Compliance Analysis Method

With Examples from NEI 08-09 Cyber Security Plans

Copyright 2016 cmplid:// Inc. All Rights Reserved
# Compliance Analysis Method

**About cmplid://** ................................................................. 4

Overview.............................................................................. 4

Flexible Design..................................................................... 4

Resource-Based..................................................................... 5

Attribute-Aligned............................................................... 5

Risk-Informed....................................................................... 5

**Cmplid Glossary** ............................................................... 6

Artifact Type......................................................................... 6

Attribute ................................................................................ 6

Attribute Type ....................................................................... 7

Attribute Value ..................................................................... 7

Compliance Scope.................................................................. 7

Consequence.......................................................................... 7

Control................................................................................... 7

Control Map.......................................................................... 7

Control Test.......................................................................... 7

Guidance................................................................................ 7

Related Standard..................................................................... 8

Resource................................................................................ 8

Resource Type........................................................................ 8

Resource Prototype............................................................ 8

Security Objective.............................................................. 9

Standard................................................................................. 9

Standard Map......................................................................... 9

**Introduction** .................................................................... 10

Background............................................................................ 10

Diagram Legend...................................................................... 10

**Compliance Analysis Method** .......................................... 11

Correlate Standards to Resource Types................................ 12

Purpose.................................................................................. 12

  Control Inheritance........................................................... 12

  Hybrid Control..................................................................... 12

  System Specific Control.................................................... 13

  Analysis Process................................................................... 13

Copyright 2016 cmplid:// Inc.
ABOUT CMPLID://

Overview
The Compliance Daemon (cmplid://) is a security management solution, that moves beyond assessments and overly simplistic GRC metric tracking to provide real Security Management Automation.

cmplid:// was designed to integrate security program management with everyday operations. It does this by: enabling a consistent understanding of enterprise security programs; providing a mechanism for communicating responsibilities within those programs; and documenting the implementation and ongoing management of the programs.

Security management requires applying security standards to resources within scope, and cmplid:// facilitates this on a granular level.

cmplid:// fully supports the following aspects of security program management:

Compliance Management
Ensures that the security posture required to meet regulatory, internal, or third-party security standards is in place.

Risk Management
Ensures that the security posture appropriately protects business processes or system functions from identified negative events.

Vulnerability Management
Ensures that the security posture is functioning correctly.

Governance Management
Ensures that the security posture is managed according to organizationally defined roles and responsibilities.

Configuration Management
Ensures that the security posture is consistently maintained.

Flexible Design
Security management is a broad discipline, cmplid:// provides a very flexible approach to automating relevant operations, within a structured methodology. The methodology employed: Unified Security Management (USM) is resource-based, attribute-aligned, and risk-informed. USM is based on principles documented within NIST SP 800-53, and designed to work with any Information Technology (IT) or Operational Technology (OT) security program.
**Resource-Based**

cmplid:// utilizes the concept of control inheritance, granularly applied to the components of NIST SP 800-53’s Information Systems, NEI 08-09’s Critical Digital Assets, or NERC CIP’s Bulk Electric Cyber Systems to ensure that enterprise security programs are implemented, appropriate, functioning properly, and sufficiently maintained.

**Attribute-Aligned**

Characteristics of a resource will dictate where (upon which resources) the security standards must be implemented. These characteristics, or attributes, will dictate if the standards must be implemented on a given resource and how (through what implementing controls) the security standards will be implemented.

Attributes also indicate which specific resources are within scope of a managed security program.

**Risk-Informed**

cmplid:// provides for detailed analysis of the purpose and consequence of the individual security standards, attack pathways, and the threat agents that could exploit vulnerabilities in the resources within scope. This enables detailed tailoring of the security posture of the resources to organization or regulation specific criteria.

Documentation of the presence of threat vectors (NEI 08-09) or the significance or expected impact of risks (NIST CSF) can be defended to internal stakeholders and external auditors or regulators.
**Complied Glossary**

This section provides an introduction to the concepts that will be discussed throughout the remainder of the document.

**Artifact Type**

Artifact Types describe the documentation necessary to validate the implementation of a Control.

**Attribute**

Attributes define various characteristics of Resources that are used to determine when Standards must be implemented and how they will be implemented. They can also be used in other aspects of security management including determining appropriate baseline configuration requirements, vulnerability analysis, and risk analysis. Attributes are described within cmplid:// through both Attribute Types and Attribute Values and may apply to either Resources or Resource Prototypes. Attributes may be used for one of three purposes:

- Determine Compliance Scope: designated as SCOPE Attributes within cmplid://
- Determine Security Posture: designated as SECURITY POSTURE Attributes within cmplid://
- Provide additional Information: designated as INFORMATIONAL Attributes within cmplid://

Attributes are defined by a hierarchical structure according to the applicable Attribute Type. An example of Attributes that could be used to determine the security posture of CDAs subject to 10 CFR 73.54 is shown below:

![Example Security Posture Attributes Diagram](image-url)
Attribute Type
Attribute Types describe characteristics of Resources or Resource Prototypes. They document the purpose of the attribute: Scope; Security Posture; or Informational, as well as the DATA TYPE: Choice or Resource, and the applicability: Resource or Resource Prototype, for all attributes within cmplid://.

Attribute Inheritance is identified through selection of the RESOURCE PROVIDES INHERITANCE value for Attribute Types whose DATA TYPE is Resource. Inheritance allows one Resource Type to utilize the Attributes of another Resource Type for the context of Compliance Scope determinations and the applicability of Standard Maps and Control Maps.

Attribute Value
Attribute Values are either text-based choices defined within cmplid:// or the Resources within the cmplid:// database.

Compliance Scope
A Compliance Scope associates a group of Standards with a Resource Type that the Standards are applicable to, based on dependent Resource Attribute Values, either resource specific or inherited, that determine a particular Resource's compliance requirements.

Consequence
Consequences, closely related to Security Objectives, define the negative impact that would be expected upon failure or absence of related Standards.

Control
Controls are the detailed implementation mechanisms used to fulfill the Standards.

Control Map
Control Maps associate one or more Controls to a Standard Map according to the (optional) relevant Attribute Values (Resource-Specific or Inherited) that indicate how a the Standards will be implemented. Resources within the Compliance Scope that do not match the Attribute Values, if applicable will implement the associated Standards through another Control Map. Control Maps also indicate if the Controls implemented should be considered a DIRECT, ALTERNATE, or INHERITED implementation of the relevant Standards.

Control Test
Control Tests describe the process necessary to verify the implementation of a Control.

Guidance
Guidance provides clarifying information, implementation advice, background, or similar information for Standards.
**Related Standard**
Related Standards describe the connections between Standards that may assist in the implementation or management of the Security Program. The relationships are organizationally defined, and generally indicate the origin of Standards, similarities between Standards, or provide background or similar implementation guidance for Standards.

**Resource**
Resources are the various technical and business assets that an organization must protect in order to comply with a given Security Program. Organizational resources are categorized according to their Resource Type then by Resource Prototype.

**Resource Type**
Resource type's are the fundamental business and technical objects upon which all security management activities are performed. They most often represent physical or logical assets owned by an organization that must have security requirements applied, managed, and reported on for compliance, risk, vulnerability, or governance management.

There are nine default Resource Types within cmplid://

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software</td>
<td>Compiled computer code.</td>
</tr>
<tr>
<td>Hardware</td>
<td>Automated processing systems and the underlying Operating Systems</td>
</tr>
<tr>
<td>Network</td>
<td>Physically and logically connected devices, usually communicating via the TCP/IP protocol suite.</td>
</tr>
<tr>
<td>Source Code</td>
<td>Human modifiable (uncompiled or interpreted) source code.</td>
</tr>
<tr>
<td>Media</td>
<td>Information storage</td>
</tr>
<tr>
<td>Information</td>
<td>General classes of information that require protection based on the sensitivity to compromise of confidentiality, integrity, or availability.</td>
</tr>
<tr>
<td>Location</td>
<td>Facilities, rooms, racks, containing resources requiring protection.</td>
</tr>
<tr>
<td>Organization</td>
<td>Collections of resources (people, equipment, facilities, etc...) with a common mission, business objective, or purpose.</td>
</tr>
<tr>
<td>Personnel</td>
<td>People within scope of the compliance program</td>
</tr>
</tbody>
</table>

Default cmplid:// Resource Types

**Resource Prototype**
Resource Prototypes are distinct categories of Resource Type. They most often describe physical or logical assets (e.g. specific make and model or generic class of similar assets) owned by an organization that have fixed Attribute Values. All Resources are instances of Resource Prototypes and inherit all of the Attribute Values assigned.
Security Objective
Security Objectives define the purpose for the Standards; they explain, generally at a high level, the conditions that necessitate application of a security mechanism. Security Objectives should give an indication of the method or process that could be used by an unauthorized person to compromise the confidentiality, integrity, or availability of Resources or the Business Processes or System Functions supported by Resources.

Standard
Standards are the specific regulatory or internal security requirements that must be addressed for all organizational resources subject to the security program they are derived from. The Cyber Security Plans (CSP) defined for nuclear licensees subject to 10 CFR 73.54, provide two source documents for Standards NEI 08-09, appendices A, D, and E, and NEI 13-10, which provides guidance for addressing the NEI 08-09 controls for various types of “Indirect” CDAs.

Standard Map
Standard Maps associate one or more Standards within a Compliance Scope to the (optional) relevant Attribute Values (Resource-Specific or Inherited) that indicate a Resource must implement the selected Standards. Resources within the Compliance Scope that do not match the Attribute Values, if applicable will not need to implement the selected Standards; those Standards will be dispositioned according to the governing Security Program's configuration.
INTRODUCTION

Background

The compliance management analysis methodology employed by cmplid:// is designed to reduce the confusion created by the inherent ambiguity within all cyber security program requirements. Each step in the analysis process reduces ambiguity and provides further clarity to the cyber security program.

Upon completion of this process, the organization gains granular insight of, at a minimum:

- Where the Standards will be addressed
- What classes of Resources require which specific Standards
- Why the Standards are necessary
- What Resources the Standards will be applied to
- What categories of Resources exist
- How the Standards will be implemented and optionally how they can be verified and validated

The process progresses through converting information obtained from relevant documentation into structured data. This structured data is stored within the cmplid:// database back-end, however, non cmplid:// users can benefit from following this process as well, storing that structured data in whatever backend (spreadsheets, user-developed db, third-party tool, etc…) is available.

Diagram Legend

The following diagram illustrates the elements used within the following diagrams.
The following diagram illustrates the overall cmplid:// compliance analysis method tasks and the information that will be learned from each task:

- **Correlate Standards to Resource Types**: Where the Standards will be addressed
- **Document Compliance Scopes**: What classes of Resources require which specific Standards
- **Document Security Objectives**: Why the Standards are necessary
- **Map Standards**: What Resources the Standards will be applied to
- **Document Resource Prototypes**: What categories of Resources exist
- **Map Controls**: How the Standards be implemented and optionally how they can be verified and validated

**Compliance Analysis Task Diagram**

It must be noted before beginning, this analysis may seem complex and time consuming, however, review of the questions listed above will provide that it is nothing more than a formal documentation of what must be known in order to implement a cyber security program.

Nothing more is required by this method than what otherwise must be done; it simply formalizes the documentation of the analysis that those who are implementing the project will be executing. This provides the basis for a sustainable and mature security program.

The process was designed to be flexible and should not be adopted with strict dogmatic adherence. There may be occasions where your organizations culture, resources, or approach to security management require deviations from elements of this approach. Tailor the approach to your specifics where necessary.
Correlate Standards to Resource Types

The following diagram depicts the first task in the Compliance Analysis process:

**Correlate Standards to Resource Types Task Diagram**

**Purpose**

The purpose of this step of the methodology is to determine where the Standards will be applied. In this context “applicability” refers to the objects or resources upon which the Standards will be implemented, considering the concept of control inheritance, as described in NIST SP 800-53:

**Control Inheritance**

*A situation in which an information system or application receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.*

NIST SP 800-53, Glossary

The key in this definition is the emphasized portion: entities other than those responsible for the system or application. Inherited (common) controls are not implemented directly on information systems or components thereof. They are applied to other resources or resource types.

**Hybrid Control**

*A security control that is implemented in an information system in part as a common control and in part as a system-specific control.*

NIST SP 800-53, Glossary
System Specific Control

A security control for an information system that has not been designated as a common security control or the portion of a hybrid control that is to be implemented within an information system.

NIST SP 800-53, Glossary

To further clarify the concept, it is important to consider upon what type of Resource the Standards will be applied, as the entity responsible will often be delineated by Resource Type, e.g. the entity responsible for developing and maintaining policies and procedures will often be different than the entity responsible for managing hardware.

The policies and procedures written will generally apply to an organization or group of organizations and the guidance within will be followed by all personnel within those organizations managing hardware. In this example the policies and procedures “apply” to organizations and are inherited by the hardware owned or managed by the organization.

Additional examples are provided below:

- Firewalls and data diodes are applied to networks and all hardware and software running on those networks inherit the protection from the network
- Training and background investigations are provided to personnel with access to all other Resources, which then inherit those controls from their users
- Physical security measures are generally applied to physical locations; the hardware, networks, and information within inherit those controls
- Many security controls applied to hardware, e.g. malicious code prevention, network access control mechanisms, etc… are inherited by the software applications installed on the hardware
- Controls associated with centralized log aggregation, correlation, and analysis system management are inherited by all of the hardware and software configured to forward their logs to the central system.

As can be seen by the above examples, inheritance requires and understanding of the relationships between various resources. A specific hardware device can only inherit the physical security protections of the location it is within. Use of control inheritance is central to the methodology supported by cmplid://. It provides significant efficiency to cyber security management and is foundational to reducing ambiguity and confusion.

Analysis Process

Correlating Standards to Resource Types involves reviewing each individual Standard (NEI 08-09 Appendix A, D, & E control and a through g of section 5 of NEI 13-10) and determining upon which Resource Type they will be applied. NOTE: Many of the Standards apply to more than one Resource Type. Additionally through this review, a determination must be made of which Resource Types will inherit the protections applied from the other Resource Types and the relationships that will provide that inheritance.
cmplid:// Operation

Standard applicability is identified within cmplid:// through the RESOURCE TYPES checkboxes on each Standard form. Alternatively, this can be accomplished through the initial (or an update) import of the Standards in a batch process.

Standard Form

Resource Type inheritance is documented through the INHERITS PROTECTION FROM checkboxes on each Resource Type form.

Resource Type Form

Value Provided

This task provides value by explaining *where the Standards will be addressed.*
Document Compliance Scopes

The following diagram depicts the second task in the Compliance Analysis process:

![Document Compliance Scopes Diagram](image)

**Purpose**

The purpose of this step of the methodology is to determine what characteristics of the organizational Resources require protection under the Security Program and what those specific protections are.

This requires analysis of the scoping documents relevant to the Security Program. The text of NEI 08-09 provides high-level guidance of what constitutes a Critical Digital Asset (CDA), but the text of NEI 10-04 contains the industry accepted and NRC endorsed criteria.

Additionally, NEI 13-10 provides the criteria, generally regarded as by system, that determines the classification of CDA as either one of the “Indirect” classifications or a “Direct” CDA.

From these documents we understand that CDAs may be classified as one of the following Compliance Scopes:

- **Direct CDA**: Those CDAs that, if compromised, could result in an adverse impact to SSEP functions or systems or equipment that are used or relied on for performing SSEP functions or for making SSEP-related decisions. Direct CDAs would also include CDAs associated with support systems and equipment that, if compromised, could adversely impact systems or equipment that are used for performing SSEP functions or relied-on for making SSEP-related decisions.

---

1 NEI 13-10 Section 3.2
• Indirect CDA\(^2\)
  • Those CDAs that cannot have an adverse impact on or degrade SSEP functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee.

Indirect CDAs may be further grouped into the following Compliance Scopes:

• Indirect EP CDA\(^3\)
  • [Where] cyber attacks on CDAs associated with EP functions would not adversely impact the ability to implement the EP function, due to the availability of an alternate means of performing that function

• Indirect Balance of Plant (BOP) CDA\(^4\)
  • CDAs whose failure or cyber compromise could cause a reactor scram/trip

What is conspicuously absent from all of the NRC endorsed guidance documents for implementation of 10 CFR 73.54 is the identification of any Compliance Scopes other than the types of CDAs documented above. This does not mean that all of the Standards will be applied to CDAs. It simply means that all of the Standards are designed to protect CDAs, though the majority of the Standards will be applied to Resources other than CDAs.

Standard inheritance, consistent with the guidance from NIST SP 800-53 presented above, is used to ensure that all CDAs are protected by all (relevant) NEI 08-09 Standards. Review of many of the NEI 08-09 and NEI 13-10 Standards will provide that Resources of all the cmplid:// Resource Types are within scope and must have Compliance Scopes developed for them.

A partial list of those Compliance Scopes follows:

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Resource Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDA Location</td>
<td>Locations containing CDAs</td>
<td>Location</td>
</tr>
<tr>
<td>CDA Contingency Personnel</td>
<td>Personnel with responsibilities for responding to contingencies for CDAs</td>
<td>Personnel Group</td>
</tr>
<tr>
<td>CDA Incident Response Personnel</td>
<td>Personnel with responsibilities for responding to CDA cyber incidents</td>
<td>Personnel Group</td>
</tr>
<tr>
<td>Personnel with Access to CDAs</td>
<td>Personnel with physical or logical access to CDAs</td>
<td>Personnel Group</td>
</tr>
<tr>
<td>CDA Security Personnel</td>
<td>Personnel with responsibilities for CDA cyber security</td>
<td>Personnel Group</td>
</tr>
<tr>
<td>CDA Technical Personnel</td>
<td>Personnel with responsibilities for managing or maintaining CDAs</td>
<td>Personnel Group</td>
</tr>
<tr>
<td>CSAT Members</td>
<td>Members of the CSAT</td>
<td>Personnel Group</td>
</tr>
</tbody>
</table>

\(^2\) NEI 13-10 Section 3.1
\(^3\) NEI 13-10 Section 4 Paragraph 2
\(^4\) NEI 13-10 Section 5 Paragraph 6
Compliance Analysis Method

Additional NEI 08-09 Required Compliance Scopes

Every line in this table is derived directly from the requirements within NEI 08-09. All of these Resource Types required protection in order to comply with NEI 08-09. Designating the controls applicable to these Resource Types as generic “common” controls, or associated them with CDAs, is extremely inefficient and results in an immature security program that is difficult to maintain. There is simply too much ambiguity and too much data to manage absent defining these Compliance Scopes.

After Compliance Scopes are created the applicable Standards can be associated with them. This provides for each Standard to be managed independently for each Resource matching the Compliance Scope. This is where inheritance proves its value:

- Standards applicable to locations, e.g. physical security controls, can be managed only for each location containing CDAs not each individual CDA
- Standards applicable to organizations, e.g. policies and procedures, can be managed only for each organization within scope not each individual CDA
- Standards applicable to personnel groups, e.g. training requirements, can be managed only for each personnel group that matches the scoping criteria not each individual CDA

The implementation of these Standards can then be inherited by the other related Resource Types.

Analysis Process

Documenting Compliance Scopes requires reviewing the scoping questions contained throughout NEI 10-04 and NEI 13-10 and determining the classifications of CDAs that have distinct sets of Standards prescribed. Once the classifications have been identified, the specific Standards prescribed must be associated with the Compliance Scopes. For the non-CDA Compliance Scopes, review of the NEI 08-09 and NEI 13-10 Standards must be completed to find the sets of Standards prescribed for the other Resource Types.
Additionally, it is necessary to identify the characteristics of the Resources that indicate what Compliance Scope it must comply with. This is done by creating appropriate Attribute Types and Attribute values, from the guidance provided in NEI 10-04 and NEI 13-10.

**cmplid:// Operation**

Compliance Scopes are defined within cmplid:// using the Compliance Scope form. The relevant Standards are associated through the Standards select box (A) and the Specific Attribute Values (B) and Inherited Attribute Values (C) are associated through their respective select boxes.

**Compliance Scope Form**

Creation of the Attribute Types and Attribute Values is done through their forms within cmplid://.
Value Provided

This task provides value by explaining *what classes of Resources require which specific Standards.*
Document Security Objectives

The following diagram depicts the third task in the Compliance Analysis process:

![Diagram of Document Security Objectives](image)

**Purpose**

The purpose of this step of the methodology is to document the Security Objectives, used for vulnerability and risk management, for each of the Standards in scope of the security program. This is a necessary step for compliance management as it provides the basis for situations where a specified Standard will not be implemented for a Resource within scope.

There may be analysis that is documented during this step that is never referred to again, except when demonstrating to internal personnel, auditors, and the NRC inspectors the rationale for NOT implementing a given Standard on a given Resource.

**Analysis Process**

Documenting the Security Objectives requires definition of a simple statement of the purpose of the Standard from a business perspective i.e. the support they provide to SSEP functions. A correlating Consequence (of absence or failure of each control) in regard to the SSEP functionality impacted must also be documented. Consider the following examples:

<table>
<thead>
<tr>
<th>Index</th>
<th>Text</th>
<th>Security Objective</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 1.1 c1</td>
<td>The access control policy addresses: Access control rights (i.e., which individuals and processes can access what resources) and access control privileges (i.e., what these individuals and processes can do with the resources accessed);</td>
<td>Ensures policies and procedures address all relevant security topics.</td>
<td>Necessary security requirements will not be addressed in management model documentation.</td>
</tr>
</tbody>
</table>
## Index

<table>
<thead>
<tr>
<th>Index</th>
<th>Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>E 3.3 a1</td>
<td>Data communication between systems, CDAs, removable media, or other common means; and</td>
</tr>
<tr>
<td>D 1.2 a1</td>
<td>Manages and documents CDA accounts, including authorizing, establishing, activating, modifying, reviewing, disabling, and removing accounts.</td>
</tr>
<tr>
<td>D 1.17 a1</td>
<td>Restricts wireless devices to access through a boundary security control device and treats wireless connections as outside of the boundary.</td>
</tr>
<tr>
<td>D 3.9 a1</td>
<td>Manages cryptographic keys using automated mechanisms with supporting procedures or manual procedures when cryptography is required and employed within the CDAs in accordance with NRC Regulatory Issue Summary (RIS) 2002-15, Revision 1, NRC Approval of Commercial Data Encryption Products for the Electronic Transmission of Safeguards Information.</td>
</tr>
<tr>
<td>E 8.5 a1</td>
<td>Conducting backups of user-level and system-level information.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensures malicious code cannot propagate or execute within the technology infrastructure.</td>
<td>Malicious code will be used to compromise organizational resources.</td>
</tr>
<tr>
<td>Ensures all personnel granted logical access to technical resources are and remain appropriate to support business objectives.</td>
<td>Logical user accounts will be initially granted to or remain granted to inappropriate personnel or the logical permissions granted will exceed business objectives.</td>
</tr>
<tr>
<td>Prevents unauthorized devices from being connected to the network switches, routers, or hubs.</td>
<td>Unauthorized devices will gain access to the network.</td>
</tr>
<tr>
<td>Ensures that information with high-confidentiality requirements is protected from unauthorized disclosure.</td>
<td>The confidentiality of information will be compromised.</td>
</tr>
<tr>
<td>Ensures reliable operational state of and prompt restitution of technical infrastructure components upon failure.</td>
<td>Unreliable operation of technical infrastructure components upon failure.</td>
</tr>
</tbody>
</table>

### Example Security Objectives and Consequences

Once the Security Objectives and Consequences have been identified, the association of Specific Attribute Values and Inherited Attribute Values with the Standards, through the Standard Maps described in the next section will provide the analysis required to document the absence of Threat Vectors. Consider the following: if the Security Objective of D3.9a1 is to “Ensure that information with high-confidentiality requirements is protected from unauthorized disclosure” and the Consequence of that controls absence or failure on a specific CDA would be that “The confidentiality of information will be compromised” the Standard Map will limit application of the Standard through a Specific Attribute Value “The CDA contains sensitive information that must be protected (to ensure the reliability of its SSEP Function: True.”

This analysis informs us that this control and others focused on the protection of confidentiality of information would only be considered for CDAs where the relevant Attribute is true. If the Attribute is false for a given CDA, no negative impact to the SSEP functionality could be caused by the disclosure of the information, therefore the Threat Vector could not exist for that CDA.
cmplid:// Operation

Security Objectives and Consequences are created through their respective forms. Consequences are associated with Security Objectives through the SECURITY OBJECTIVES select box on the Consequence form. Dependent Attribute Values for the Security Objectives are inferred from the SPECIFIC ATTRIBUTE VALUES and INHERITED ATTRIBUTE VALUES select boxes on the related Standards Standard Map form (discussed below).

### Security Objective Form

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>The purpose of having restrictions on open and/or insecure protocols is to prevent the use of such protocols from causing the disclosure of confidential information (such as user credentials) that could be used in a cyber attack and/or to prevent the abuse of such protocols as a means for attacking and maliciously manipulating a CDA. The objective of open and/or insecure protocol restrictions is to ensure that their use, if necessary, is limited and controlled in a manner that reduces the likelihood of their being abused.</td>
</tr>
<tr>
<td>Security Functions</td>
<td></td>
</tr>
<tr>
<td>Standards</td>
<td>D.1.4.d8: This technical cyber security control: Configures CDA(s) such that user credentials are not transferred insecure protocols.</td>
</tr>
<tr>
<td>Rating</td>
<td>9.0</td>
</tr>
<tr>
<td>Confidentiality Rating</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Rating</td>
<td>None</td>
</tr>
<tr>
<td>Availability Rating</td>
<td>None</td>
</tr>
</tbody>
</table>

### Consequence Form

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>Unauthorized personnel with access to the network may gain access to or be able to modify sensitive but un protección information or gain access to system resources through the insecure protocols.</td>
</tr>
<tr>
<td>Security Objectives</td>
<td>The purpose of having restrictions on open and/or insecure protocols is to prevent the use of such protocols from causing the disclosure of confidential information (such as user credentials) that could be used in a cyber attack and/or to prevent the abuse of such protocols as a means for attacking and maliciously manipulating a CDA. The objective of open and/or insecure protocol restrictions is to ensure that their use, if necessary, is limited and controlled in a manner that reduces the likelihood of their being abused.</td>
</tr>
<tr>
<td>Confidential Impact</td>
<td>Significant</td>
</tr>
<tr>
<td>Availibility Impact</td>
<td>None</td>
</tr>
<tr>
<td>Integrity Impact</td>
<td>Significant</td>
</tr>
</tbody>
</table>

### Value Provided

This task provides value by explaining why the Standards are necessary.
Map Standards

The following diagram depicts the fourth task in the Compliance Analysis process:

Purpose

The purpose of this step of the methodology is to group Standards within each Compliance Scope and associate the Specific Attribute Values or Inherited Attribute Values that indicate the Standards must be applied.

Analysis Process

Mapping the Standards for each Compliance Scope requires reviewing each Standard and identifying those that have identical dependent Attribute Values and, optionally, are expected to be implemented through similar Controls. There are two different approaches that can be taken to group Standards:

- Focus on the dependent Attribute Values
- Focus on the implementing Controls

The first approach results in the least number of Standards Maps, however, there will still be significant ambiguity within them, the second results in a larger number of Standard Maps, each with
much less ambiguity. Consider the following examples:

**Standard Map: Document and Implement System Hardening**

<table>
<thead>
<tr>
<th>Index</th>
<th>Text</th>
<th>Dependent Attribute Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 5.1 f</td>
<td>This technical cyber security control removes and/or disables software components that are not required for the operation and maintenance of the CDA prior to incorporating the CDA into the production environment. This technical cyber security control documents what components were removed and/or disabled. The software removed and/or disabled includes, but is not limited to:</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>D 5.3 a3</td>
<td>Document the changing or disabling of access to files and functions.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 a1</td>
<td>Documenting the most restrictive mode,</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 a3</td>
<td>Enforcing and documenting the most restrictive operational configuration settings based upon explicit operational requirements.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b1</td>
<td>Establishing and documenting configuration settings for CDAs that reflect the most restrictive mode.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b2</td>
<td>Documenting and approving any exceptions from the most restrictive mode configuration settings for individual components within CDAs based upon explicit operational requirements.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b3</td>
<td>Enforcing the configuration settings in CDAs</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
</tbody>
</table>

**Dependent Attribute Value Focused Standard Map Example**

All of the Standards in this excerpt from the Compliance Scope Direct CDA are dependent on the same Specific (Hardware) Attribute Value, following the first approach would result in all of these Standards grouped into one Standard Map. However, there are two independent mechanisms required to implement these Standards (ambiguity), and that is not clear from this Standard Map.

Multiple Control Maps (discussed in the next analysis step) would be required to disposition this Standard Map, one which required the baseline configuration documentation requirements of:

D 5.1 f    D 5.3 a3    E 10.7 a1    E 10.7 a3    E 10.7 b1    E 10.7 b2

And one that required the system configuration settings configured according to the requirements of:

D 5.1 f    E 10.7 a3    E 10.7 b1    E 10.7 b3

This is of course, the minimal number of Control Maps that would be required. Resources that match this specific Attribute Value may have dissimilar additional specific or inherited Attribute Values that dictated different implementation mechanisms, increasing the number of Control Maps.
The next example shows the second approach, keeping the implementation mechanisms in mind when creating the Standard Maps:

### Standard Map: Document Baseline Configuration

<table>
<thead>
<tr>
<th>Index</th>
<th>Text</th>
<th>Dependent Attribute Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 5.1 f</td>
<td>This technical cyber security control removes and/or disables software components that are not required for the operation and maintenance of the CDA prior to incorporating the CDA into the production environment. This technical cyber security control documents what components were removed and/or disabled. The software removed and/or disabled includes, but is not limited to:</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>D 5.3 a3</td>
<td>Document the changing or disabling of access to files and functions.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 a1</td>
<td>Documenting the most restrictive mode,</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 a3</td>
<td>Enforcing and documenting the most restrictive operational configuration settings based upon explicit operational requirements.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b1</td>
<td>Establishing and documenting configuration settings for CDAs that reflect the most restrictive mode.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b2</td>
<td>Documenting and approving any exceptions from the most restrictive mode configuration settings for individual components within CDAs based upon explicit operational requirements.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
</tbody>
</table>

### Implementation Mechanism Focused Standard Map Example-1

### Standard Map: Harden System

<table>
<thead>
<tr>
<th>Index</th>
<th>Text</th>
<th>Dependent Attribute Values</th>
</tr>
</thead>
<tbody>
<tr>
<td>D 5.1 f</td>
<td>This technical cyber security control removes and/or disables software components that are not required for the operation and maintenance of the CDA prior to incorporating the CDA into the production environment. This technical cyber security control documents what components were removed and/or disabled. The software removed and/or disabled includes, but is not limited to:</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 a3</td>
<td>Enforcing and documenting the most restrictive operational configuration settings based upon explicit operational requirements.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b1</td>
<td>Establishing and documenting configuration settings for CDAs that reflect the most restrictive mode.</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
<tr>
<td>E 10.7 b3</td>
<td>Enforcing the configuration settings in CDAs</td>
<td>Specific Attribute Value: End-User Defined Software Configuration = True</td>
</tr>
</tbody>
</table>

### Implementation Mechanism Focused Standard Map Example-2
Multiple Control Maps may still be necessary to fully disposition both of these Standard Maps, depending on the characteristics of the Resources in scope. However, the context of the Standard Maps eliminates all ambiguity in these Standards. It is clear what the focus of each of the Standard Maps are in both of them by their titles, regardless of the multiple concepts discussed within some of the individual Standards therein.

**cmplid:// Operation**

Standard Maps are generally created by selecting a Standard from the table in a given Compliance Scope’s Standards tab, though they can be created from the main table. NOTE: When creating a Standard Map from the main table the Standards presented to the user will not be filtered until a Compliance Scope is selected.
Value Provided

This task provides value by explaining *what Resources the Standards will be applied to.*
Document Resource Prototypes

The following diagram depicts the fifth task in the Compliance Analysis process:

![Diagram of Document Resource Prototypes](image)

**Purpose**

The purpose of this step of the methodology is to document similarities between Resources of a given Resource Type and associate required Attribute Types to these Resource Prototypes. The use of Resource Prototypes allows for inheritance of the Attribute Values associated with the prototype for each Resource instance of the Resource Prototype. This is an efficiency-enabler that significantly reduces the ongoing Resource management effort within cmplid://.

**Analysis Process**

Documenting Resource Prototypes focuses solely on the Resources within scope of the Security Program and identifying consistent Attribute Types for a given Resource Type. Of the six basic interrogatives: *who, what, when, where, why, and how*; only *what a resource is*, is capable of being described by an Attribute for a Resource Prototype. Consider the following examples

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Applicability</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains Communications Ports</td>
<td>Resource Prototype</td>
<td>Describes what a hardware resource is</td>
</tr>
<tr>
<td>Connected to Network</td>
<td>Resource</td>
<td>Describes how (or where) a resource is used</td>
</tr>
<tr>
<td>Contains Sensitive Information</td>
<td>Resource</td>
<td>Describes how a resource is used</td>
</tr>
<tr>
<td>End User Defined Logical Permissions</td>
<td>Resource Prototype</td>
<td>Describes what a hardware resource is</td>
</tr>
<tr>
<td>Local Storage and Processing of Audit Logs</td>
<td>Resource</td>
<td>Describes how a resource is configured</td>
</tr>
<tr>
<td>Multi-User Mixed Function OS</td>
<td>Resource Prototype</td>
<td>Describes what a hardware resource is</td>
</tr>
</tbody>
</table>
Compliance Analysis Method

<table>
<thead>
<tr>
<th>Attribute Type</th>
<th>Applicability</th>
<th>Rationale</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted End-User Defined Configuration</td>
<td>Resource</td>
<td>Describes how a resource is configured</td>
</tr>
<tr>
<td>Supports Logical User Authentication</td>
<td>Resource</td>
<td>Describes how a resource is configured</td>
</tr>
<tr>
<td>Is located within a Vital Area</td>
<td>Resource</td>
<td>Describes where a resource is used</td>
</tr>
</tbody>
</table>

Attribute Applicability Examples

Identification of the Attribute Types that apply to Resource Prototypes introduces great efficiencies into ongoing security management activities. Resource Prototypes can be defined and all of the Resource Prototype Attributes can be documented for them once. Two identical digital transmitters may used by different teams, at different times, in different locations, for different purposes, and in different ways, but they will always have the same Resource Prototype Attributes. Those Resource Prototype Attributes can be documented and every transmitter added to the cmplid:// database can inherit those values, ensuring consistent understanding of Resources throughout the organization.

A review of the Resources within scope will provide the similarities, consistent with the Resource Prototype Attributes identified for the Resource Type, that allow Resource Prototype to be defined.

cmplid:// Operation

Attribute Types are associated with Resource Prototypes through the APPLIES TO radio button widget on the Attribute Type form:

---

5 Meaning they have the same Resource Prototype Attribute Values, not necessarily that they are the same make and model
Value Provided
This task provides value by explaining *what categories of Resources exist.*
Map Controls
The following diagram depicts the final task in the Compliance Analysis process:

Purpose
The purpose of this step of the methodology is to document the detailed implementation mechanisms, called Controls within cmplid://, that will be used to fulfill the Standards within the context of a specific Standard Map.

Analysis Process
Mapping Controls is a similar process to mapping Standards, the key differences is the additional information that can be associated with Control Maps. For a given Standard Map all of the various mechanisms that will be used to fulfill the Standards must be documented within a Control Library. Users are encouraged to use industry guidance documents such as NIST SP 800-53, the SANS Top 20 Controls and other sources to develop detailed implementation statements for each Standard Map.

Control Maps may be designated as either DIRECT implementations, ALTERNATE implementations, or INHERITED implementations of the Standards. Control Maps may also implement all of the Standards or only some of the Standards for their related Standard Map.
Specific Attribute Values and Inherited Attribute Values may be identified as limiting the Resources the Control Map is used for and Control Maps may be further limited to only apply to Resources with specified Resource Prototypes.

Default Comments and Initial Assessment Responses may be provided for efficient execution of Compliance Assessments. For those Control Maps that are known to always be have the Initial Assessment Response status, they may be designated as Auto Answered to eliminate the need to respond to the Control Map during a Compliance Assessment.

**cmplid:// Operation**

Control Maps are created through the Control Map form available from the Standard Map table for a given Compliance Scope:

**Control Map Form**

**Value Provided**

This task provides value by explaining how the Standards will be implemented and optionally how they can be verified and validated.