Appendices A - Q

Appendicies Overview

Most attachments required by FedRAMP are called out in the NIST SP 800-53 controls appearning in FedRAMP baselines.

Where a legacy FedRAMP attachment is handled as machine-readable content, you have the option of attaching the legacy attachment or representing the content as machine-readable content.

See the Document Attachments section for general attachment patterns as OSCAL `resources`.

The following table describes how each attachment is handled:

Appendix Name	Machine Readable	How to Handle in OSCAL
Appendix A: FedRAMP Security Controls	**Yes**	See the FedRAMP Security Controls section.
Appendix B: Related Acronyms	No	Attach using the `back-matter`, `resource` syntax. For Acronyms, resource must include a `prop` with `@ns="http://fedramp.gov/ns/oscal"`, `@name="type"`, and `@value="fedramp-acronyms"`.
Appendix C: Security Policies and Procedures	No	From each `-1` control (i.e. AC-1, IA-1) use `links` to identify the related policy and procedure attachments.
Appendix D: User Guide	No	From SA-5 (`id`=`sa-5`) use `links` to identify this attachment.
Appendix E: Digital Identity Worksheet	**Yes**	See the Digital Identity Determination section.
Appendix F: Rules of Behavior	No	From PL-4 (`id`=`pl-4`) use `links` to identify this attachment.
Appendix G: Information System Contingency Plan (ISCP)	No	From CP-2 (`id`=`cp-2`) use `links` to identify this attachment.
Appendix H: Configuration Management Plan (CMP)	No	From CM-9 (`id`=`cm-9`) use `links` to identify this attachment.
Appendix I: Incident Response Plan (IRP)	No	From IR-8 (`id`=`ir-8`) use `links` to identify this attachment.

Appendix Name	Machine Readable	How to Handle in OSCAL
Appendix J: CIS and CRM Workbook	Yes	This is generated from the content in the Security Controls section and does not need to be maintained separately nor attached.
Appendix K: FIPS 199 Worksheet	**Yes**	See the Appendix K: FIPS-199 Worksheet section.
Appendix L: CSO-Specific Required Laws and Regulations	No	Attach using the `back-matter`, `resource` syntax. For CSO-Specific Required Laws and Regulations, resource must include a `prop` with `@name="type"` and `@value="law"`.
Appendix M: Integrated Inventory Workbook	**Yes**	See the Inventory Approaches section.
Appendix N: Continuous Monitoring Plan	No	From CA-7 (`id`=`ca-7`) use `links` to identify this attachment.
Appendix O: POA&M	**Yes**	From CA-5 (`id`=`ca-5`) use `links` to identify this attachment.
Appendix P: Supply Chain Risk Management Plan (SCRMP)	No	From SR-2 (`id`=`sr-2`) use `links` to identify this attachment.
Appendix Q: Cryptographic Module Table	**Yes**	See the Appendix Q: Cryptographic Modules section.

Appendix A: FedRAMP Security Controls

See the FedRAMP Security Controls chapter.

Appendix B: Related Acronyms

There is no OSCAL construct for representing an acronyms list.

Attach a document (e.g., Word, Excel, PDF) with acronyms using a `back-matter`, `resources` entry.

See Attachments for details.

Appendix C: Security Policies and Procedures

See Control Response: Policies and Procedures.

Appendix D: User Guide

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The SA-5 (`id`=`sa-5` control should have `links` entries to the user guide

This is not normalized and is only for legacy conversion MVP

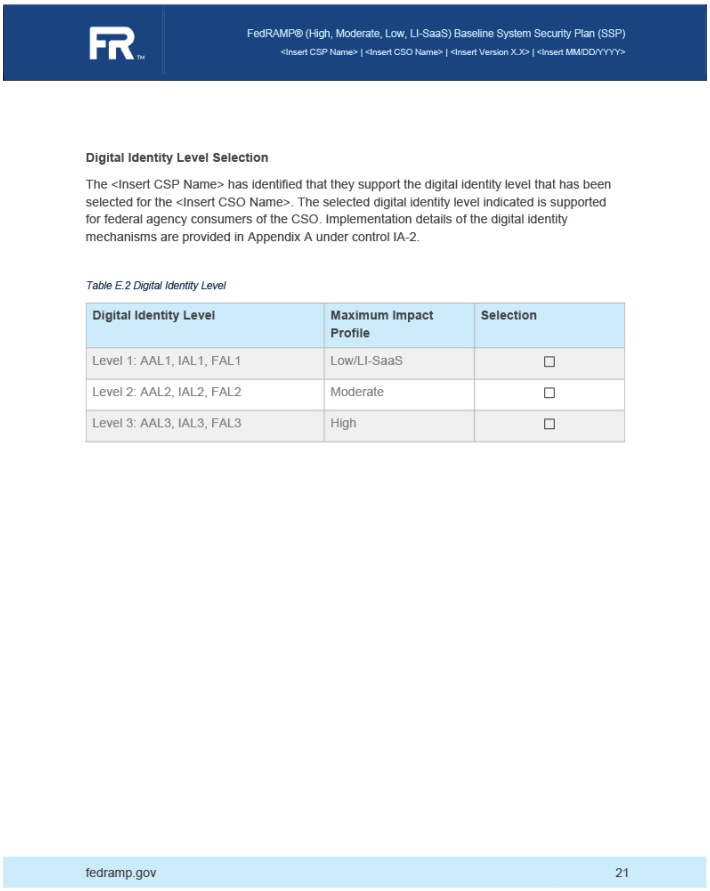
Normalized Key points include:

- attach the user guide as a back-matter/`resources` entry
- create a component for the user guide
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The SA-5 control has `by-components` entrys that cite the user guide component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix E: Digital Identity Level (DIL) Determination

The Digital Identity Level (DIL) is represented on the page below.



FedRAMP® (High, Moderate, Low, LI-SaaS) Baseline System Security Plan (SSP)

<Insert CSP Name> | <Insert CSO Name> | <Insert Version X.X> | <Insert MM/DD/YYYY>

Digital Identity Level Selection

The <Insert CSP Name> has identified that they support the digital identity level that has been selected for the <Insert CSO Name>. The selected digital identity level indicated is supported for federal agency consumers of the CSO. Implementation details of the digital identity mechanisms are provided in Appendix A under control IA-2.

Table E.2 Digital Identity Level

Digital Identity Level	Maximum Impact Profile	Selection
Level 1: AAL1, IAL1, FAL1	Low/LI-SaaS	☐
Level 2: AAL2, IAL2, FAL2	Moderate	☐
Level 3: AAL3, IAL3, FAL3	High	☐

fedramp.gov 21

Within `system-characteristics` there must be three entries to the `props` array as follows:

- `name` set to `identity-assurance-level` and a `value` set to `1`, `2` or `3`.
- `name` set to `authenticator-assurance-level` and a `value` set to `1`, `2` or `3`.
- `name` set to `federation-assurance-level` and a `value` set to `1`, `2` or `3`.
- The value of all three should match each other and align with the FIPS-199 impact level of the system.

OSCAL Representation

```
system-security-plan:
  system-characteristics:
    props:
    - name: identity-assurance-level
      value: '2'
    - name: authenticator-assurance-level
```

```
    value: '2'
  - name: federation-assurance-level
    value: '2'
```

OSCAL Allowed Values

Valid IAL, AAL, and FAL values (as defined by NIST SP 800-63):

- 1
- 2
- 3

Appendix F: Rules of Behavior (RoB)

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The PL-4 (`id`=`pl-4` control should have `links` entries to the RoB

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the RoB as a back-matter/`resources` entry
- create a component for the RoB
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The PL-4 control has `by-components` entrys that cite the RoB component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix G: Information System Contingency Plan (ISCP)

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The CP-2 (`id`=`cp-2` control should have `links` entries to the RoB

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the ISCP as a back-matter/`resources` entry
- create a component for the ISCP
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The CP-2 control has `by-components` entrys that cite the ISCP component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix H: Configuration Management Plan (CMP)

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The CM-9 (`id`=`cm-9` control should have `links` entries to the RoB

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the CMP as a back-matter/`resources` entry
- create a component for the CMP
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The CM-9 control has `by-components` entrys that cite the CMP component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix I: Incident Response Plan (IRP)

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The IR-8 (`id`=`ir-8` control should have `links` entries to the RoB

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the IRP as a back-matter/`resources` entry
- create a component for the IRP
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The IR-8 control has `by-components` entrys that cite the IRP component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix J: CIS and CRM Workbook

The FedRAMP Control Information Summary (CIS) and Customer Responsibility Matrix (CRM) are derived directly from the OSCAL control responses.

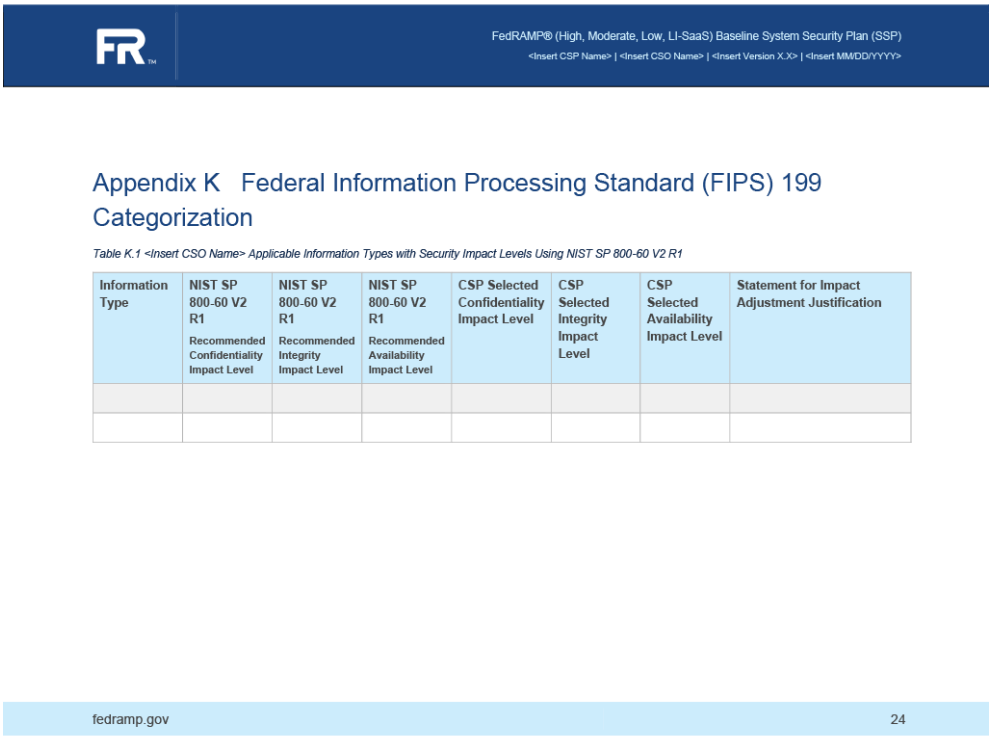
There is no need to maintain a separate CIS/CRM artifact; however, this information must be properly represented in the control responses. Tools can then summarize control information into the CIS and produce a list of customer responsibilities consistent with the CRM.

Needs Work

- It needs an App J page image
- It needs to reference and link to the customer respopnsibility topic in controls

Appendix K: FIPS-199 Worksheet

The system's overall FIPS-199 impact level is determined primarily by the sensitivity of the information it processes.



The overall FIPS-199 impact level is represented under `system-characteristics`:

- `security-sensitivity-level`
  - The value must be one of `fips-199-low`, `fips-199-moderate` or `fips-199-high`

The FIPS-199 Categorization worksheet is an inventory of information types in the system, based on NIST SP 800-60 Volume 2.

- Create one entry under `information-types` for each information type.
- For each information type:
  - Assign a `uuid`
  - Assign the NIST SP 800-63 information type name to the `title`
  - `description` is a required OSCAL field that is not acknowledged by FedRAMP. Consider offering context or citing 800-60.
  - The `categorizations` array should have one entry that includes:
    - `system` set to "http://doi.org/10.6028/NIST.SP.800-60v2r1"
    - the `information-type-ids` arraqy should have one entry
      - Use the NIST SP 800-60 invormation type ID
      - Exactly match the case as it appears in 800-60. (e.g., `C.2.3.1` or `D.15.5`)
  - The `confidentiality-impact` must have:

    - a `base` field with the value defined in 800-60.
    - a `selected` field with the value selected by the CSP.
    - If the value in `selected` does not match the value in `base`, use `adjustment-justification` to capture the "Statement for Impact Adjustment Justification"
    - `base` and `selected` values must be one of `fips-199-low`, `fips-199-moderate` or `fips-199-high`
  - `integrity-impact and` availability-impact`are treated the same as` confidentiality-impact` above.

Other information types or categorizations may be present if the SSP also represents compliance with other frameworks; however, the US Government must operate under NIST RMF and will only recognize the NIST SP 800-60 types.

OSCAL Representation

```
system-security-plan:
  system-characteristics:

    security-sensitivity-level: fips-199-high

    system-information:
      information-types:
        - uuid: 11111111-2222-4000-8000-006000000001
          title: Information Type Name
          description: A description of the information.
          categorizations:
          - system: http://doi.org/10.6028/NIST.SP.800-60v2r1
            information-type-ids:
            - C.2.4.1
          confidentiality-impact:
            base: fips-199-moderate
            selected: fips-199-moderate
            adjustment-justification: Required if the base and selected values do not
              match.
          integrity-impact:
            base: fips-199-moderate
            selected: fips-199-low
            adjustment-justification: Required if the base and selected values do not
              match.
          availability-impact:
            base: fips-199-moderate
```

```
        selected: fips-199-moderate
        adjustment-justification: Required if the base and selected values do not
          match.
```

OSCAL Allowed Values

Reqired value for `system`:

- `http://doi.org/10.6028/NIST.SP.800-60v2r1`

Valid values for `security-sensitivity-level`, `base` and `selected` fields:

- `fips-199-low`
- `fips-199-moderate`
- `fips-199-high`

Appendix L: CSO-Specific Required Laws and Regulations

Needs Work

- Content cleanup
- YAML Example

For MVP:

- attach a Word or PDF document enumerating the applicable laws and regulations.

For Normalized:

- Provide one back-matter/`resources` entry per applicable law or regulation that includes:
  - a `title` with the title of the law or regulation
  - a `props` entry with:
    - `name` = `type`
    - `value` = `law`
    - `rlinks` entry that links to the law or regulation

Appendix M: Integrated Inventory Workbook

See Inventory Approaches for guidance.

Appendix N: Continuous Monitoring Plan

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The CA-7 (`id`=`ca-7` control should have `links` entries to the RoB

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the Continuous Monitoring Plan as a back-matter/`resources` entry
- create a component for the Continuous Monitoring Plan
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The CA-7 control has `by-components` entrys that cite the Continuous Monitoring Plan component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix O: POA&M

See the FedRAMP POA&M book.

Appendix P: Supply Chain Risk Management Plan (SCRMP)

This needs work that may have been completed elsewhere and nees to be moved into here. This needs MVP and Normalized content examples

---

MVP Key Points Include:

- The SR-2 (`id`=`sr-2` control should have `links` entries to the user guide

This is not normalized and is only for legacy conversion MVP

Normalized Key points include:

- attach the SCRMP as a back-matter/`resources` entry
- create a component for the SCRMP
  - From the componet, add a `links` entry that references the `resource` (#uuid-value)
- The SR-2 control has `by-components` entrys that cite the SCRMP component

Reference Components [need citation - there may be a page for document-type compnents] and Attachments pages. Don't duplicate those explanations here.

Appendix Q: Cryptographic Modules

Cryptographic Modules Implemented for Data-in-Transit (DIT)

OSCAL's component model treats independent validation of products and services as if that validation were a separate component. This means when using components with FIPS 140 validated cryptographic modules, there must be two component assemblies:

- **The Validation Definition**: A component that provides details about the validation.
- **The Product Definition**: A component that describes the hardware or software product.

The validation definition is a component that provides details about the independent validation. Its type must have a value of "validation". In the case of FIPS 140 validation, this must include a link field with a rel value set to "validation-details". This link must point to the cryptographic module's entry in the NIST Computer Security Resource Center (CSRC) Cryptographic Module Validation Program Database.

The product definition is a product with a cryptographic module. It must contain all of the typical component information suitable for reference by inventory-items and control statements. It must also include a link field with a rel value set to "validation" and an href value containing a URI fragment. The fragment must start with a hashtag (#) and include the UUID value of the validation component. This links the two together.

Appendix Q <CSO Name> Encryption Implementation Status

Data in Transit (DIT)										
	Source				Destination					
Ref #	Areas of DIT[1]	CMVP #[2]	CM Vendr	Module Name	Areas of DIT	CMVP #[3]	CM Vendor	Module Name	Usage	Notes[4]
1	NGINX Server <*Use Case Example - Please Delete*>	#4271 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other	Red Hat, Inc.	RHEL 8 OpenSSL	All Application Servers	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other	Canonical Ltd.	Ubuntu 18.04 OpenSSH Server	Load Balancer TLS to Application Server ☐ TLS 1.1 or earlier ☒ TLS 1.2 ☐ TLS 1.3 ☐ Other _____	
2	All Application Servers <*Use Case Example - Please Delete*>	None ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☐ In FIPS Mode ☐ Other	CentOS 7.9	OpenSSL 1.0.1	PostgreSQL	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other	Canonical Ltd.	Ubuntu 18.04 OpenSSH Server	Application servers to common DB ☐ TLS 1.1 or earlier ☒ TLS 1.2 ☐ TLS 1.3 ☐ Other _____	Plans to move to RHEL 8. See POA&M ID 111.

[1] Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located.
[2] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[3] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[4] For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc.

Component Representation: Data-In-Transit Example Product with FIPS 140-2 Validation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000300003
      type: software
      title: OpenSSL
      description: 'Provide a description and any pertinent note regarding the use
        of this CM.'
      props:
      - name: asset-type
        value: cryptographic-module
      - name: version
        value: 3.0.8
      - name: vendor-name
        ns: http://fedramp.gov/ns/oscal
        value: OpenSSL FIPS Provider
      - name: function
        ns: http://fedramp.gov/ns/oscal
        value: data-in-transit
        remarks: Usage statement
      links:
      - href: '#11111111-2222-4000-8000-009001200002'
        rel: validation
        text: A link to the 3rd party validation information related to this cryptographic
          module.
      status:
        state: operational

    - uuid: 11111111-2222-4000-8000-009001200002
      type: validation
      title: OpenSSL FIPS 140-2 Validation
      description: Describe any relevant information regarding this validation of
        the CM.
      props:
      - name: asset-type
        value: cryptographic-module
```

```
      - name: validation-type
        value: fips-140-2
      - name: validation-reference
        value: '4811'
    status:
        state: operational
```

Understanding the Data-in-Transit (DIT) Mapping

When documenting cryptographic protections for data-in-transit, the OSCAL model focuses on the relationship between the specific software provider and its validated state.

- **Software Component & Function:** The first block defines the actual implementation (e.g., **OpenSSL**). The property `name: function` with the value `data-in-transit` explicitly categorizes the module's role. This allows auditors and automated tools to identify which software is responsible for protecting communication channels, such as TLS or SSH connections, across the system boundary.
- **Decoupled Validation Metadata:** Rather than burying version-specific details in a text field, OSCAL uses a `link` to connect the software component to a separate `validation` component. This second component (highlighted by the `validation-reference` value **4811**) points directly to the NIST CMVP certificate.
- **Operational Status:** The `state: operational` field confirms that the module is currently in use within the environment. If a module were undergoing an update or was in a "historical" state, this status could be updated to reflect the current risk posture without needing to rewrite the entire narrative.

By structuring the SSP this way, you ensure that every cryptographic module used for DIT is traceable to a specific FIPS 140-2 or 140-3 certificate, satisfying the requirements for **SC-13 (Cryptographic Protection)** in a machine-verifiable format.

Cryptographic Modules Implemented for Data-at-Rest (DAR)

The approach is the same as in the *cryptographic module data-in-transit* section.

Data at Rest (DAR)							
Ref #	**Areas of DAR[5]**	**CMVP # [6]**	**CM Vendor Name**	**Module Name**	**Usage**	**Encryption Type**	**Notes[7]**
1	PostgreSQL database *<Use Case Example - Please Delete>*	#3980 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Canonical Ltd.	Ubuntu 18.04 OpenSSL Cryptographic Module	Volume encryption	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	
2	App server local storage *<Use Case Example - Please Delete>*	#2931 ☐ Embedded CM ☐ Third-party CM ☒ Uses OS CM ☒ In FIPS Mode ☐ Other _____	Microsoft	Windows Server 2016	OS and application binaries	☐ Full disk ☒ File ☐ Record ☐ None ☐ Other _____	CM is Historical, per NIST CMVP. Plans to move to Windows 2019 upon Active FIPS-140-validation achieved. See POA&M ID 123.
3	S3 buckets *<Use Case Example - Please Delete>*	#4177 ☒ Embedded CM ☐ Third-party CM ☐ Uses OS CM ☒ In FIPS Mode ☐ Other _____	AWS	Key Management Service (KMS) HSM	Server-side encryption with KMS keys (SSE-KMS) used to encrypt bucket	☒ Full disk ☐ File ☐ Record ☐ None ☐ Other _____	

[5] Each entry should be the component or asset where the FIPS-140 validated cryptographic module is located.
[6] If using cryptography that lacks FIPS validation, state "No FIPS". If unencrypted, state "Unencrypted".
[7] For example, specify if the historical CM is used or the store lacks encryption entirely. Include the related POA&M ID, remediation plans, etc.

Component Representation: Data-At=Rest Example Product with FIPS 140-2 Validation

```
system-security-plan:
  uuid: 11111111-2222-4000-8000-000000000000
  system-implementation:
    components:
    - uuid: 11111111-2222-4000-8000-009000300012
      type: software
      title: Database Row Encryption Module
      description: Briefly describe the cryptographic module.
      props:
      - name: asset-type
        value: cryptographic-module
      - name: version
        value: 1.2.3
      - name: vendor-name
        ns: http://fedramp.gov/ns/oscal
        value: Databases-R-Us
      - name: function
```

```
      ns: http://fedramp.gov/ns/oscal
      value: data-at-rest
      remarks: Used to encrypt and decrypt rows in the database.
    status:
      state: operational

  - uuid: 11111111-2222-4000-8000-009001200001
    type: validation
    title: Database Row Encryption Module (DREM)
    description: Briefly describe the cryptographic module.
    props:
    - name: asset-type
      value: cryptographic-module
    - name: validation-type
      value: fips-140-2
    - name: validation-reference
      value: '0000'
    status:
      state: operational
```

Understanding the Data-at-Rest (DAR) Mapping

In the OSCAL representation of data-at-rest protections, the focus shifts from communication protocols to the specific encryption mechanisms securing stored information.

- **Defining the Storage Function:** The property `name: function` with the value `data-at-rest` explicitly categorizes the module's role. The accompanying `remarks` field—such as "Used to encrypt and decrypt rows in the database"—provides the necessary context for human reviewers to understand the scope of the encryption (e.g., full-disk vs. application-layer encryption).
- **Asset Categorization:** By using the `asset-type: cryptographic-module` property, the component is tagged for automated compliance auditing. This allows the system to verify that every component handling sensitive federal data is linked to a valid cryptographic implementation, directly supporting **SC-28 (Protection of Information at Rest)**.
- **Validation Linkage:** Similar to the data-in-transit model, the software component is linked to a `validation` component that holds the NIST CMVP metadata. The `validation-reference` (e.g., **0000**) acts as the source of truth for the FIPS 140-2 or 140-3 certificate number, ensuring that the module meets the mandatory federal security standards for data storage.

By organizing DAR in this manner, the SSP provides a granular inventory of encryption at every layer of the technology stack—from the database row level up to the storage volume—while maintaining a clear audit trail to the validated cryptographic provider.

> **NOTE:**
>
> While the examples show FIPS 140-2, the same OSCAL structure applies to FIPS 140-3. Simply update the `validation-type` property to reflect the current standard.