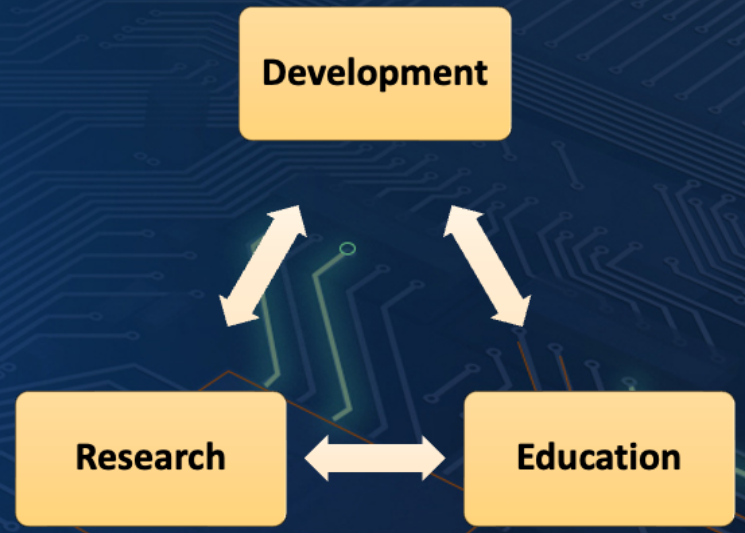
OSCAL DEFINE

Develop Enhancements, Future Implementations and New Education



NIST 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 Pattern
- The Example

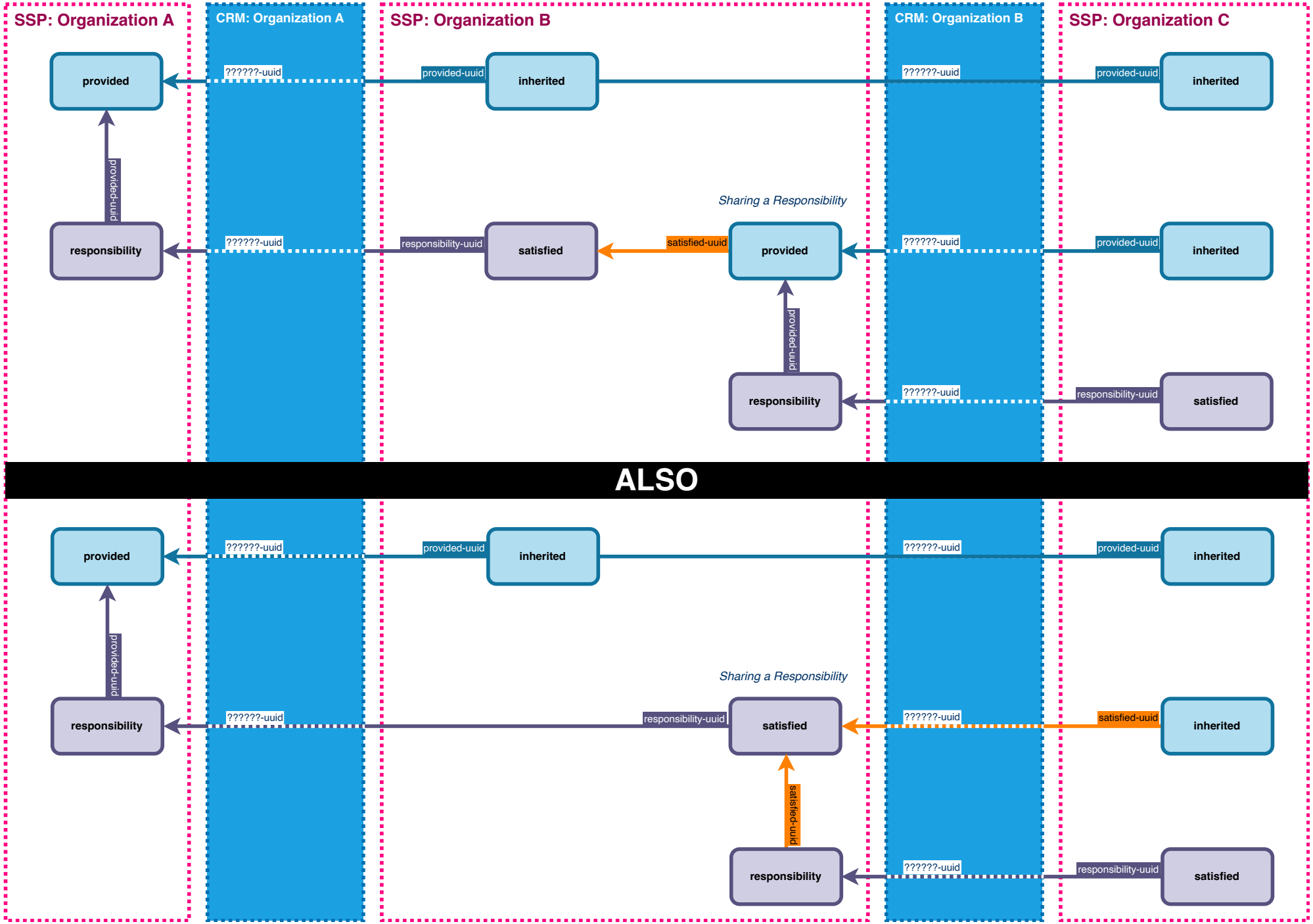
Concerns Today

1. The Pattern
2. Associations in the Pattern
3. Does it make sense?

The Responsibility Pattern

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

Information Technology Laboratory
Computer Security Division

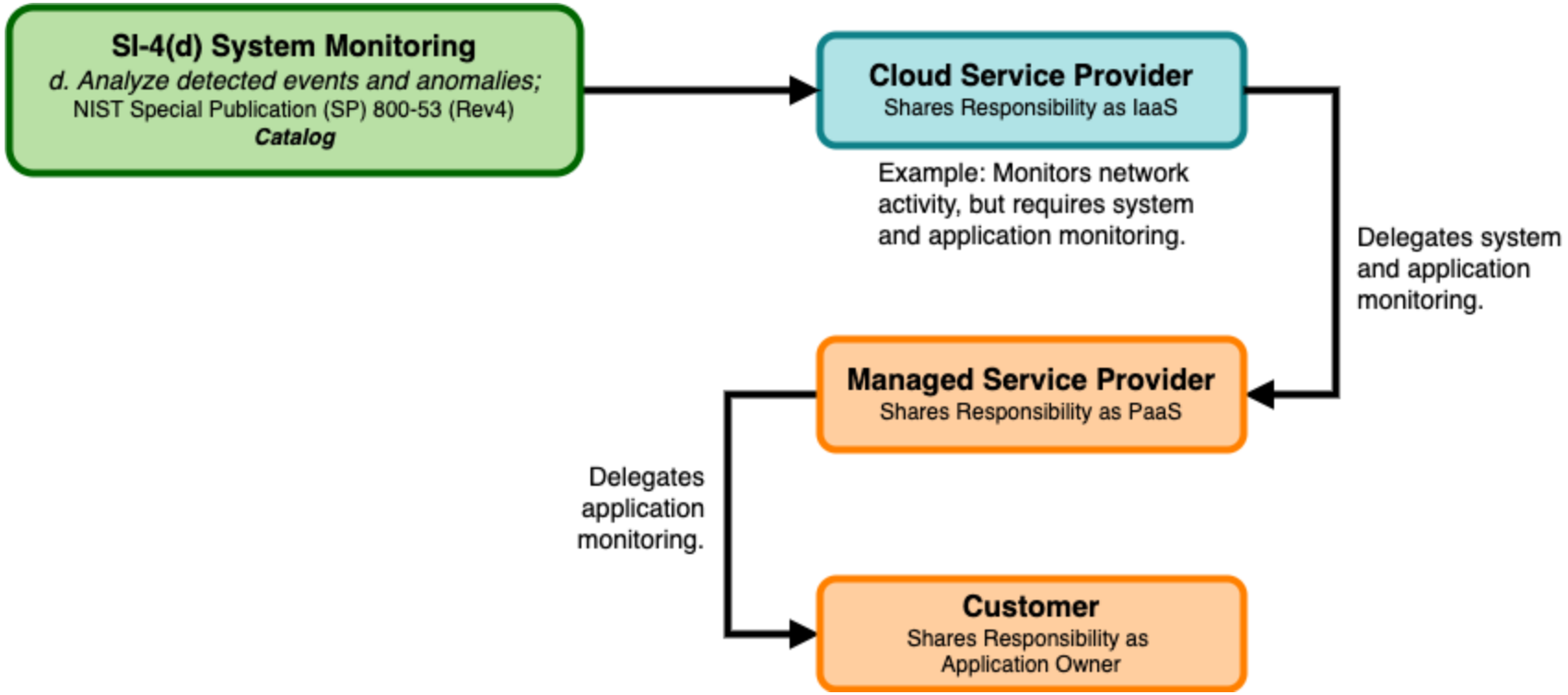

SSP: Organization A
CRM: Organization A
SSP: Organization B
CRM: Organization B
SSP: Organization C
provided
??????-uuid
provided-uuid
inherited
??????-uuid
provided-uuid
inherited
provided-uuid
Sharing a Responsibility
responsibility
??????-uuid
responsibility-uuid
satisfied
satisfied-uuid
provided
??????-uuid
provided-uuid
inherited
provided-uuid
responsibility
??????-uuid
responsibility-uuid
satisfied
ALSO
provided
??????-uuid
provided-uuid
inherited
??????-uuid
provided-uuid
inherited
provided-uuid
Sharing a Responsibility
responsibility
??????-uuid
responsibility-uuid
satisfied
??????-uuid
satisfied-uuid
inherited
satisfied-uuid
responsibility
??????-uuid
responsibility-uuid
satisfied

An Example

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

Information Technology Laboratory
Computer Security Division

Applied Example



Control: Analyze Events

> ***Requirement: Analyze detected events.***

- **Cloud Service Provider**
  - Analyze the network events.
- **Managed Service Provider**
  - Analyze the container events.
- **Application Owner**
  - Analyze the application events.

And… (with Proprietary Info)

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

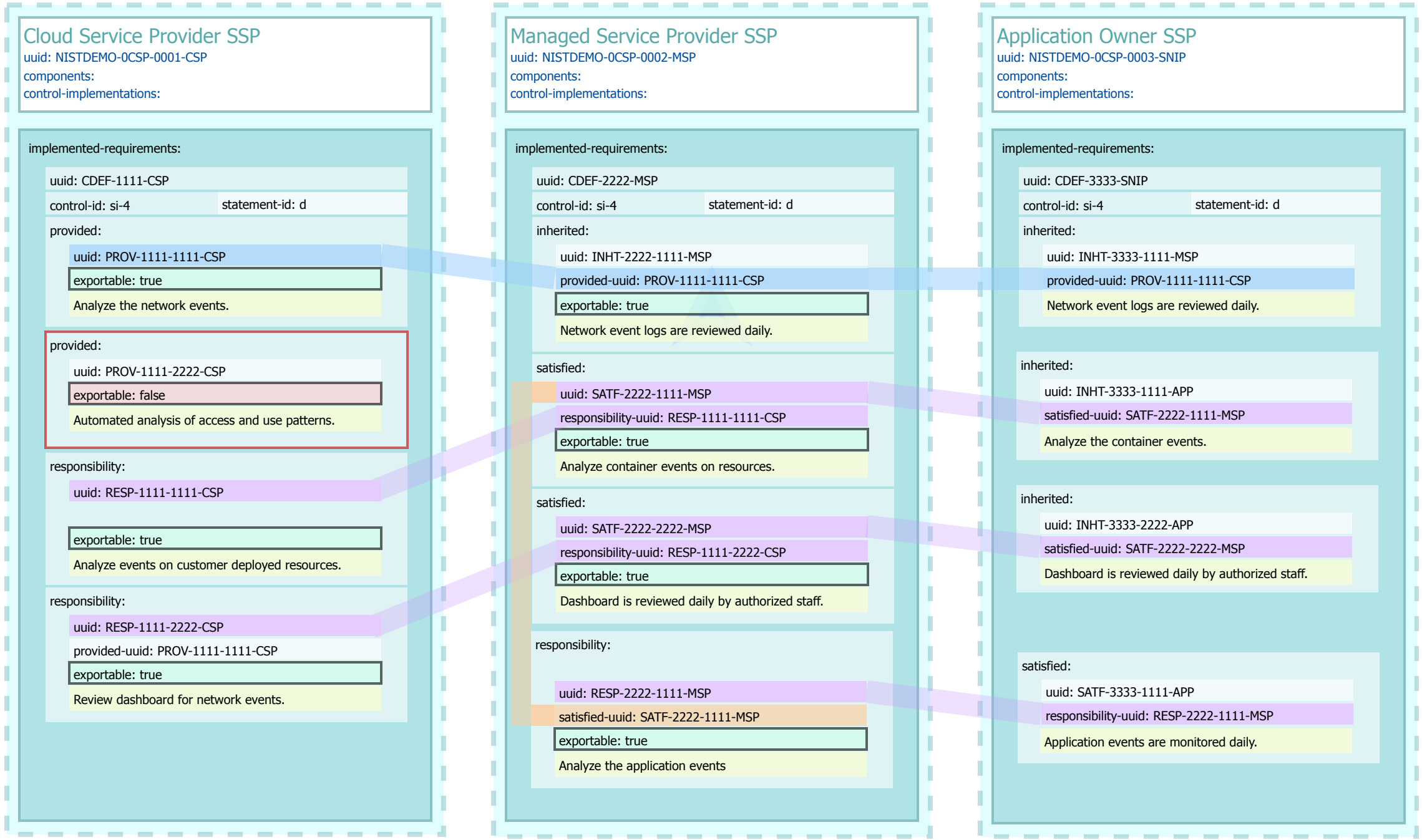
Cloud Service Provider | Analyze the network events

- PI: **Automated analysis** of patterns and characteristics of access and use.
- **Access** dashboard for events.

Managed Service Provider | Analyze the container events.

- **Review** service provider network dashboard on daily basis.

Application Owner | Analyze the application events.


Cloud Service Provider SSP
uuid: NISTDEMO-0CSP-0001-CSP
components:
control-implementations:
implemented-requirements:
uuid: CDEF-1111-CSP
control-id: si-4
statement-id: d
provided:
uuid: PROV-1111-1111-CSP
exportable: true
Analyze the network events.
provided:
uuid: PROV-1111-2222-CSP
exportable: false
Automated analysis of access and use patterns.
responsibility:
uuid: RESP-1111-1111-CSP
exportable: true
Analyze events on customer deployed resources.
responsibility:
uuid: RESP-1111-2222-CSP
provided-uuid: PROV-1111-1111-CSP
exportable: true
Review dashboard for network events.
Managed Service Provider SSP
uuid: NISTDEMO-0CSP-0002-MSP
components:
control-implementations:
implemented-requirements:
uuid: CDEF-2222-MSP
control-id: si-4
statement-id: d
inherited:
uuid: INHT-2222-1111-MSP
provided-uuid: PROV-1111-1111-CSP
exportable: true
Network event logs are reviewed daily.
satisfied:
uuid: SATF-2222-1111-MSP
responsibility-uuid: RESP-1111-1111-CSP
exportable: true
Analyze container events on resources.
satisfied:
uuid: SATF-2222-2222-MSP
responsibility-uuid: RESP-1111-2222-CSP
exportable: true
Dashboard is reviewed daily by authorized staff.
responsibility:
uuid: RESP-2222-1111-MSP
satisfied-uuid: SATF-2222-1111-MSP
exportable: true
Analyze the application events
Application Owner SSP
uuid: NISTDEMO-0CSP-0003-SNIP
components:
control-implementations:
implemented-requirements:
uuid: CDEF-3333-SNIP
control-id: si-4
statement-id: d
inherited:
uuid: INHT-3333-1111-MSP
provided-uuid: PROV-1111-1111-CSP
Network event logs are reviewed daily.
inherited:
uuid: INHT-3333-1111-APP
satisfied-uuid: SATF-2222-1111-MSP
Analyze the container events.
inherited:
uuid: INHT-3333-2222-APP
satisfied-uuid: SATF-2222-2222-MSP
Dashboard is reviewed daily by authorized staff.
satisfied:
uuid: SATF-3333-1111-APP
responsibility-uuid: RESP-2222-1111-MSP
Application events are monitored daily.