NEI 13-10 [Revision 0]

Cyber Security Control Assessments

January 2014

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

NEI 13-10 [Revision 0]

Nuclear Energy Institute

Cyber Security Control Assessments

January 2014

Nuclear Energy Institute, 1201 F Street N. W., Suite 1100, Washington D.C. (202.739.8000)

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

ACKNOWLEDGMENTS

This document has been prepared by the nuclear power industry with input and guidance from the United States Nuclear Regulatory Commission. While many individuals contributed heavily to this document, NEI would like to acknowledge the significant leadership and contribution of the following individuals.

Executive sponsor:
James Meister Exelon Corporation

Core project team:
Patrick Asendorf Tennessee Valley Authority
William Gross Nuclear Energy Institute
Christopher Kelley Exelon Corporation
Jay Phelps South Texas Project Nuclear Operating Company

The core project team was supported by:
Nathan Faith Exelon Corporation
Jan Geib South Carolina Electric & Gas Company
James Shank PSEG Services Corporation
Laura Snyder Tennessee Valley Authority

Industry review team:
Glen Frix Duke Energy Corporation
Matthew Coulter Duke Energy Corporation
Geoff Schwartz Entergy

NOTICE

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

EXECUTIVE SUMMARY

When the methodology to address cyber security controls was developed in the template for the cyber security plan, the industry believed there would be small handfuls of digital assets (CDAs) that would require a cyber security assessment. However, NEI understands that plants, including those with no digital safety-related systems, have identified many hundreds if not thousands of CDAs. Included are assets that range from those directly related to operational safety and security to those that, if compromised, would have no direct impact on operational safety, security, or emergency response capabilities.

This guidance document was developed to streamline the process for addressing the application of cyber security controls to the large number of CDAs identified by licensees when conducting the analysis required by 10 CFR 73.54(b). The goal is to minimize the burden on licensees of complying with their NRC approved cyber security plan, while continuing to ensure that the adequate protection criteria of 10 CFR 73.54 are met.

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

TABLE OF CONTENTS

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

CYBER SECURITY CONTROL ASSESSMENTS

1 INTRODUCTION

1.1 BACKGROUND

Title 10 of the Code of Federal Regulations, Part 73, "Physical Protection of Plants and Materials," Section 73.54, "Protection of Digital Computer and Communication Systems and Networks," requires that licensees provide high assurance that digital computer and communication systems and networks are adequately protected against cyber attacks, up to and including the design basis threat as described in 10 CFR 73.1.

10 CFR 73.54 requires that each licensee currently licensed to operate a nuclear power plant submit a cyber security plan (CSP) for Commission review and approval. Current applicants for an operating license or combined license must submit with or amend their applications to include a cyber security plan.

Further, 10 CFR 50.34(c)(2) states in part that "Each applicant for an operating license for a utilization facility that will be subject to the requirements of 10 CFR 73.55 of this chapter must include a cyber security plan in accordance with the criteria set forth in 10 CFR 73.54 of this chapter." The Cyber Security Plan establishes the licensing basis for the Cyber Security Program.

The purpose of the Cyber Security Plan is to provide a description of how the requirements of 10 CFR 73.54, "Protection of digital computer and communication systems and networks" (Rule) are implemented.

Section 3.1.6 of the licensee's CSP describes how that licensee addresses cyber security controls for digital assets that have been identified for protection against cyber attacks. NEI 13-10 provides guidance licensees may use to streamline the process to address cyber security controls for CDAs consistent with the methodology described in CSP Section 3.1.6.

1.2 SCOPE

This document provides guidance licensees may use to streamline the process for addressing the application of cyber security controls to those digital assets that a site specific analysis, performed in accordance with the requirements of 10 CFR 73.54 (b)(1), determined require protection from cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

1.3 PURPOSE

The purpose of this document is to provide guidance licensees may use to address cyber security controls for CDAs consistent with the methodology described in Section 3.1.6 of the Cyber Security Plan.

2 USE OF THIS DOCUMENT

The following method may optimize the use of the guidance in this document:

a) PRINT this document.

b) GATHER CDA-related information documented when implementing CSP Sections 3.1.3, 3.1.4, and 3.1.5.

c) PERFORM a consequence assessment of CDAs using the guidance in Section 3 of this document.

d) USE the guidance in Sections 3, 4, and 5 of this document to divide the CDAs identified in Milestone 2 into two categories, direct and indirect CDAs, for streamlining the application of cyber security controls to identified CDAs consistent with Section 3.1.6 of the CSP.

e) DOCUMENT the assessment and RETAIN the documents in accordance with the CSP.

3 CONSEQUENCE ASSESSMENT OF CDAS

Consequence Assessment provides a method to assess alternate means of protecting CDAs from cyber attacks. Licensees may use the guidance detailed in Table 1, "Consequence Assessment," to determine which of the approaches described in this document may be used to assess alternate controls and streamline the process of addressing the application of cyber security controls to CDAs. It is intended that any CDA subject to this assessment would proceed to one of the two exit states illustrated in Figure 1.

Consequence Assessment may result in the application of certain minimum cyber security controls to specific identified CDAs. These minimum cyber security controls are described in Section 5 of this document, "Minimum Cyber Security Protection Criteria." The Consequence Assessment and the minimum requirements in Section 5 may be used as a means to address the alternative analysis requirements specified in Section 3.1.6 of the CSP. The impact of the cyber compromise of identified CDAs can be divided into two categories: direct and indirect impacts to SSEP functions.

Consequence Assessment also provides a method to assess alternate means of protecting EP functions, including offsite communications. The methodology of assessing alternate means for EP functions is described in Section 4, "EP Function Maintained through Alternate Means." For CDAs associated with EP functions, the licensee may perform and document an analysis for the use of alternative controls or countermeasures as described in Table 2 of this document.

Consistent with Section 4.4 and 4.5 of their cyber security plans, licensees will establish a program to ensure that CDAs are continuously protected from cyber attacks including implementing any necessary measures to address new vulnerabilities in accordance with the CSP.

3.1 INDIRECT CDAS

Indirect CDAs are those CDAs that cannot have a near-term impact on or degrade SSEP functions prior to their compromise or failure being detected and compensatory measures being implemented by a licensee. Specifically, indirect CDAs include only those CDAs that meet all three of the following criteria: (1) if compromised, would not have a direct impact on systems and equipment that perform Safety or Security functions; (2) are not indicators/annunciators solely relied-on for making Safety or Security-related decisions; and, (3) the compromise of which can be detected, and compensatory measures taken, prior to an adverse impact to direct CDAs or Safety or Security functions.

For indirect CDAs only, licensees may comply with the requirements of Section 3.1.6 of their Cyber Security Plans by implementing the guidance set forth in Table 1.

3.2 DIRECT CDAS

Direct CDAs include those CDAs that, if compromised, could result in an immediate 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. Direct CDAs are those CDAs that have not been determined to be indirect CDAs.

Licensees may use streamlining techniques, when applicable, for addressing the applicability of security controls to direct CDAs. These include the use of common controls, control inheritance, and type assessments when such measures adequately address attack pathways and vectors associated with the direct CDAs. These techniques can reduce the effort required for addressing protections for direct CDAs.

In general, the term "common control" means a particular security control is applied to multiple CDAs. The term "technical inheritance" refers to a situation in which a CDA receives protection from technical security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by another CDA. Finally, the term "type assessment" or "grouping of CDAs" refers to a situation in which multiple CDAs share a substantially similar security posture. For type assessments, a single assessment is created noting the differences, if any, between the devices.

In cases where a technical control cannot be implemented, the threat vector associated with the technical control exists, and the CDA is unable to inherit the technical control from another CDA, an alternate control (including administrative controls if alternative technical security controls cannot be used to address the security controls) can be used to mitigate the associated risk. The alternate control must provide the same degree of protection found in the original control.

Redundancy should not be used as a factor in determining if a CDA is an indirect or direct CDA.

Some examples of direct CDAs for which the criteria in Section 3.1 of this document do not apply include:

- Digital Emergency diesel generator governor;
- Digital turbine driven Auxiliary Feedwater pump governors;
- RCS pressure instruments with control functions and/or input to the Reactor Protection System for initiation of a plant trip;
- CDAs identified in accordance with Milestone 6;
- CDAs that could cause a 300 MW or greater electric power change in less than 15 minutes;
- Main Feedwater Regulating valve digital positioners;
- Digital EHC Control Systems;
- Digital Feedwater Control Systems; and
- Security computer alarm station server(s).

Table 1, Consequence Assessment

Figure 1 Question	Guidance
1.1	Is the CDA associated with EP functions, including offsite communications, or are EP support systems or equipment for EP-related CDAs? If YES, proceed to question 1.2 of this table. If NO, proceed to question 1.4 of this table.
1.2	Has an assessment using the process described in Section 4 and illustrated in Figure 2 determined that the EP functions are maintained through alternate means? If YES, proceed to 1.3 of this table. If NO, proceed to 1.4 of this table.
1.3	Are minimum cyber security protection criteria d, e, f, and g, described in Section 5 of this document in place for the EP-related CDAs? If YES, current cyber security controls are adequate to meet CSP Section 3.1.6. End assessment here. If NO, implement minimum cyber security protection criteria d, e, f, and g, described in Section 5 of this document or proceed to 1.4 of this table.
1.4	Has the licensee determined that the CDA is an indirect CDA as described in Section 3.1 of this document? If YES, proceed to 1.5 of this table If NO, proceed to 1.7 of this table.

Figure 1 Question	Guidance
1.5	Has the licensee documented, and implemented the following? 1. Determine the minimum time period required, once an indirect CDA has been compromised, for both detection and compensatory measures to take place prior to an adverse impact to direct CDAs or SSEP functions (in all operating modes). The minimum time period required may be based on existing analyses. 2. Document a method, and associated implementing procedures, for the detection of an indirect CDA compromise and/or failure within the minimum time period. 3. Document implementation strategies for compensatory measures to eliminate the adverse impact to direct CDAs or SSEP functions in all operating modes. 4. Document the technical justification for how the detection activities and compensatory measures (i.e., Steps 2 and 3 above) for the indirect CDA compromise and/or failure are sufficient and will occur within the minimum time period determined by the licensee in Step 1. If YES then proceed to 1.6 of this table. If NO, proceed to 1.7 of this table.
1.6	Are the minimum cyber security protections described in Section 5 of this document in place for the CDA? If YES, then current cyber security controls are adequate to meet CSP Section 3.1.6. End assessment here. If NO, implement the minimum cyber security protection criteria described in Section 5 of this document or proceed to 1.7 of this table.
1.7	Address the cyber security controls as referenced in Section 3.1.6 of the licensee's CSP.

4 EP FUNCTION MAINTAINED THROUGH ALTERNATE MEANS

As specified in Section 3.1.6 of licensees' NRC-approved CSPs, a licensee has the flexibility to perform and document an analysis for the implementation of alternative controls and/or countermeasures for EP CDAs that eliminate threat/attack vector(s) associated with, and that provide at least the same degree of cyber security protection as one or more of the corresponding cyber security controls enumerated in Appendices D and E of NEI 08-09, Revision 6. The licensee must perform and document an analysis for the use of alternative controls or countermeasures as described in Table 2 to address the cyber security controls as specified in Section 3.1.6 of the licensee's NRC-approved CSPs. Table 2 is illustrated in Figure 2, which can be found in Appendix A to this document. This guidance may be used for CDAs associated with EP functions that are not otherwise also relied on for safety-related, important-to-safety, or security functions.

Where an assessment using the guidance in Table 2 determines that 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, then the CDAs may be considered adequately protected. The guidance in Table 2 can be used to determine whether an alternative means allows the EP equipment to remain operable to perform the intended emergency response function despite cyber attacks.

Changes to measures credited as providing an alternate method of maintaining the EP function must be subject to review (e.g., existing program reviews, procedure revision reviews, or use of configuration management) to ensure the changes would not challenge the adequacy of the alternate method.

Table 2, Alternative Means Assessment for EP CDAs

Figure 2 Question	Guidance
2.1	Are alternate means available for performing the intended EP function, including offsite communications? If YES, proceed to question 2.2 of this table. If NO, proceed to 1.4 in Table 1 or implement alternate means and then proceed to 2.2 of this table.

Figure 2 Question	Guidance
2.2	Is one or more of the alternate means administrative, non-digital, or if digital are adequately independent? If YES, proceed to question 2.3 of this table. If NO, proceed to question 1.4 of Table 1. Two means would be considered adequately independent if they do not rely on equipment that if compromised by cyber attacks would adversely impact both means of performing the EP function (e.g., a PBX-based phone system vs. satellite phones, data obtained by MET tower vs. data obtained through a weather service, data obtained from SPDS vs. received via fax, etc.). Administrative methods, including actions performed by personnel, can be considered as an alternate means provided they do not depend on identified CDA(s) for which controls have not been assessed.
2.3	Is the alternate means documented? If YES, proceed to 2.4 of this table. If NO, proceed to 1.4 in Table 1 or document the alternate means and then proceed to 2.4 of this table. **Note: the means must be documented in a plan, policy, or implementing procedure.**
2.4	Is the equipment that a compromise of the CDA would impact periodically checked to ensure the equipment is capable of performing its intended function and an appropriate response initiated, if needed? Specifically, can a cyber attack that would prevent the EP-related equipment from performing its intended function be detected and responded to prior to an adverse impact on the EP-related function during a radiological emergency? If YES, proceed to 2.5 of this table. If NO, proceed to 1.4 in Table 1 or implement detection and response measures and then proceed to 2.5 of this table. Measures for detection and response may be technical, procedural, or administrative, and could include periodic functional or availability testing (e.g., existing periodic operability tests performed on plant systems or equipment). The measures in place must be performed at a frequency to ensure the ability to employ the alternate means in a timeframe sufficient to mitigate the adverse consequences of a cyber attack.

Figure 2 Question	Guidance
2.5	Are appropriate facility personnel trained to use the alternate method? If YES, then the function is maintained through alternate means, proceed to 1.3 in Table 1. If NO, proceed to 1.4 in Table1 or perform training of appropriate facility personnel and then proceed to 1.3 in Table 1.

5 MINIMUM CYBER SECURITY PROTECTION CRITERIA

An assessment using the guidance in Section 3.1 permits licensees to demonstrate that alternative controls and countermeasures are sufficient to provide adequate protection of indirect CDAs. For these CDAs, the minimum set of cyber security protections are sufficient to provide high assurance that the CDAs are adequately protected against cyber attacks up to and including the design basis threat as described in 10 CFR 73.1.

Where these minimum cyber security criteria are not met, the licensee must document and implement additional cyber security controls to ensure adequate protections are in place for the CDA. These additional cyber security controls are implemented using the methodology in CSP Section 3.1.6.

Changes to the minimum cyber security controls must be reviewed in accordance with the CSP to ensure the indirect CDAs remain adequately protected from cyber attacks.

Where a licensee chooses to credit these minimum cyber security controls for an indirect CDA, the licensee must confirm these baseline minimum controls criteria are met.

An indirect CDA may be considered to be adequately protected from cyber attacks if all of the following minimum criteria are met:

a) The indirect CDA, as identified using the analysis set forth in Section 3.1 of this document, is located within a Protected or Vital area or the cyber security controls in NEI 08-09, Appendix E, Section E.5 “Physical and Operational Environment Protection,” is addressed.

b) The indirect CDA and any interconnected assets do not have wireless internetworking communications technologies.

c) The indirect CDA and any interconnected assets are either air-gapped or isolated by a deterministic isolation device.

d) Use of portable media and mobile devices is controlled according to NEI 08-09 D1.19 in order to ensure the indirect CDA will not be compromised as a result of the use of portable media and mobile devices.

e) Changes to the indirect CDA are evaluated before implementation in accordance with CSP Section 4.5, “Addition and Modification of Digital Assets.”

f) The indirect CDA, or the interconnected equipment that would be affected by the compromise of the indirect CDA, is periodically checked to ensure the equipment is capable of performing its intended function. These checks could include any routine check performed to determine the functional or operational availability of the equipment. The periodicity of checks must be sufficient to ensure detection and mitigation of cyber attacks prior to an adverse impact to SSEP functions resulting from cyber attacks.

g) Ongoing Monitoring and Assessment in accordance with CSP is performed.

APPENDIX A – FIGURES

Appendix A provides figures illustrating the guidance in Sections 3 and 4 of this document.

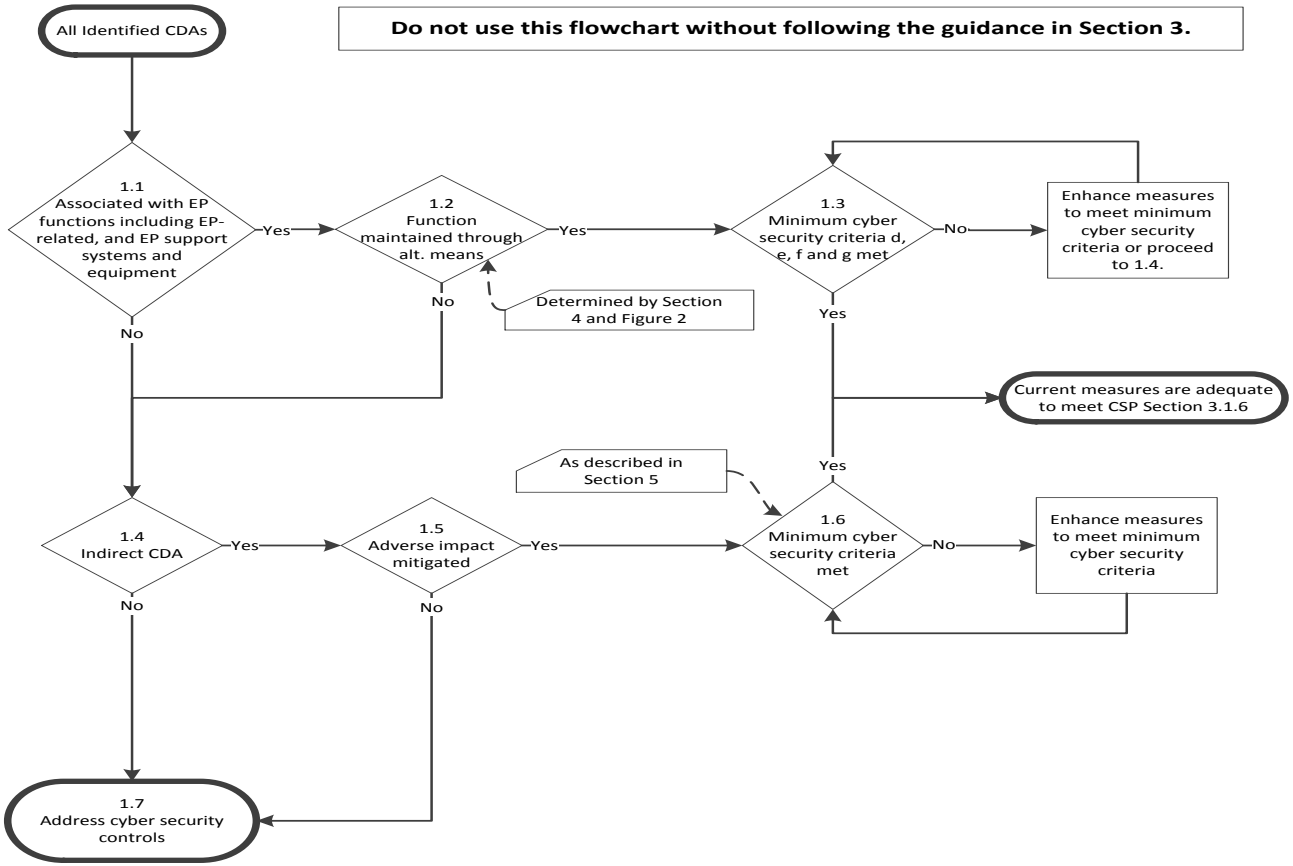

Figure 1 – Consequence Assessment

[THIS PAGE IS LEFT BLANK INTENTIONALLY]

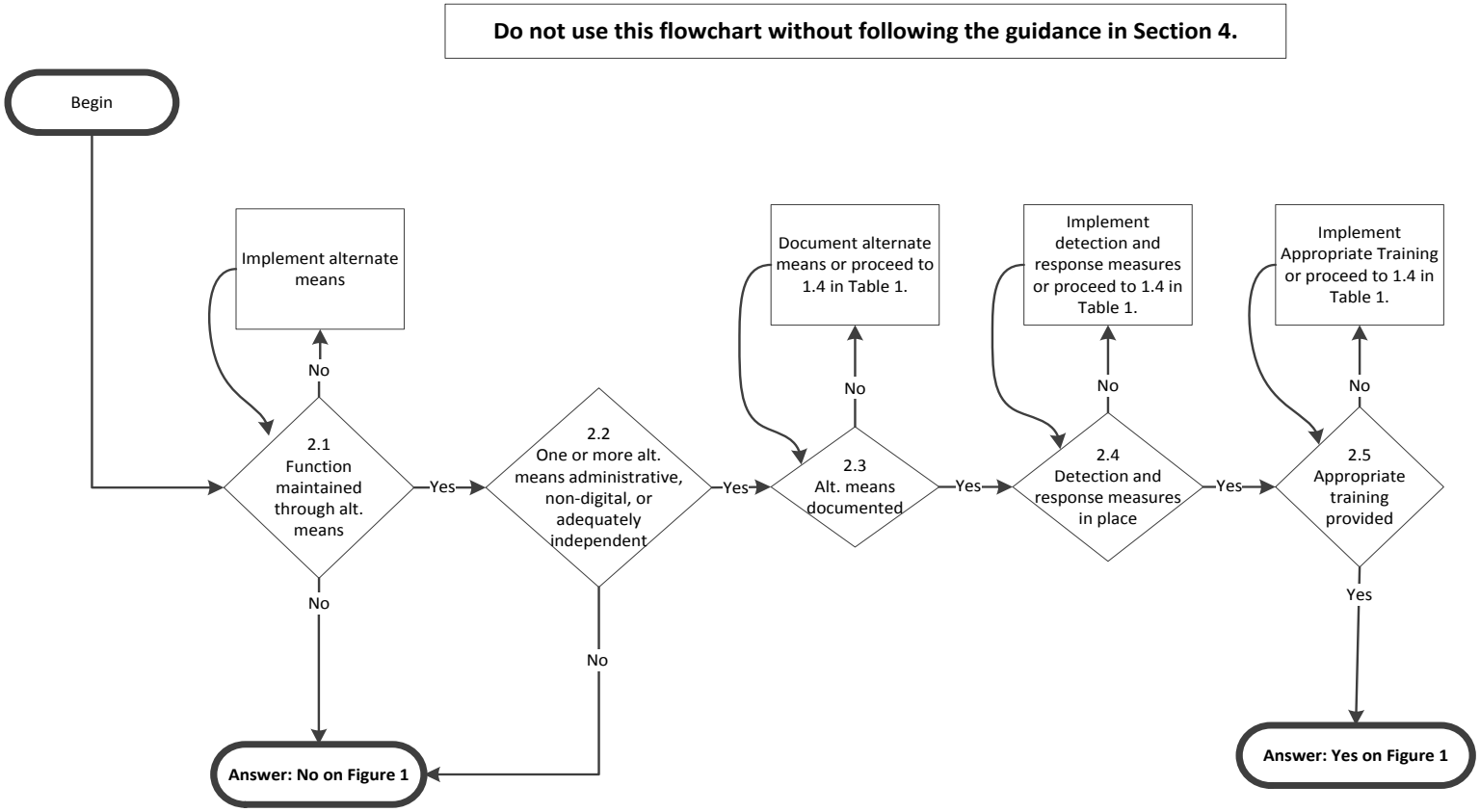

Figure 2 – Alternative Means Assessment for EP