Our Future Health

Trusted Research Environment (TRE) Accreditation Scoping Guide

Version 1.0 January 2023

This document is intended to provide guidance to help applicants identify systems that, at a minimum, need to be included in scope for their TRE Accreditation application: self-assessment questionnaire Applicant Details Part 3.

Introduction

The best practice approach is to assume that all systems, components, physical locations, business processes, and users are in scope until verified otherwise.

This guidance is intended for any applicants looking to understand scoping and segmentation principles when applying to accredit their TRE.

Scoping and Segmentation

Scoping involves the identification of components, physical locations, business processes, and users that reside within, interact with, or could otherwise access the TRE. Improper scoping (deciding something is out of scope without proper verification) can cause delays to an application while the scope is redefined.

Segmentation involves the implementation of technical controls to separate in-scope systems from out-of-scope systems. Segmentation can consist of logical controls, physical controls, or a combination of both and is achieved via purpose-built controls that specifically create and enforce separation to prevent exposing research data. To be effective, scoping and segmentation require careful planning, design, implementation, and monitoring.

The intent of segmentation is to prevent out-of-scope systems from being able to communicate with systems in the TRE or impact the security of the TRE. Segmentation is typically achieved by technologies and process controls that enforce separation between the TRE and out-of-scope systems. When properly implemented, an out-of-scope system or component cannot impact the security of the TRE, even if an attacker obtained privileged access on that out-of-scope system or component. Note that connectivity or access is allowed into the TRE from systems outside of the TRE. However, all such connectivity is in scope.

When properly implemented, network segmentation is one method that defines a boundary of the TRE, for which systems or components residing inside are considered in scope. Other methods may also be effective at defining the boundary of the TRE.

Service Providers and other Third Parties

In addition to including internal systems and networks in scope, all connections from third-party entities—for example, business partners, entities providing remote support services, and other service providers—need to be identified to determine inclusion for the TRE accreditation application. Once the in-scope connections have been identified, the applicable controls must then be implemented.

Similarly, if an entity outsources in-scope functions or facilities to a third party or utilizes a third-party service that impacts how it meets the application requirements, the applicant will need to work with the third party to ensure the applicable aspects of the service are included in scope. It is also important for both parties to clearly understand which requirements are being provided by the service provider and which are the responsibility of the applicant using the service.