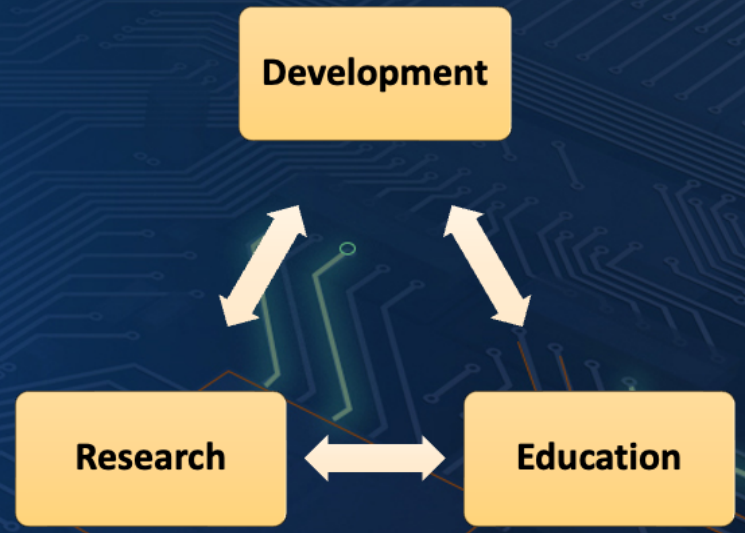
OSCAL DEFINE

Develop Enhancements, Future Implementations and New Education



NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

Agenda

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- The Patterns
- The Assemblies
- The Examples

Concerns Today

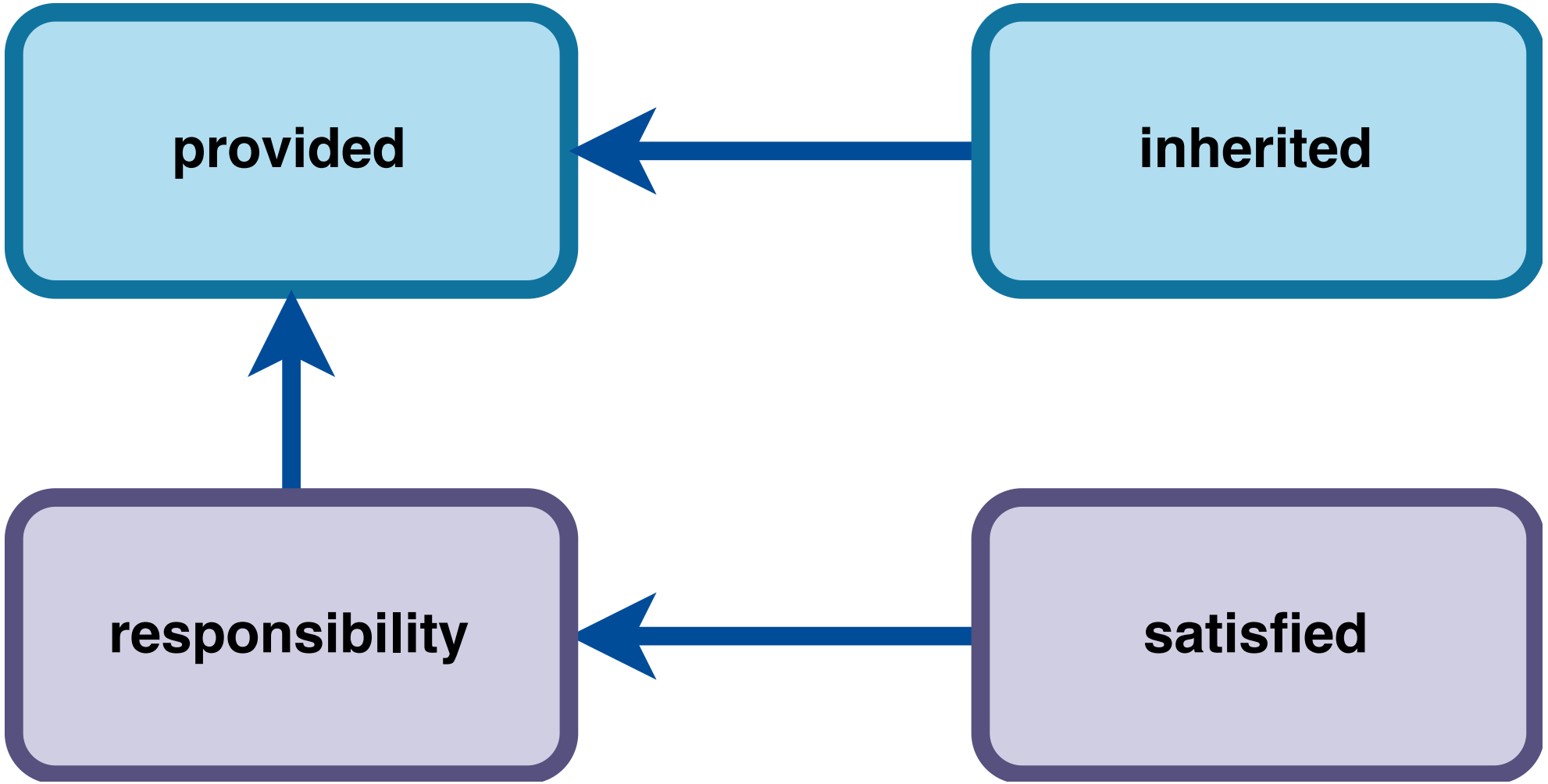
1. Patterns
2. Assemblies
3. Identifier Propagation (UUIDs)

The Responsibility Pattern

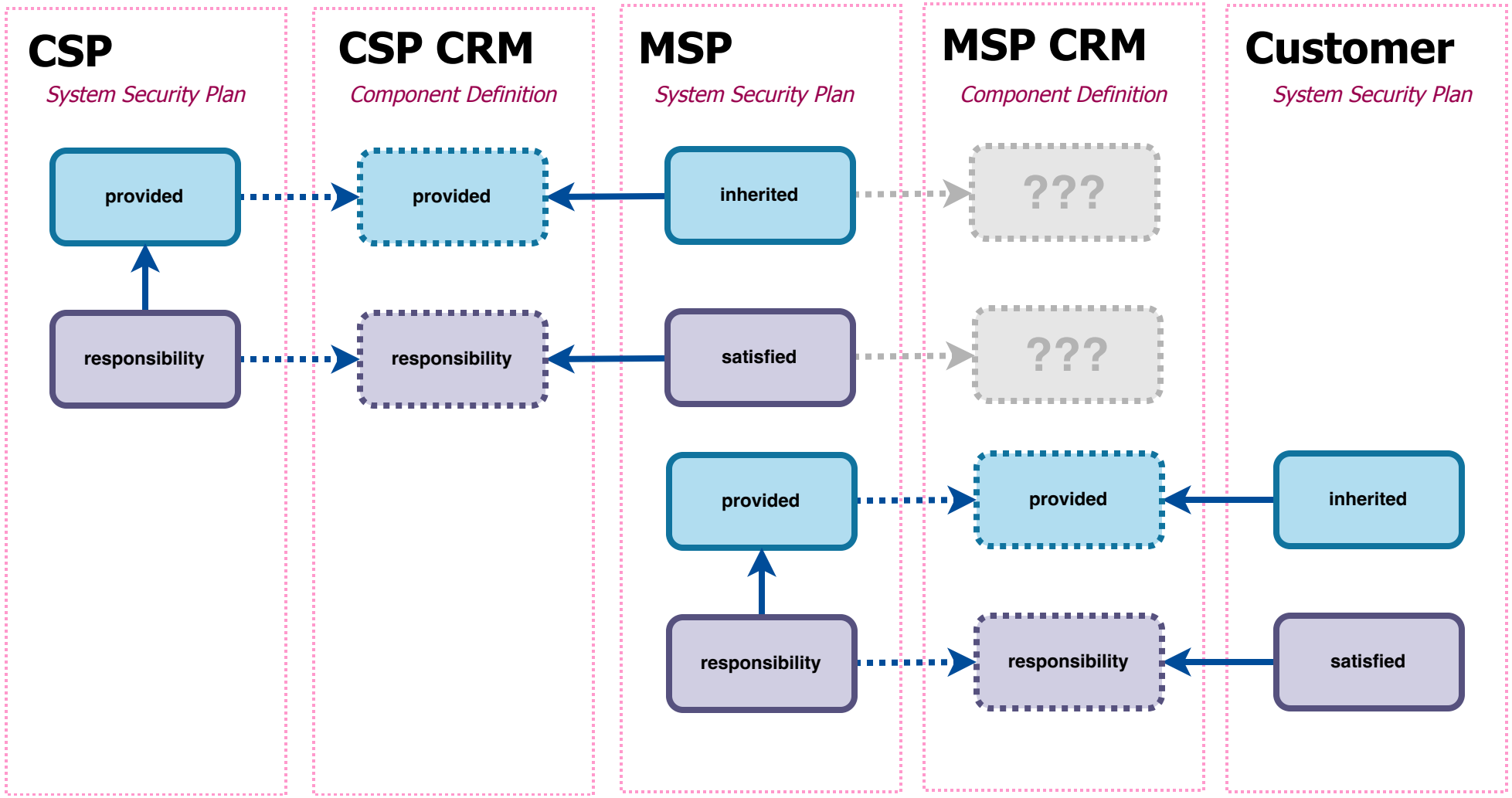
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

Basic Pattern



CRM Sharing Pattern



SSP Assemblies

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

System Security Plan

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- Exportable flag (attribute) on:
  - `implementation-status`
  - assemblies
- Added `provided` outside of export.
- Added `responsibility` outside of export

```
==========================================
sysetm-security-plan:
    control-implementation:
        implemented-requirements:
            by-components:
==========================================
implementation-status [0 or 1]: {
++    exportable [0 or 1]: boolean,
}

inherited [0 or 1]: [
    An array of inherited object [1] {
    }
],

satisfied [0 or 1]: [
    An array of satisfied object [1] {
    }
],

++provided [0 or 1]: [
    An array of provided object [1] {
    }
],

++responsibility [0 or 1]: [
    An array of responsibility object [1] {
    }
],
```

System Security Plan

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Rendered Example

```
▼ by-components [0 or 1]: [
      An array of by-component objects [1 to ∞] {
          component-uuid [1]: uuid,
          uuid [1]: uuid,
          description [1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        ▶ set-parameters [0 or 1]: [ … ],
        ▼ implementation-status [0 or 1]: {
              exportable [0 or 1]: boolean,
              state [1]: token,
              remarks [0 or 1]: markup-multiline,
          },
        ▶ provided [0 or 1]: [ … ],
        ▶ responsibility [0 or 1]: [ … ],
        ▶ inherited [0 or 1]: [ … ],
        ▶ satisfied [0 or 1]: [ … ],
        ▶ export [0 or 1]: { … },
        ▶ responsible-roles [0 or 1]: [ … ],
          remarks [0 or 1]: markup-multiline,
      }
  ],
```

CDef Assemblies

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Information Technology Laboratory
Computer Security Division

Component Definition

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

- Exportable flag (attribute) on:
  - `implementation-status`
  - assemblies
- Added `provided` outside of export.
- Added `responsibility` outside of export

```
========================================
component-definition:
    components:
        control-implementations:
            implemented-requirements:
========================================
++ implementation-status [0 or 1]: {
++    exportable [0 or 1]: boolean,
++ }

++inherited [0 or 1]: [
    An array of inherited object [1] {
    }
],

++satisfied [0 or 1]: [
    An array of satisfied object [1] {
    }
],

++provided [0 or 1]: [
    An array of provided object [1] {
    }
],

++responsibility [0 or 1]: [
    An array of responsibility object [1] {
    }
],
```

Component Definition

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Rendered Example

```
▼ implemented-requirements [1]: [
      An array of implemented-requirement objects [1 to ∞] {
          uuid [1]: uuid,
          control-id [1]: token,
          description [1]: markup-multiline,
        ▶ props [0 or 1]: [ … ],
        ▶ links [0 or 1]: [ … ],
        ▶ set-parameters [0 or 1]: [ … ],
        ▶ responsible-roles [0 or 1]: [ … ],
        ▶ implementation-status [0 or 1]: { … },
        ▶ provided [0 or 1]: [ … ],
        ▶ responsibility [0 or 1]: [ … ],
        ▶ inherited [0 or 1]: [ … ],
        ▶ satisfied [0 or 1]: [ … ],
        ▶ export [0 or 1]: { … },
        ▶ statements [0 or 1]: [ … ],
          remarks [0 or 1]: markup-multiline,
      }
  ],
```

The Examples

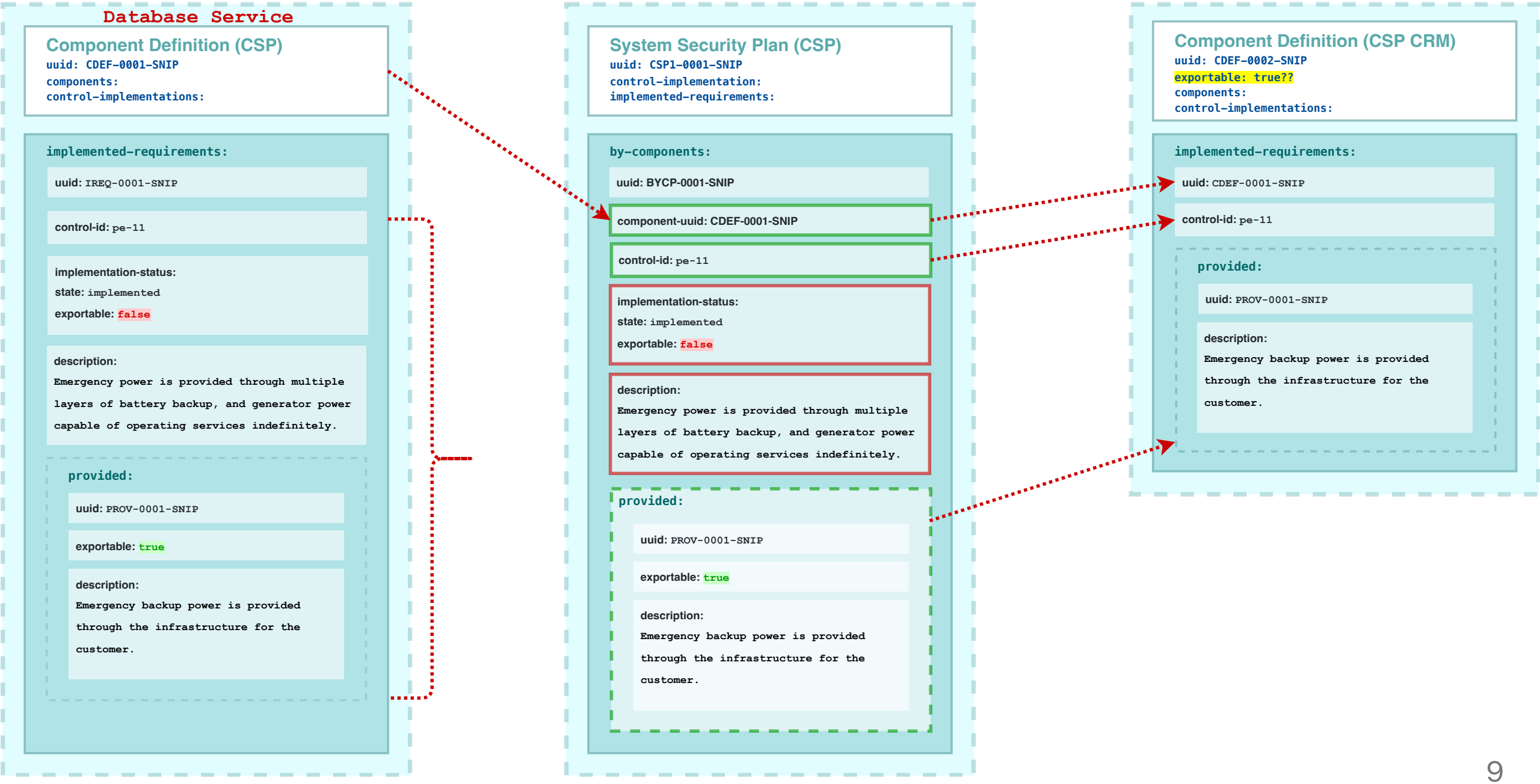
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

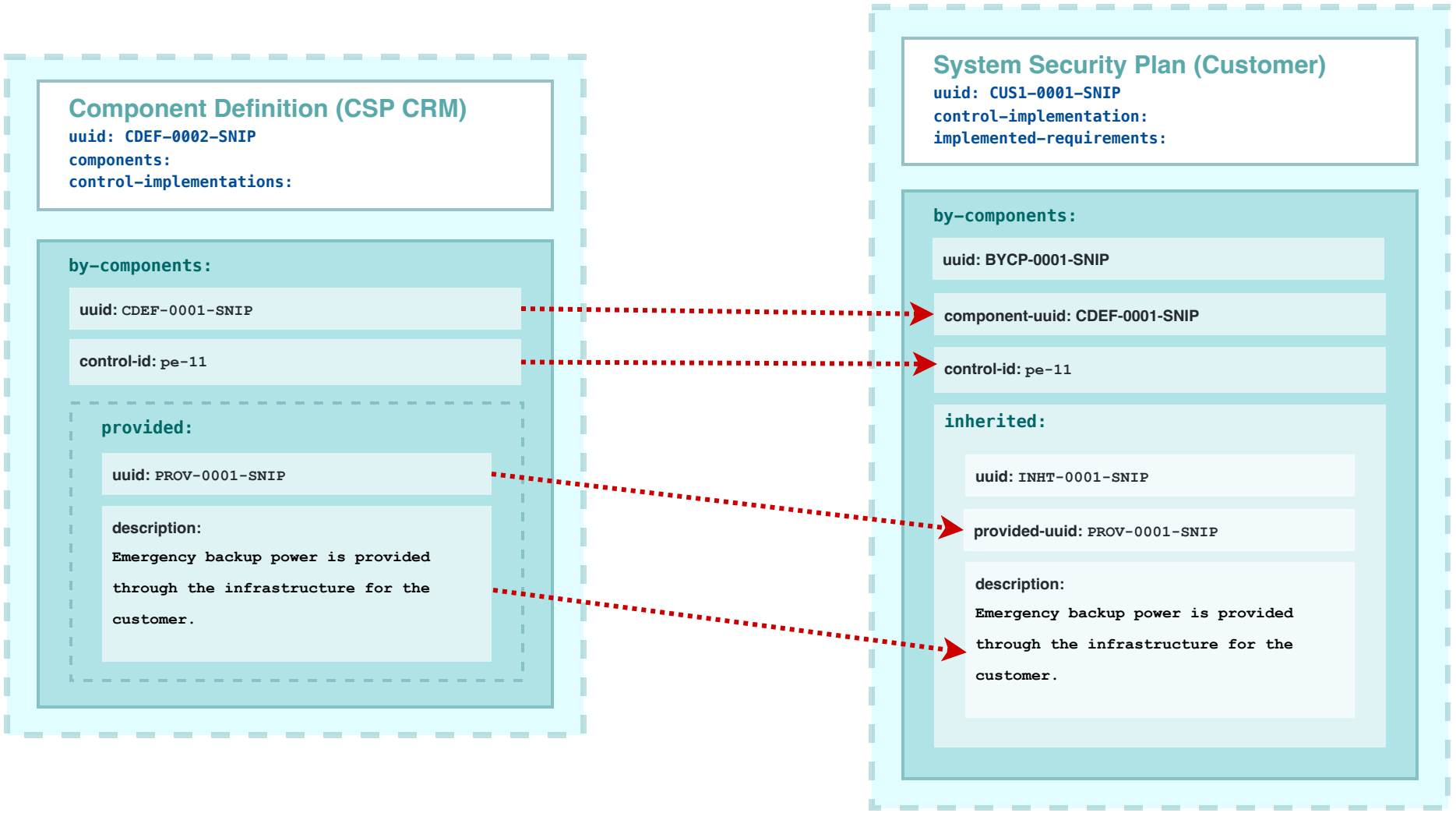
Information Technology Laboratory
Computer Security Division

Applied Example #1

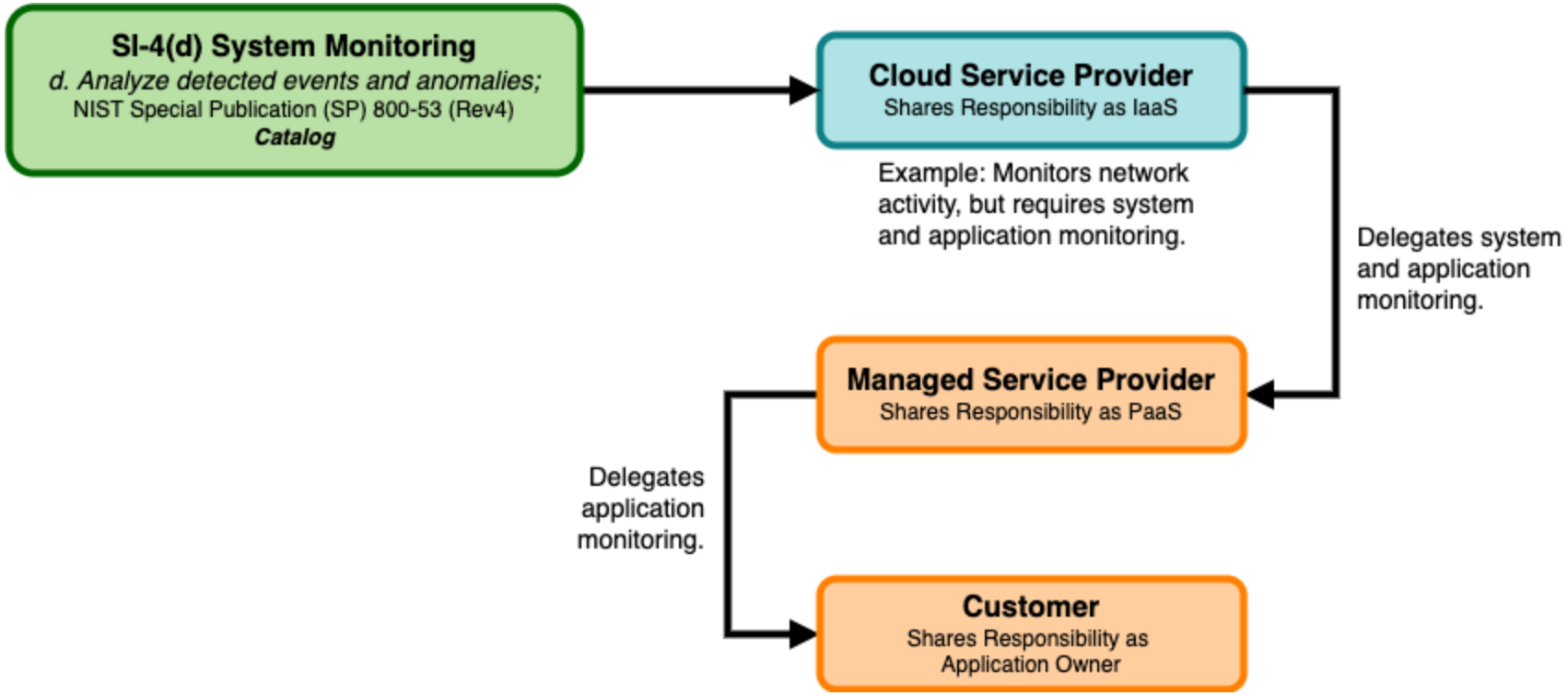
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Single Control, Fully Inherited


Database Service
Component Definition (CSP)
uuid: CDEF-0001-SNIP
components:
control-implementations:
implemented-requirements:
uuid: IREQ-0001-SNIP
control-id: pe-11
implementation-status:
state: implemented
exportable: false
description:
Emergency power is provided through multiple layers of battery backup, and generator power capable of operating services indefinitely.
provided:
uuid: PROV-0001-SNIP
exportable: true
description:
Emergency backup power is provided through the infrastructure for the customer.
System Security Plan (CSP)
uuid: CSP1-0001-SNIP
control-implementation:
implemented-requirements:
by-components:
uuid: BYCP-0001-SNIP
component-uuid: CDEF-0001-SNIP
control-id: pe-11
implementation-status:
state: implemented
exportable: false
description:
Emergency power is provided through multiple layers of battery backup, and generator power capable of operating services indefinitely.
provided:
uuid: PROV-0001-SNIP
exportable: true
description:
Emergency backup power is provided through the infrastructure for the customer.
Component Definition (CSP CRM)
uuid: CDEF-0002-SNIP
exportable: true??
components:
control-implementations:
implemented-requirements:
uuid: CDEF-0001-SNIP
control-id: pe-11
provided:
uuid: PROV-0001-SNIP
description:
Emergency backup power is provided through the infrastructure for the customer.


Component Definition (CSP CRM)
uuid: CDEF-0002-SNIP
components:
control-implementations:
by-components:
uuid: CDEF-0001-SNIP
control-id: pe-11
provided:
uuid: PROV-0001-SNIP
description:
Emergency backup power is provided through the infrastructure for the customer.
System Security Plan (Customer)
uuid: CUS1-0001-SNIP
control-implementation:
implemented-requirements:
by-components:
uuid: BYCP-0001-SNIP
component-uuid: CDEF-0001-SNIP
control-id: pe-11
inherited:
uuid: INHT-0001-SNIP
provided-uuid: PROV-0001-SNIP
description:
Emergency backup power is provided through the infrastructure for the customer.

Applied Example #2



Database Service

Component Definition (CSP)

uuid: CDEF-0001-SNIP
components:
control-implementations:

implemented-requirements:

uuid: IREQ-0001-SNIP

control-id: si-4 | statement-id: d

implementation-status:
state: implemented
exportable: false

description:

Provider implements portions of this control for IaaS and PaaS customers. Servers upload logs to a log monitoring tool and the audit logging process for aggregation and analysis. ...

provided:

uuid: PROV-0001-SNIP

exportable: true

description:
Provider implements portions of this control for IaaS and PaaS customers. Access to manage the security incident and event management tool used with the Infrastructure is limited to authorized personnel. These personnel are members of a security incident management team.

responsibility:

uuid: RESP-0001-SNIP

provided-uuid: PROV-0001-SNIP

exportable: true

description:
The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the protection of intrusion-monitoring tool information from unauthorized access, modification, and deletion.

System Security Plan (CSP)

uuid: CSP1-0001-SNIP
control-implementation:
implemented-requirements:

by-components:

uuid: BYCP-0001-SNIP

component-uuid: CDEF-0001-SNIP

control-id: si-4 | statement-id: d

implementation-status:
state: implemented
exportable: false

description:

Provider implements portions of this control for IaaS and PaaS customers. Servers upload logs to a log monitoring tool and the audit logging process for aggregation and analysis. ...

provided:

uuid: PROV-0001-SNIP

exportable: true

description:
Provider implements portions of this control for IaaS and PaaS customers. Access to manage the security incident and event management tool used with the Infrastructure is limited to authorized personnel. These personnel are members of a security incident management team.

responsibility:

uuid: RESP-0001-SNIP

provided-uuid: PROV-0001-SNIP

exportable: true

description:
The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the protection of intrusion-monitoring tool information from unauthorized access, modification, and deletion.

Component Definition (CSP CRM)

uuid: CDEF-0002-SNIP
exportable: true??
components:
control-implementations:

implemented-requirements:

uuid: CDEF-0001-SNIP

control-id: si-4 | statement-id: d

provided:

uuid: PROV-0001-SNIP

description:

Provider implements portions of this control for IaaS and PaaS customers. Access to manage the security incident and event management tool used with the Infrastructure is limited to authorized personnel. These personnel are members of a security incident management team.

responsibility:

uuid: RESP-0001-SNIP

provided-uuid: PROV-0001-SNIP

description:

The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the protection of intrusion-monitoring tool information from unauthorized access, modification, and deletion.

Component Definition (CSP CRM)

uuid: CDEF-0002-SNIP
exportable: true??
components:
control-implementations:

implemented-requirements:

uuid: CDEF-0001-SNIP

control-id: si-4 statement-id: d

provided:

uuid: PROV-0001-SNIP

description:

Provider implements portions of this control for IaaS and PaaS customers. Access to manage the security incident and event management tool used with the Infrastructure is limited to authorized personnel. These personnel are members of a security incident management team.

responsibility:

uuid: RESP-0001-SNIP

provided-uuid: PROV-0001-SNIP

description:

The customer is responsible for monitoring customer-deployed resources. The customer control implementation statement should address the protection of intrusion-monitoring tool information from unauthorized access, modification, and deletion.

System Security Plan (MSP)

uuid: CUS1-0002-SNIP
control-implementation:
implemented-requirements:

by-components:

uuid: BYCP-0002-SNIP

component-uuid: CDEF-0001-SNIP

control-id: si-4 statement-id: d

inherited:

uuid: INHT-0002-SNIP

provided-uuid: PROV-0001-SNIP

description:

Provider implements portions of this control for IaaS and PaaS customers. Access to manage the security incident and event management tool used with the Infrastructure is limited to authorized personnel. These personnel are members of a security incident management team.

satisfied:

uuid: SATD-0002-SNIP

responsibility-uuid: RESP-0001-SNIP

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion.

provided:

uuid: PROV-0002-SNIP

exportable: true

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion. The platform management team reviews alerts and logs as events are reported to the customer, and conducts daily analysis.

responsibility:

uuid: RESP-0002-SNIP

provided-uuid: PROV-0002-SNIP

exportable: true

description:

Application owners are responsible for monitoring their application logs for signs of unauthorized activity according to laws and regulations, and applying heightened scrutiny when there is an indication of increased risk.

Component Definition (MSP CRM)

uuid: CDEF-0003-SNIP
exportable: true??
components:
control-implementations:

implemented-requirements:

uuid: CDEF-0002-SNIP

control-id: si-4 statement-id: d

provided:

uuid: PROV-0002-SNIP

exportable: true

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion. The platform management team reviews alerts and logs as events are reported to the customer, and conducts daily analysis.

responsibility:

uuid: RESP-0002-SNIP

provided-uuid: PROV-0002-SNIP

exportable: true

description:

Application owners are responsible for monitoring their application logs for signs of unauthorized activity according to laws and regulations, and applying heightened scrutiny when there is an indication of increased risk.

Component Definition (MSP CRM)

uuid: CDEF-0003-SNIP

exportable: true??

components:

control-implementations:

implemented-requirements:

uuid: CDEF-0002-SNIP

control-id: si-4 | statement-id: d

provided:

uuid: PROV-0002-SNIP

exportable: true

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion. The platform management team reviews alerts and logs as events are reported to the customer, and conducts daily analysis.

responsibility:

uuid: RESP-0002-SNIP

provided-uuid: PROV-0002-SNIP

exportable: true

description:

Application owners are responsible for monitoring their application logs for signs of unauthorized activity according to laws and regulations, and applying heightened scrutiny when there is an indication of increased risk.

System Security Plan (Customer)

uuid: CUS1-0004-SNIP

control-implementation:

implemented-requirements:

by-components:

uuid: BYCP-0004-SNIP

component-uuid: CDEF-0003-SNIP

control-id: si-4 | statement-id: d

inherited:

uuid: INHT-0003-SNIP

provided-uuid: PROV-0002-SNIP

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion. The platform management team reviews alerts and logs as events are reported to the customer, and conducts daily analysis.

satisfied:

uuid: SATD-0003-SNIP

responsibility-uuid: RESP-0002-SNIP

description:

Monitors customer-deployed resources. Intrusion monitoring information protected from unauthorized access, modification and deletion.

Feedback

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

Contact us:

- oscal@nist.gov
- Issue: https://github.com/usnistgov/OSCAL-DEFINE/issues/17
- Discussion: https://github.com/usnistgov/OSCAL-DEFINE/discussions/13