CHEMICAL SECURITY SEMINARS

Virtual Expo

CISA's Cybersecurity Evaluation Tool (CSET)

Steven Geraldo – Program Manager, Vulnerability Management Department, CISA Cybersecurity

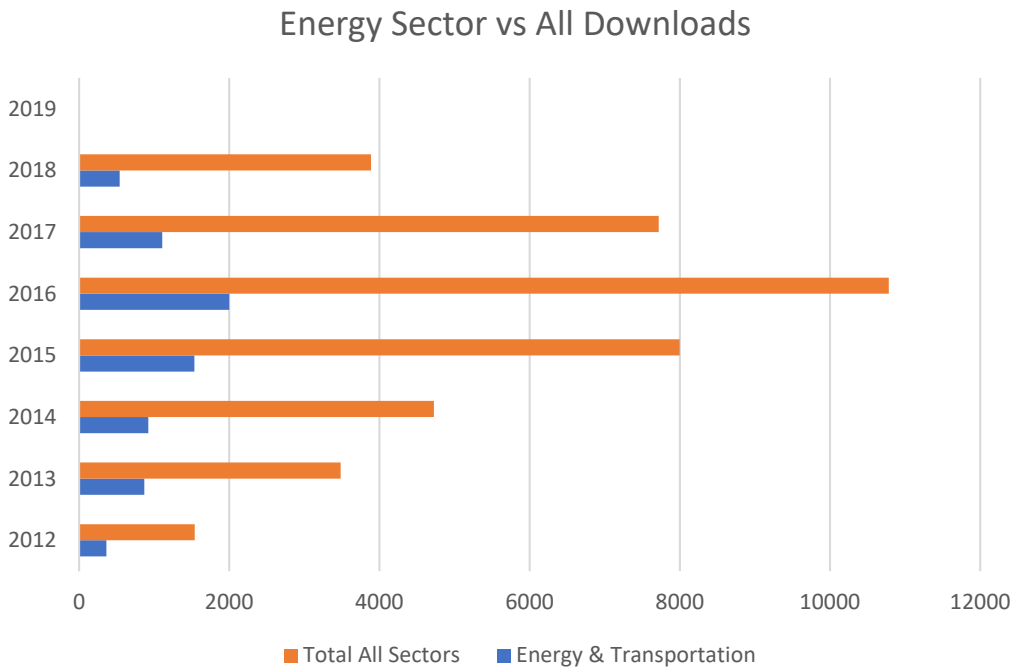
Randy Woods – Senior CSET Engineer, Idaho National Laboratory, Department of Energy

#ChemicalSecurity

CYBERSECURITY EVALUATION TOOL

CSET Usage

- 14 years
- 41,211 downloads from 2012 -2018
- 10,389 downloads for 2019
- 1,438 downloads for 2020




Where do I start?
Where do I stand now?
What are my priorities?

CSET Basis

Requirements derived from industry standards

NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems Revisions 3, 3 Appendix I (ICS Controls), 4, and 4 Appendix J
TSA Pipeline Security Guidelines	Transportation Security Administration (TSA) Pipeline Security Guidelines
NERC Critical Infrastructure Protection (CIP)	Reliability Standards CIP-002 through CIP-009, Revisions 3 and 4 Reliability Standards CIP-002 through CIP-011, Revision 5, Revision 6
DoD Instruction	**8500.2** Information Assurance Implementation **8510.01** Risk Management Framework
NIST Special Publication 800-82	Guide to Industrial Control Systems (ICS) Security, Revisions 1 and 2
Nuclear	**NRC Reg. Guide 5.71** Cyber Security Programs for Nuclear Facilities **NEI 08-09:** Cybersecurity Plan for Nuclear Power Reactors
CFATS RBPS 8- Cyber	Chemical Facilities Anti-Terrorism Standard, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27
NIST Cybersecurity Framework	Executive Order 13636, “Improving Critical Infrastructure Cybersecurity,” Cybersecurity Framework V1.1
CNSSI 1253 and Draft ICS Overlay	Committee on National Security Systems Instruction (CNSSI) No. 1253, with Draft Industrial Control Systems Overlay

CSET Capabilities

What CSET CAN do:

- Provide a consistent means of evaluating a control system network as part of a comprehensive cybersecurity assessment
- Specify cyber security recommendations
- Report using standards-based information analysis
- Provide a baseline cybersecurity posture

What CSET CAN'T do:

- Validate accuracy of user inputs
- Ensure compliance with organizational or regulatory cybersecurity policies & procedures
- Ensure implementation of cybersecurity enhancements or mitigation techniques
- Identify all known cybersecurity vulnerabilities

Assessment Team

A TEAM of participants is required to perform a successful assessment

Type of Participant	Knowledge
Control Systems Engineer	Control systems
Configuration Manager	Systems management
Operations Manager	Business operations
IT Network Specialist	IT infrastructure
IT Security Officer	Policies & procedures
Risk Analyst or Insurance Specialist	Risk

Assessment Process

Basic steps in the assessment

Free Download

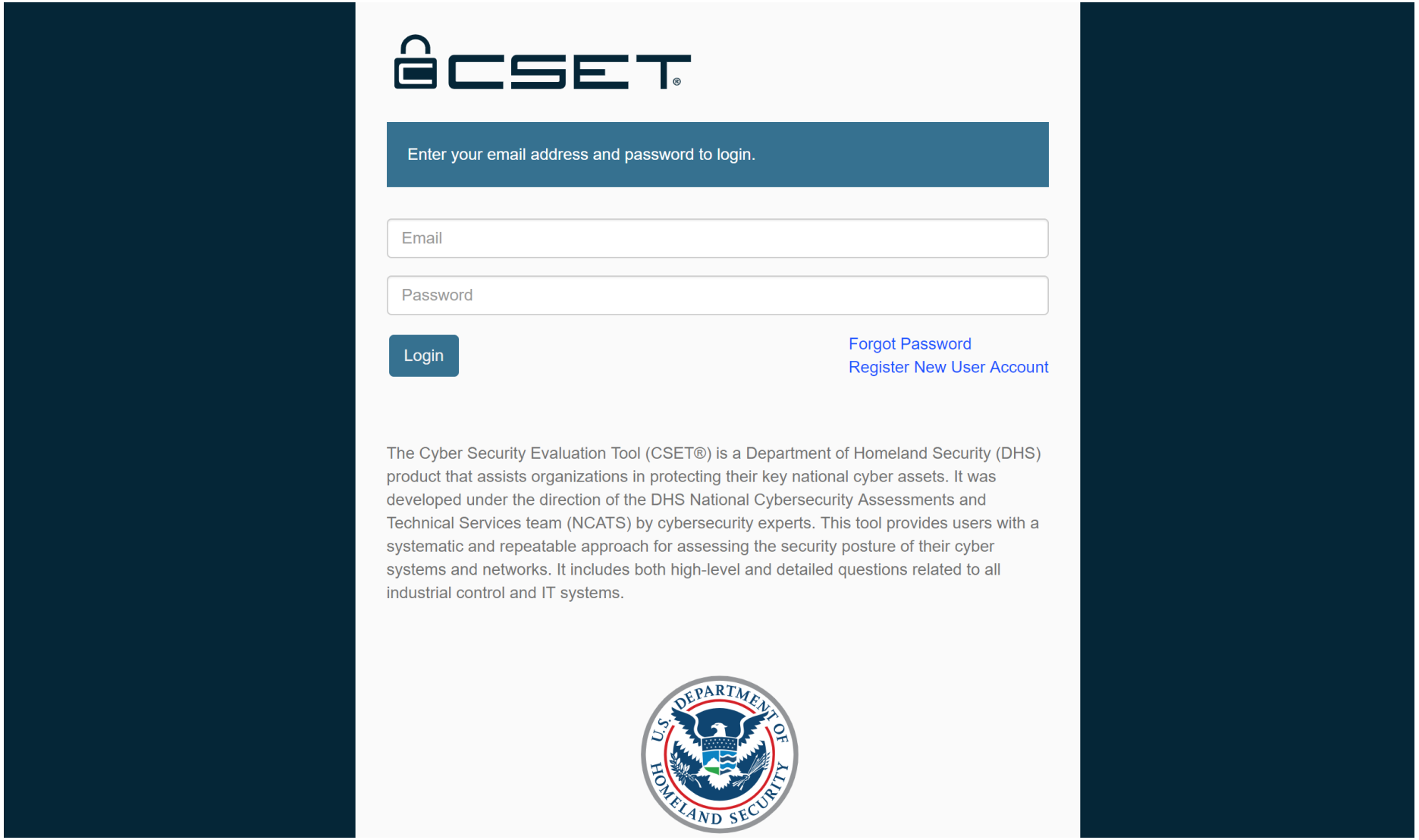
For the latest web application:

https://github.com/cisagov/cset

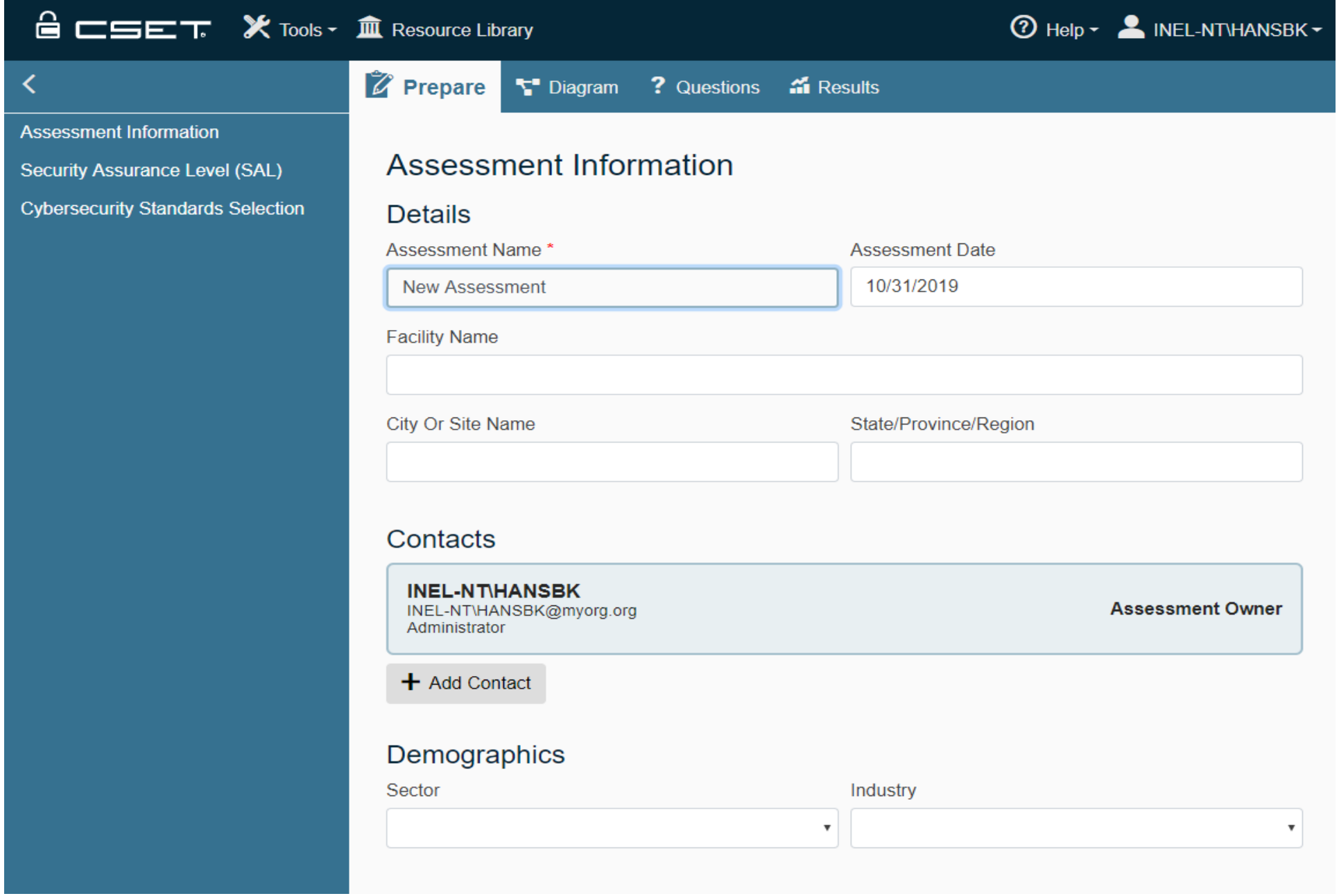
For old desktop versions:

https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

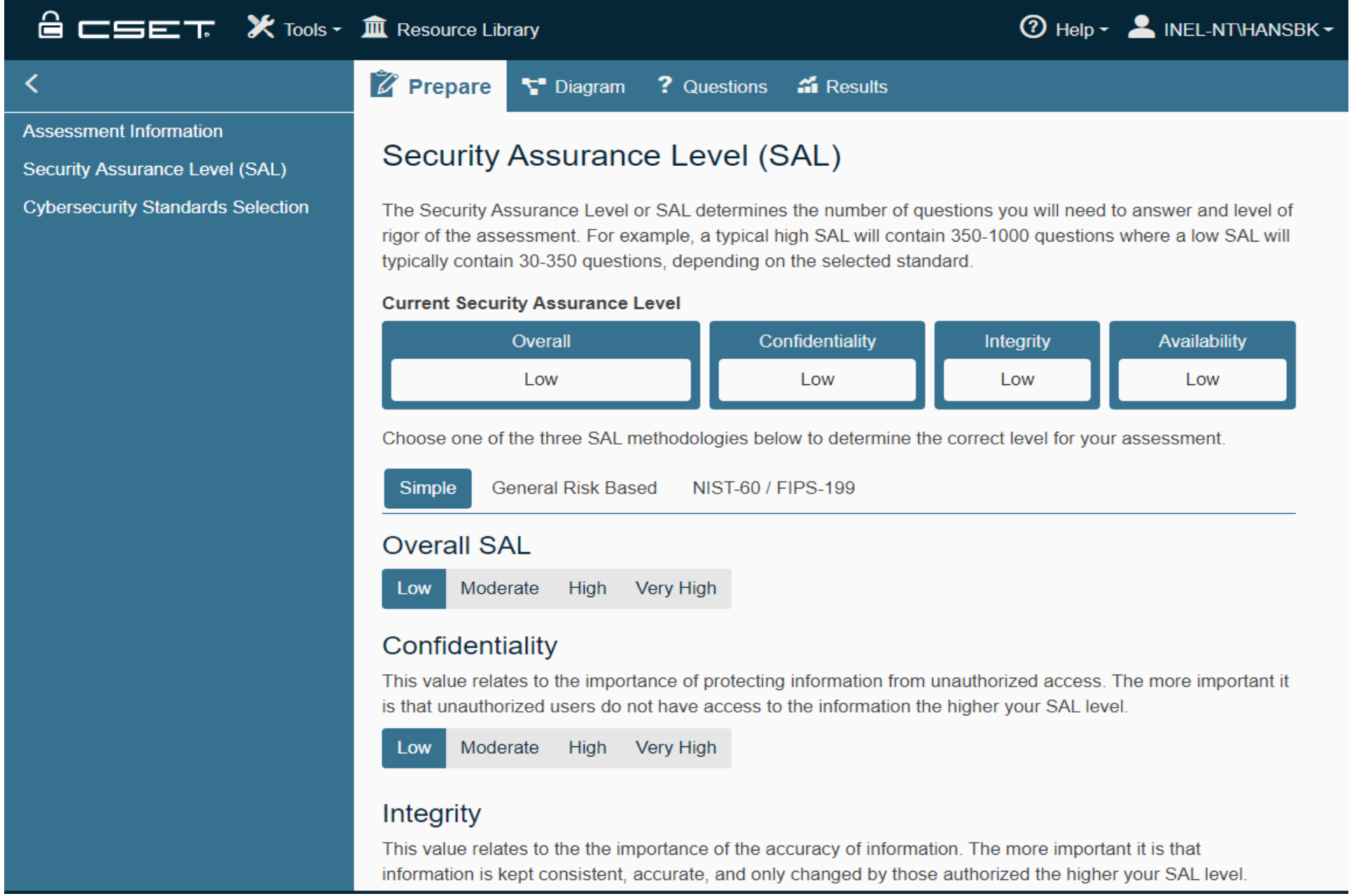
Live Demo



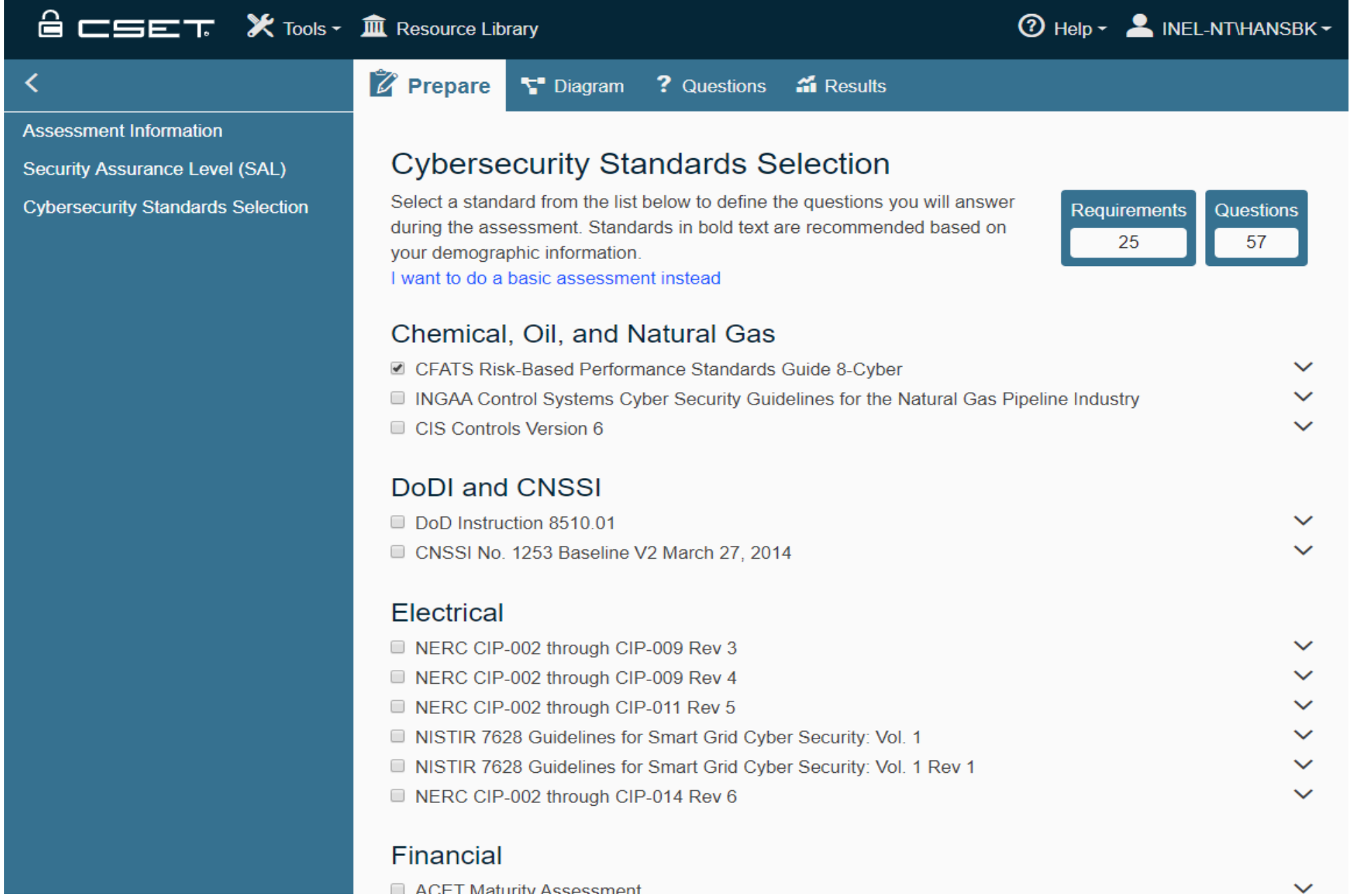
Home Page



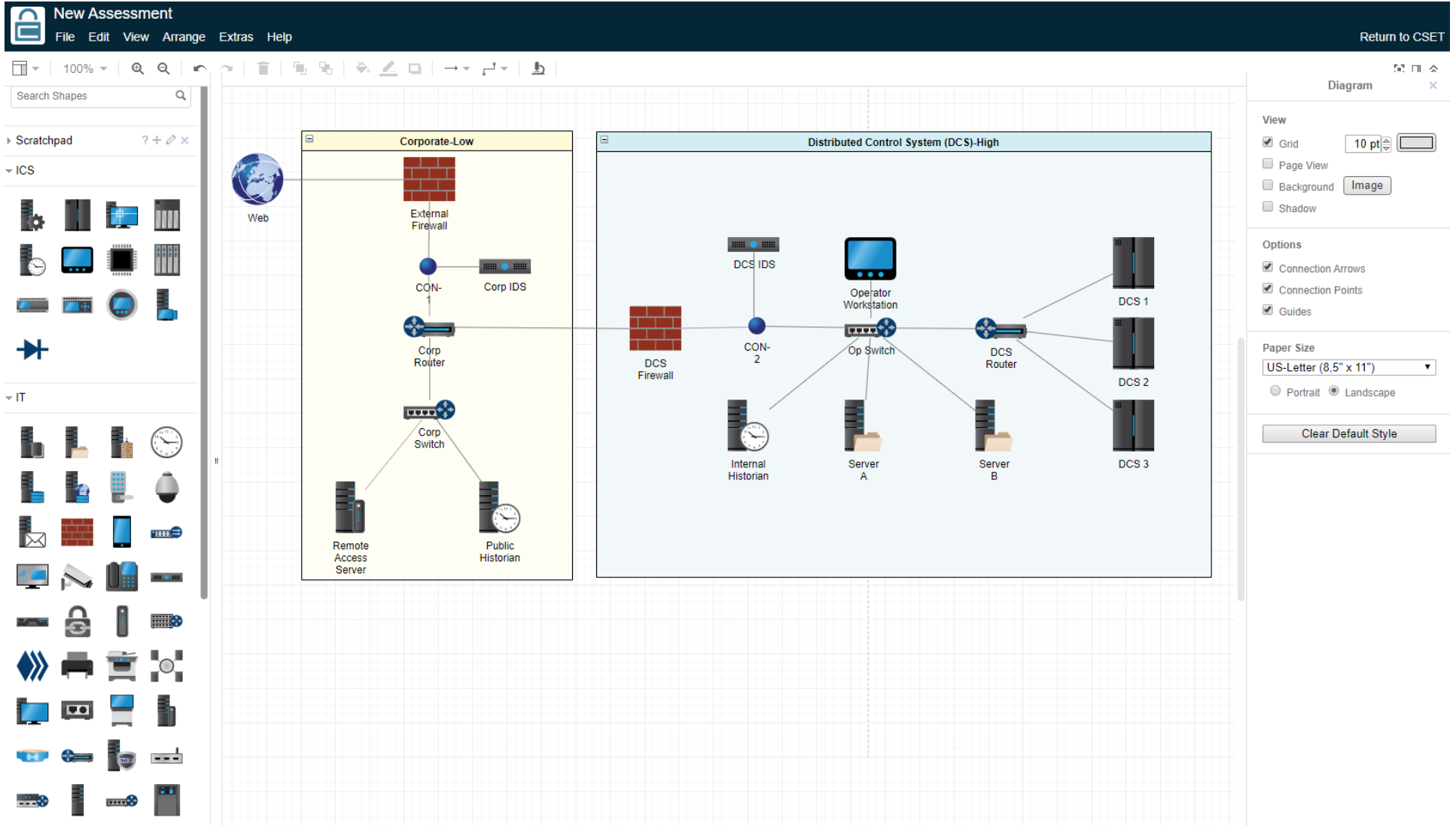
Main Navigation



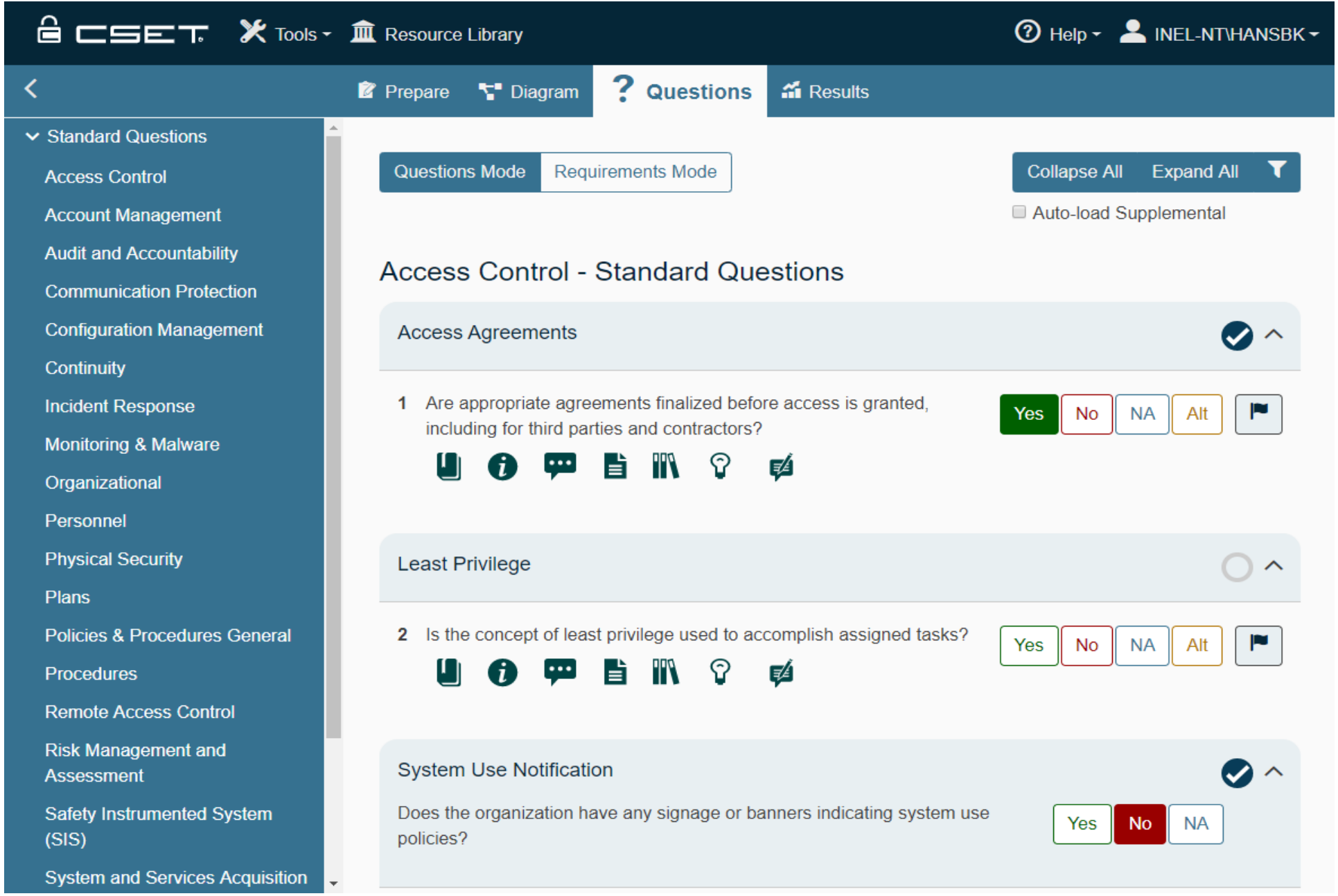
SAL Selection

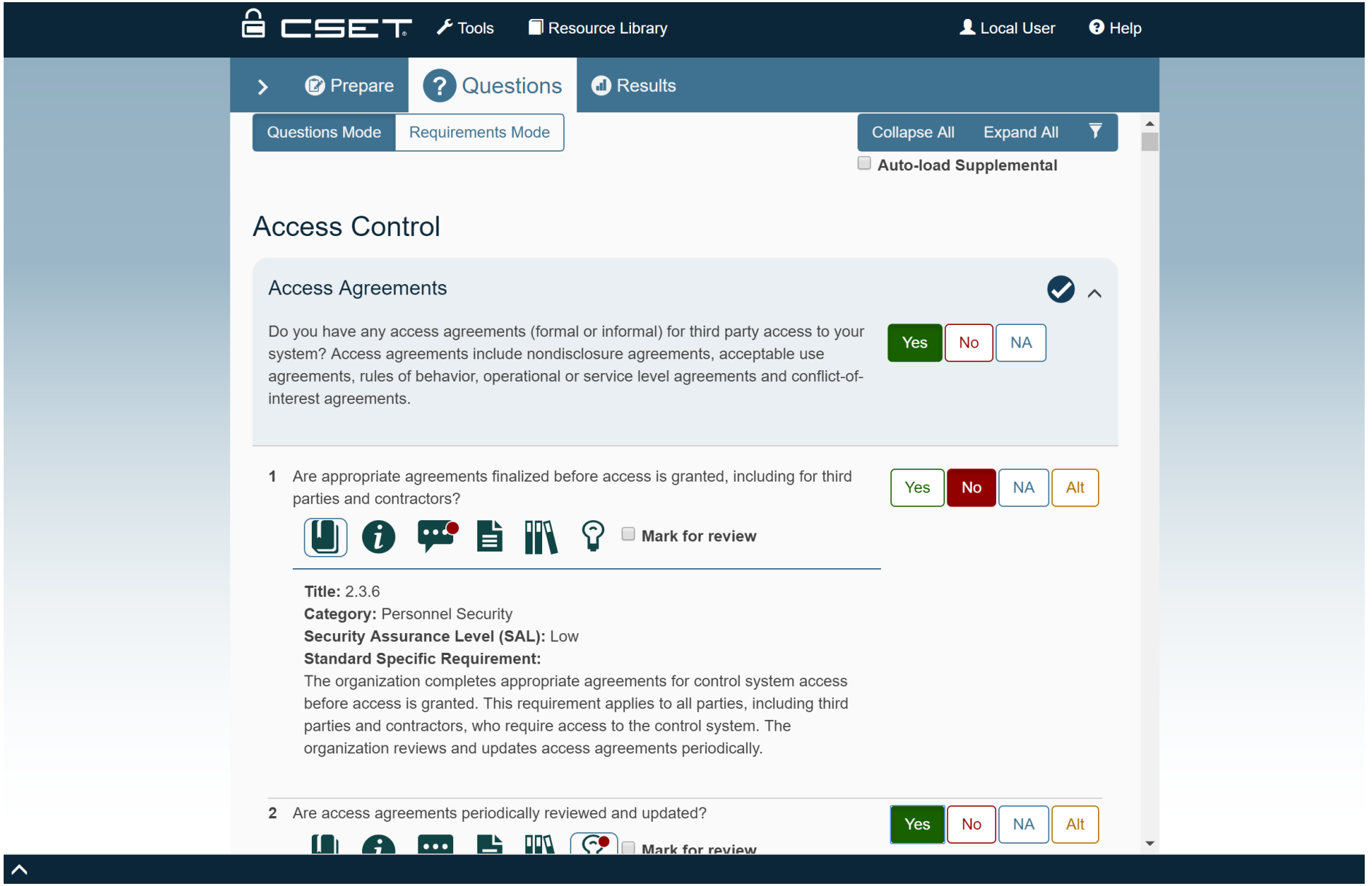


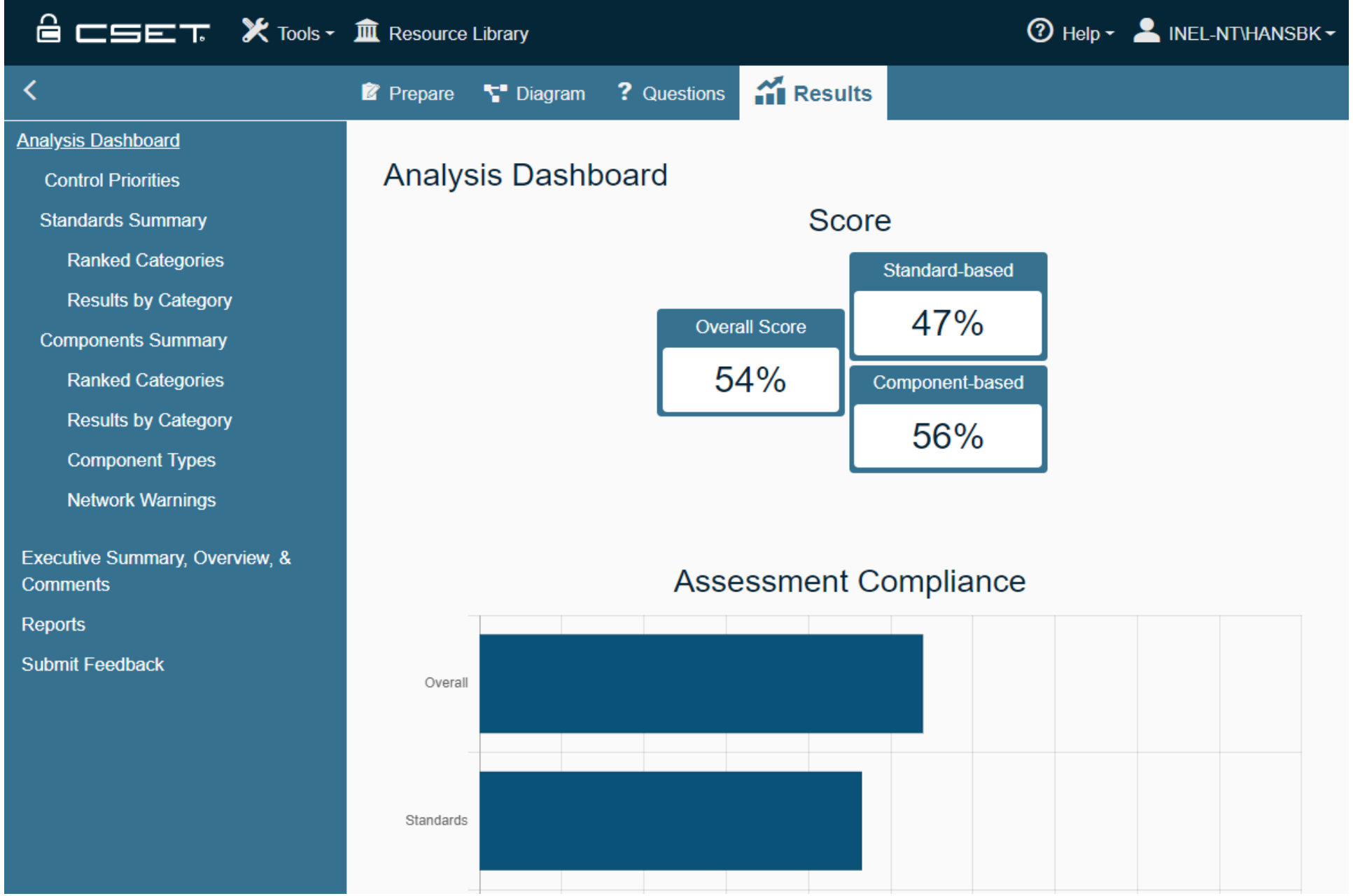
Standard Selection



Network Diagram


CSET
Tools
Resource Library
Help
INEL-NT\HANSBK
Prepare
Diagram
Questions
Results
Standard Questions
Access Control
Account Management
Audit and Accountability
Communication Protection
Configuration Management
Continuity
Incident Response
Monitoring & Malware
Organizational
Personnel
Physical Security
Plans
Policies & Procedures General
Procedures
Remote Access Control
Risk Management and Assessment
Safety Instrumented System (SIS)
System and Services Acquisition
Questions Mode
Requirements Mode
Collapse All
Expand All
Auto-load Supplemental
Access Control - Standard Questions
Access Agreements
1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?
Yes
No
NA
Alt
Least Privilege
2 Is the concept of least privilege used to accomplish assigned tasks?
Yes
No
NA
Alt
System Use Notification
Does the organization have any signage or banners indicating system use policies?
Yes
No
NA


CSET
Tools
Resource Library
Local User
Help
Prepare
Questions
Results
Questions Mode
Requirements Mode
Collapse All
Expand All
Auto-load Supplemental
Access Control
Access Agreements
Do you have any access agreements (formal or informal) for third party access to your system? Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, operational or service level agreements and conflict-of-interest agreements.
Yes
No
NA
1 Are appropriate agreements finalized before access is granted, including for third parties and contractors?
Yes
No
NA
Alt
Mark for review
Title: 2.3.6
Category: Personnel Security
Security Assurance Level (SAL): Low
Standard Specific Requirement:
The organization completes appropriate agreements for control system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the control system. The organization reviews and updates access agreements periodically.
2 Are access agreements periodically reviewed and updated?
Yes
No
NA
Alt
Mark for review


CSET
Tools
Resource Library
Help
INEL-NT\HANSBK
Prepare
Diagram
Questions
Results
Analysis Dashboard
Control Priorities
Standards Summary
Ranked Categories
Results by Category
Components Summary
Ranked Categories
Results by Category
Component Types
Network Warnings
Executive Summary, Overview, & Comments
Reports
Submit Feedback
Analysis Dashboard
Score
Standard-based
47%
Overall Score
54%
Component-based
56%
Assessment Compliance
Overall
Standards

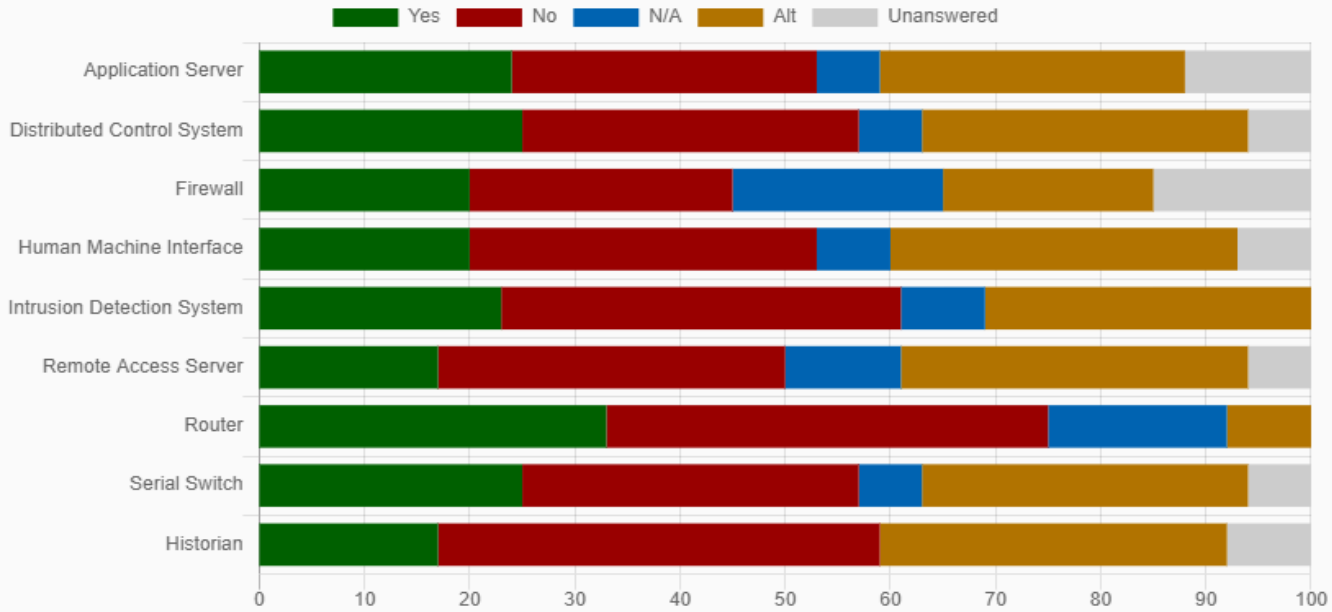
Results

CSET Tools Resource Library Help INEL-NT\HANSBK

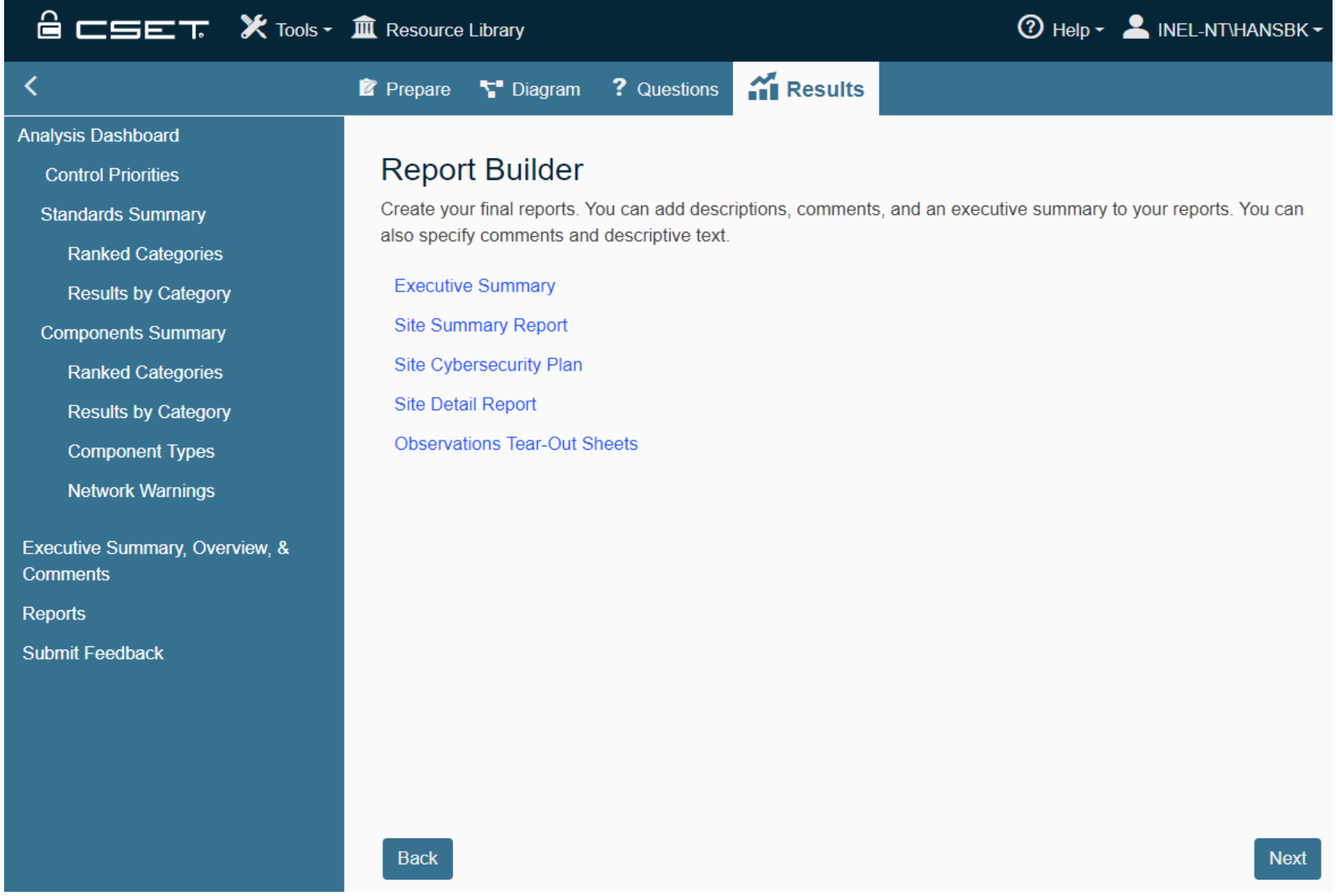
Prepare Diagram Questions Results

- Analysis Dashboard
  - Control Priorities
  - Standards Summary
    - Ranked Categories
    - Results by Category
  - Components Summary
    - Ranked Categories
    - Results by Category
    - Component Types
    - Network Warnings
- Executive Summary, Overview, & Comments
- Reports
- Submit Feedback

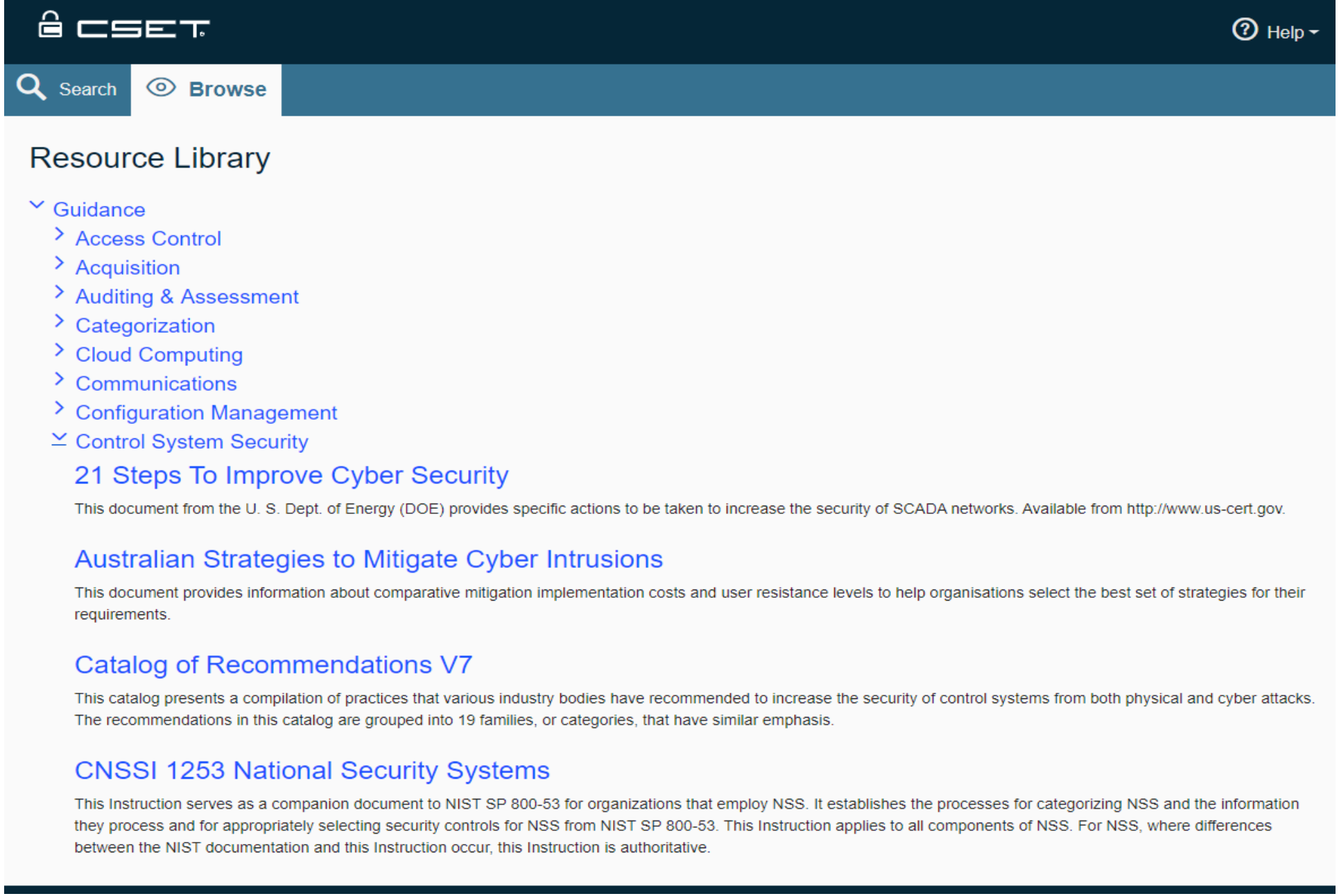
Components By Component Type



Component	Yes	No	N/A	Alternate	Unanswered	Total
Application Server	24%	29%	6%	29%	12%	68
Distributed Control System	25%	32%	6%	31%	6%	144
Firewall	20%	25%	20%	20%	15%	80
Human Machine Interface	20%	33%	7%	33%	7%	15


CSET
Tools
Resource Library
Help
INEL-NT\HANSBK
Prepare
Diagram
Questions
Results
Analysis Dashboard
Control Priorities
Standards Summary
Ranked Categories
Results by Category
Components Summary
Ranked Categories
Results by Category
Component Types
Network Warnings
Executive Summary, Overview, & Comments
Reports
Submit Feedback
Report Builder
Create your final reports. You can add descriptions, comments, and an executive summary to your reports. You can also specify comments and descriptive text.
Executive Summary
Site Summary Report
Site Cybersecurity Plan
Site Detail Report
Observations Tear-Out Sheets
Back
Next

Reports


CSET
Help
Search
Browse
Resource Library
Guidance
Access Control
Acquisition
Auditing & Assessment
Categorization
Cloud Computing
Communications
Configuration Management
Control System Security
21 Steps To Improve Cyber Security
This document from the U. S. Dept. of Energy (DOE) provides specific actions to be taken to increase the security of SCADA networks. Available from http://www.us-cert.gov.
Australian Strategies to Mitigate Cyber Intrusions
This document provides information about comparative mitigation implementation costs and user resistance levels to help organisations select the best set of strategies for their requirements.
Catalog of Recommendations V7
This catalog presents a compilation of practices that various industry bodies have recommended to increase the security of control systems from both physical and cyber attacks. The recommendations in this catalog are grouped into 19 families, or categories, that have similar emphasis.
CNSSI 1253 National Security Systems
This Instruction serves as a companion document to NIST SP 800-53 for organizations that employ NSS. It establishes the processes for categorizing NSS and the information they process and for appropriately selecting security controls for NSS from NIST SP 800-53. This Instruction applies to all components of NSS. For NSS, where differences between the NIST documentation and this Instruction occur, this Instruction is authoritative.

Home » Module Detail

Module Detail

A Module may be based on an industry standard, or may simply be a collection of questions. Modules based on standards will normally take the Requirements path in order to transfer the requirements into the Set.

If you are building a Standard, manage the requirements by clicking Requirements. The Questions path will show the structure of the related questions when in 'questions mode' of the assessment.

It is a good practice to attach any related documents to the Module. Click Manage Documents to upload and attach files.

Module Name *

A Company Custom Extension to the NIST Framework

Short Name *

ACME Custom

Description *

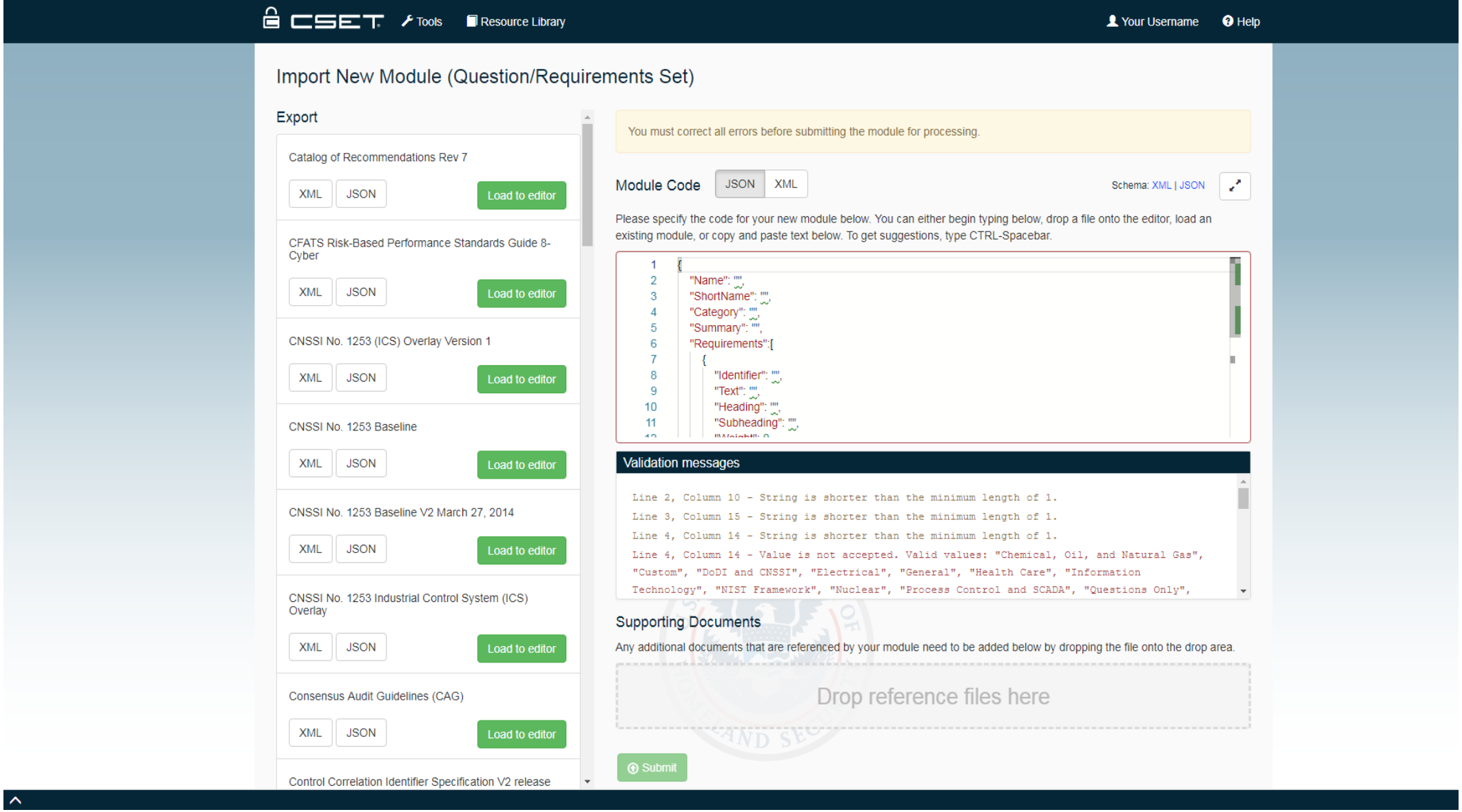
There are some additional questions both specific to our company and that we believe are not generally addressed that we would like to include in all our assessments

Category

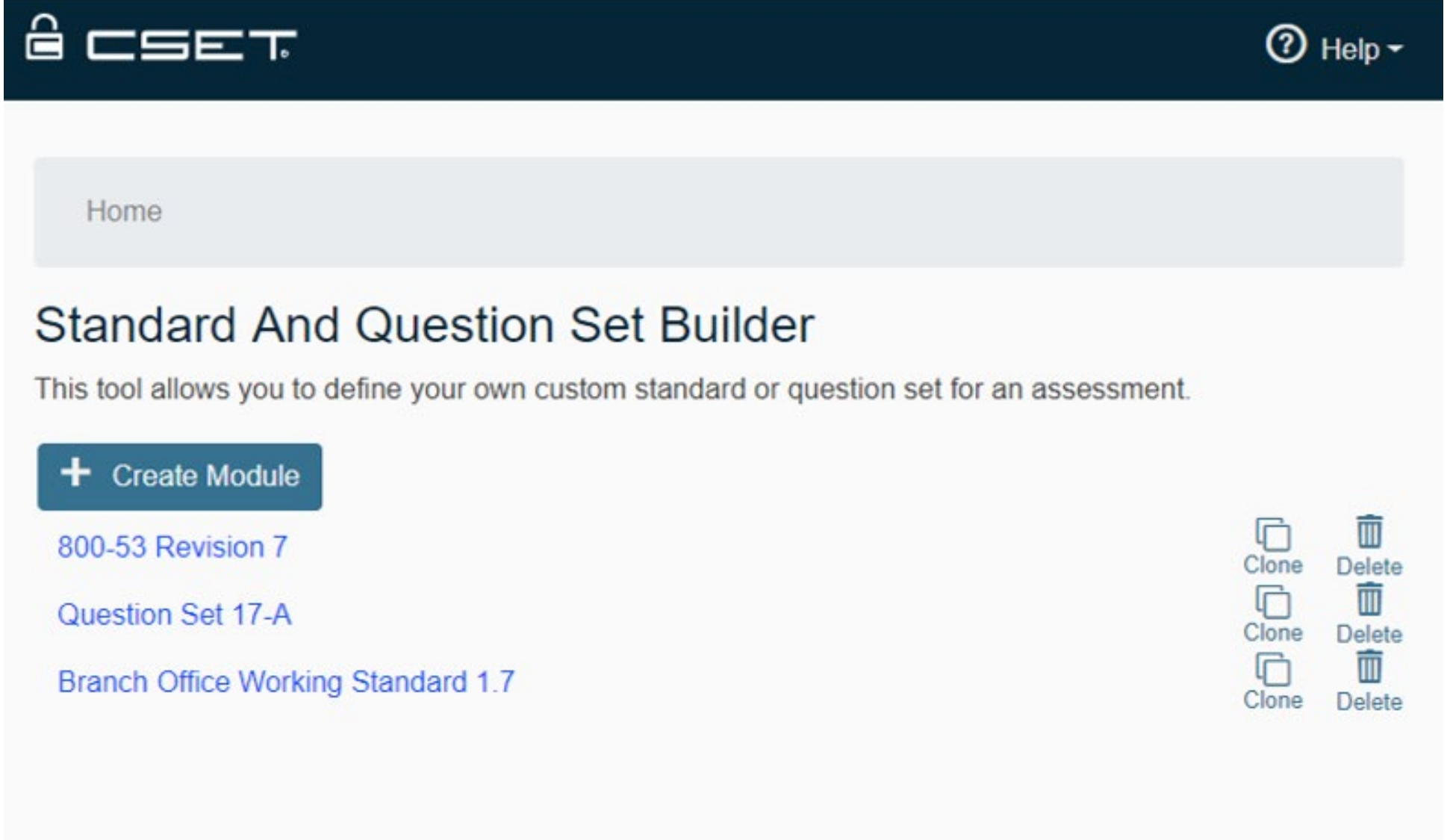
Information Technology

Requirements | ? Questions | Manage Documents

« Back to Module List



Import Modules


CSET
Help
Home
Standard And Question Set Builder
This tool allows you to define your own custom standard or question set for an assessment.
+ Create Module
800-53 Revision 7
Question Set 17-A
Branch Office Working Standard 1.7
Clone
Delete
Clone
Delete
Clone
Delete

For the latest web application:
github.com/cisagov/cset

For old desktop versions:
ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Questions?
Email: CSD_VM_Methodology@cisa.dhs.gov