls/properties/value(label) | Control ID | OPS-02 |
| Groups/Controls/title | Control | CAPACITY MANAGEMENT - MONITORING |
| Groups/Controls/parts/prose/(control-objective) | Control Objective | The capacities of critical resources such as personnel and IT resources are monitored. |
| Groups/Controls/parts/parts/properties/value(label) | Requirement ID | OPS-02.3 |
| Groups/Controls/parts/parts/prose(item) | Requirement | The provisioning and de-provisioning of cloud services shall be automatically monitored to guarantee  fulfilment of OPS-02.1 |

The resulting OSCAL representation of the EUCS requirements will be made available on the MEDINA code repositories during the execution of the project.

1. Please refer to https://pages.nist.gov/OSCAL/ [↑](#footnote-ref-1)