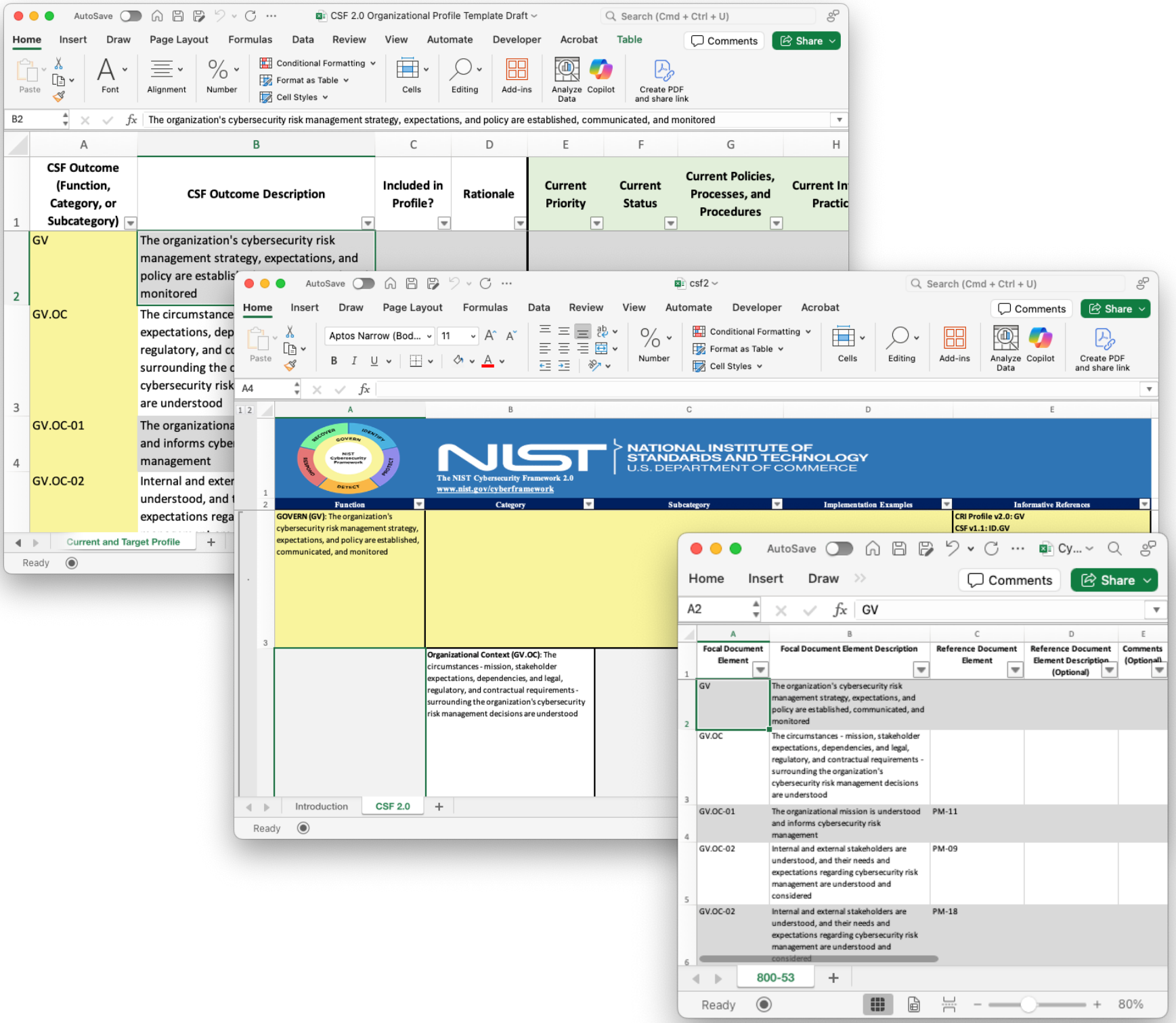

CSF 2.0 Organizational Profile Template Draft
Search (Cmd + Ctrl + U)
Home Insert Draw Page Layout Formulas Data Review View Automate Developer Acrobat Table
Comments Share
B2
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
CSF Outcome (Function, Category, or Subcategory)
CSF Outcome Description
Included in Profile?
Rationale
Current Priority
Current Status
Current Policies, Processes, and Procedures
GV
The organization's cybersecurity risk management strategy, expectations, and policy are establis
monitored
GV.OC
The circumstance
expectations, dep
regulatory, and c
surrounding the c
cybersecurity risk
are understood
GV.OC-01
The organizationa
and informs cybe
management
GV.OC-02
Internal and exter
understood, and t
expectations rega
Current and Target Profile
Ready
csf2
Aptos Narrow (Bod...
11
A4
NIST
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE
The NIST Cybersecurity Framework 2.0
www.nist.gov/cyberframework
Function
Category
Subcategory
Implementation Examples
Informative References
GOVERN (GV): The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
CRI Profile v2.0: GV
CSF v1.1: ID.GV
Organizational Context (GV.OC): The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood
Introduction
CSF 2.0
Ready
Cy...
A2
GV
Focal Document Element
Focal Document Element Description
Reference Document Element
Reference Document Element Description (Optional)
Comments (Optional)
GV
The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored
GV.OC
The circumstances - mission, stakeholder expectations, dependencies, and legal, regulatory, and contractual requirements - surrounding the organization's cybersecurity risk management decisions are understood
GV.OC-01
The organizational mission is understood and informs cybersecurity risk management
PM-11
GV.OC-02
Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
PM-09
GV.OC-02
Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered
PM-18
800-53
Ready
80%

Simply Cyber - Enterprise Risk Assessment (ERA) Security Control “Rosetta Stone” v1.1

Contents

README MIT license

Simply Cyber Academy - CSF Profile Assessment Database - v0.1_Beta

A tool designed to help organizations implement and assess their cybersecurity posture using the NIST Cybersecurity Framework (CSF). This application provides a structured approach to:

- Track and manage CSF outcomes
- Assign ownership and stakeholders to controls
- Document observations and findings
- Score current and desired security states
- Export to csv for data visualization in Excel (find a companion Excel template in public/Sample_Artifacts)
- Track remediation progress

The is an open source project, and improvement ideas to drive cyber risk reduction with CSF assessments are welcome from the Simply Cyber and other awesome communities.

SIMPLYCYBER ACADEMY

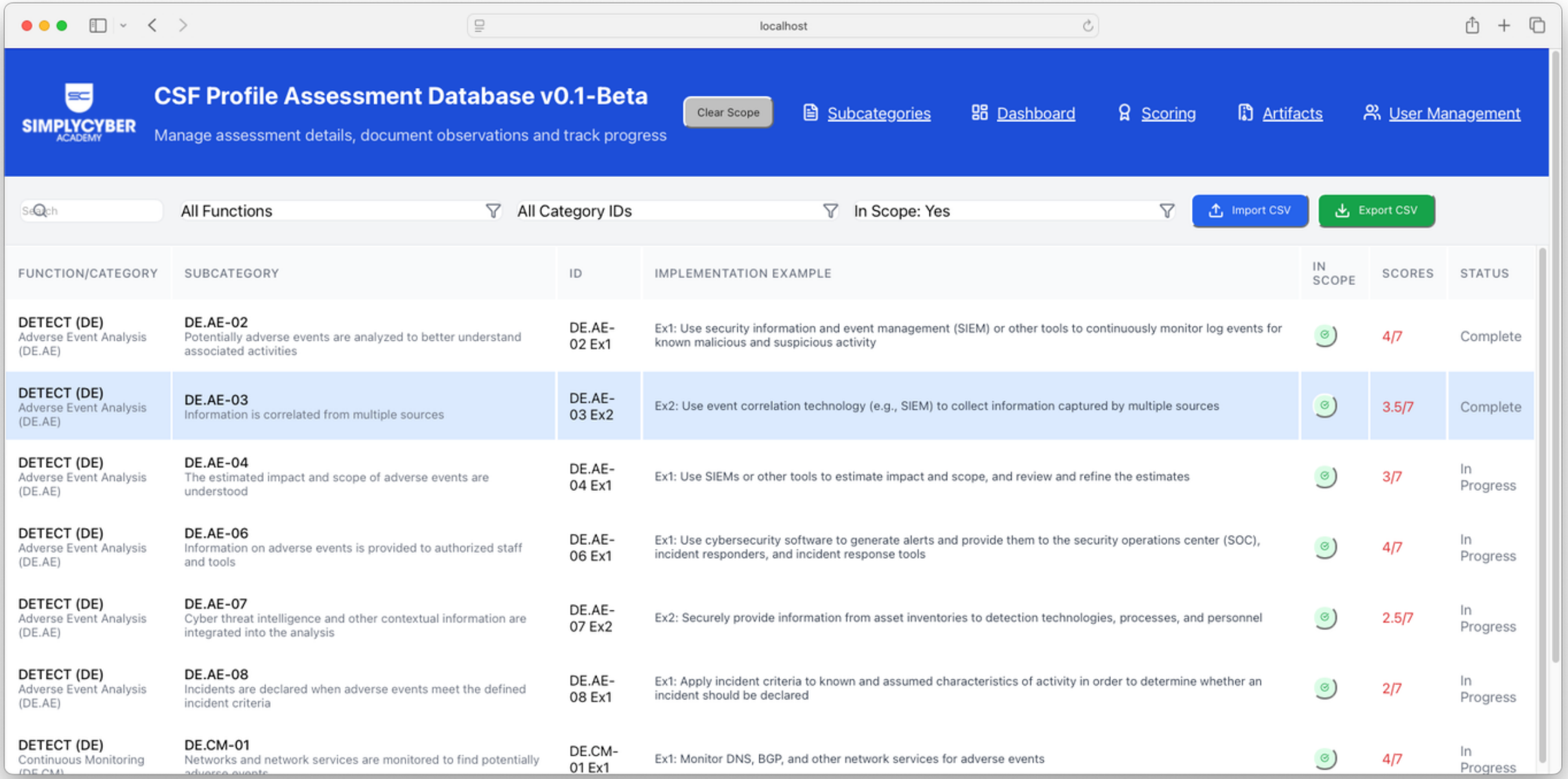
Find in depth videos for CSF profile assessments and this tool in Simply Cyber Academy here: https://academy.simplycyber.io/p/accrp

Packages

No packages published

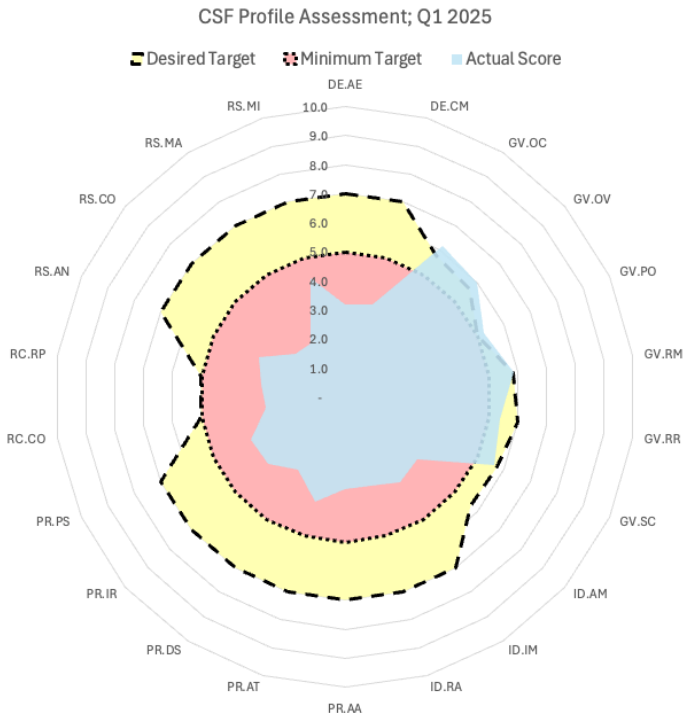
Languages

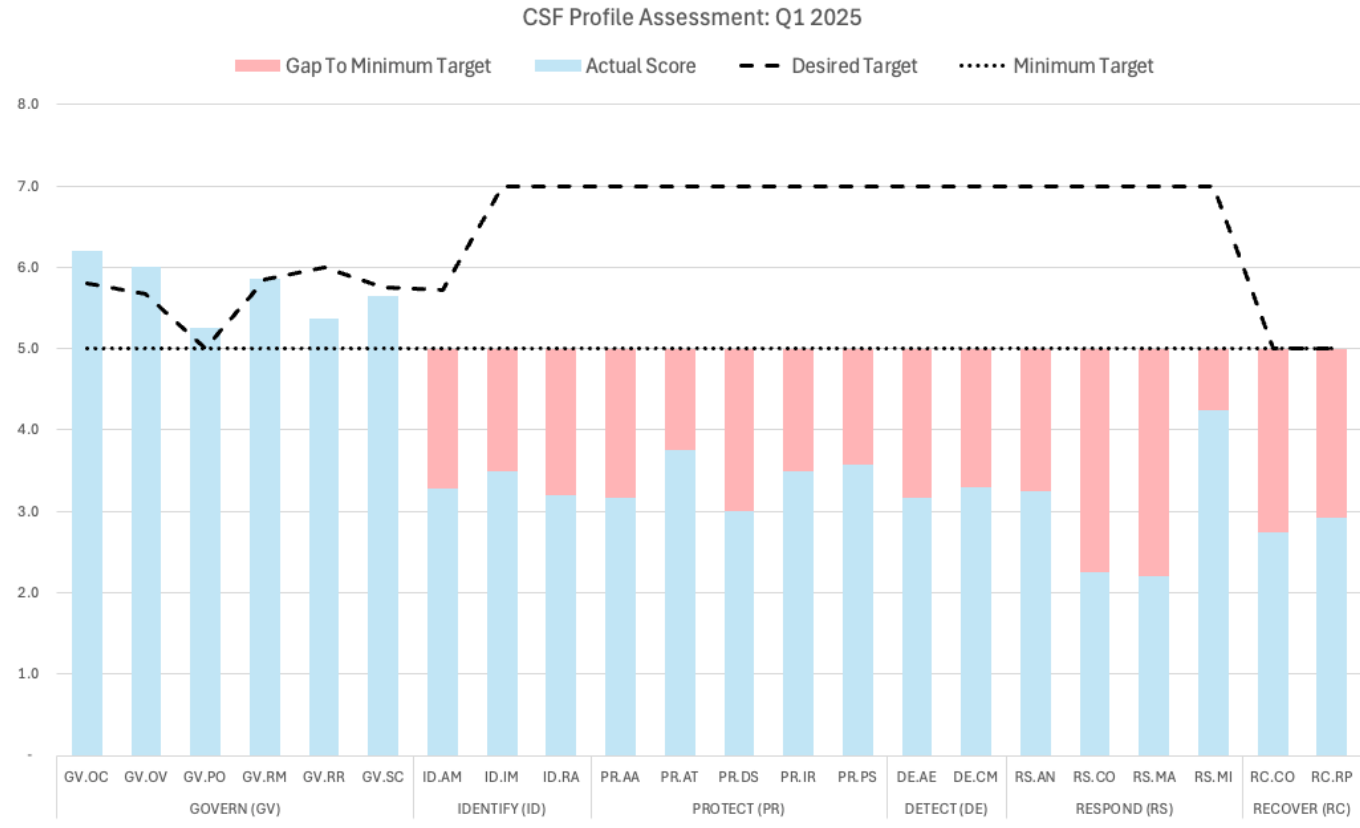
JavaScript 94.5% CSS 4.1% HTML 1.4%

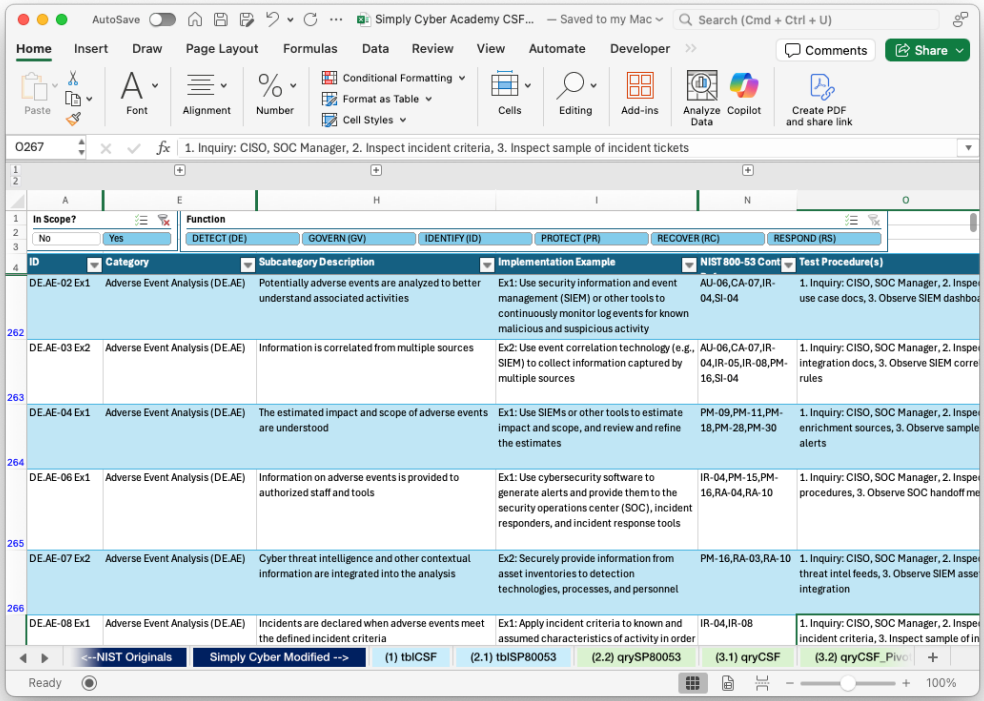

localhost
SIMPLYCYBER ACADEMY
CSF Profile Assessment Database v0.1-Beta
Manage assessment details, document observations and track progress
Clear Scope
Subcategories
Dashboard
Scoring
Artifacts
User Management
Search
All Functions
All Category IDs
In Scope: Yes
Import CSV
Export CSV
FUNCTION/CATEGORY
SUBCATEGORY
ID
IMPLEMENTATION EXAMPLE
IN SCOPE
SCORES
STATUS
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-02
Potentially adverse events are analyzed to better understand associated activities
DE.AE-02 Ex1
Ex1: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity
4/7
Complete
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-03
Information is correlated from multiple sources
DE.AE-03 Ex2
Ex2: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources
3.5/7
Complete
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-04
The estimated impact and scope of adverse events are understood
DE.AE-04 Ex1
Ex1: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates
3/7
In Progress
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-06
Information on adverse events is provided to authorized staff and tools
DE.AE-06 Ex1
Ex1: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools
4/7
In Progress
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-07
Cyber threat intelligence and other contextual information are integrated into the analysis
DE.AE-07 Ex2
Ex2: Securely provide information from asset inventories to detection technologies, processes, and personnel
2.5/7
In Progress
DETECT (DE)
Adverse Event Analysis (DE.AE)
DE.AE-08
Incidents are declared when adverse events meet the defined incident criteria
DE.AE-08 Ex1
Ex1: Apply incident criteria to known and assumed characteristics of activity in order to determine whether an incident should be declared
2/7
In Progress
DETECT (DE)
Continuous Monitoring
DE.CM-01
Networks and network services are monitored to find potentially
DE.CM-01 Ex1
Ex1: Monitor DNS, BGP, and other network services for adverse events
4/7
In Progress

CSF Profile Assessment: Q1 2025

Function	Actual	Desired Target	Variance
GOVERN (GV)	5.8	5.8	-
IDENTIFY (ID)	3.3	6.6	(3.3)
PROTECT (PR)	3.4	7.0	(3.6)
DETECT (DE)	3.2	7.0	(3.8)
RESPOND (RS)	2.8	7.0	(4.2)
RECOVER (RC)	2.9	5.0	(2.1)
Overall	**3.9**	**6.4**	**(2.5)**






AutoSave
Simply Cyber Academy CSF...
— Saved to my Mac
Search (Cmd + Ctrl + U)
Home
Insert
Draw
Page Layout
Formulas
Data
Review
View
Automate
Developer
Comments
Share
Paste
Font
Alignment
Number
Conditional Formatting
Format as Table
Cell Styles
Cells
Editing
Add-ins
Analyze Data
Copilot
Create PDF and share link
O267
1. Inquiry: CISO, SOC Manager, 2. Inspect incident criteria, 3. Inspect sample of incident tickets
In Scope?
No
Yes
Function
DETECT (DE)
GOVERN (GV)
IDENTIFY (ID)
PROTECT (PR)
RECOVER (RC)
RESPOND (RS)
ID
Category
Subcategory Description
Implementation Example
NIST 800-53 Cont
Test Procedure(s)
DE.AE-02 Ex1
Adverse Event Analysis (DE.AE)
Potentially adverse events are analyzed to better understand associated activities
Ex1: Use security information and event management (SIEM) or other tools to continuously monitor log events for known malicious and suspicious activity
AU-06,CA-07,IR-04,SI-04
1. Inquiry: CISO, SOC Manager, 2. Inspe use case docs, 3. Observe SIEM dashboa
262
DE.AE-03 Ex2
Adverse Event Analysis (DE.AE)
Information is correlated from multiple sources
Ex2: Use event correlation technology (e.g., SIEM) to collect information captured by multiple sources
AU-06,CA-07,IR-04,IR-05,IR-08,PM-16,SI-04
1. Inquiry: CISO, SOC Manager, 2. Inspe integration docs, 3. Observe SIEM corre rules
263
DE.AE-04 Ex1
Adverse Event Analysis (DE.AE)
The estimated impact and scope of adverse events are understood
Ex1: Use SIEMs or other tools to estimate impact and scope, and review and refine the estimates
PM-09,PM-11,PM-18,PM-28,PM-30
1. Inquiry: CISO, SOC Manager, 2. Inspe enrichment sources, 3. Observe sample alerts
264
DE.AE-06 Ex1
Adverse Event Analysis (DE.AE)
Information on adverse events is provided to authorized staff and tools
Ex1: Use cybersecurity software to generate alerts and provide them to the security operations center (SOC), incident responders, and incident response tools
IR-04,PM-15,PM-16,RA-04,RA-10
1. Inquiry: CISO, SOC Manager, 2. Inspe procedures, 3. Observe SOC handoff me
265
DE.AE-07 Ex2
Adverse Event Analysis (DE.AE)
Cyber threat intelligence and other contextual information are integrated into the analysis
Ex2: Securely provide information from asset inventories to detection technologies, processes, and personnel
PM-16,RA-03,RA-10
1. Inquiry: CISO, SOC Manager, 2. Inspe threat intel feeds, 3. Observe SIEM asse integration
266
DE.AE-08 Ex1
Adverse Event Analysis (DE.AE)
Incidents are declared when adverse events meet the defined incident criteria
Ex1: Apply incident criteria to known and assumed characteristics of activity in order
IR-04,IR-08
1. Inquiry: CISO, SOC Manager, 2. Inspe incident criteria, 3. Inspect sample of in
<--NIST Originals
Simply Cyber Modified -->
(1) tblCSF
(2.1) tblSP80053
(2.2) qrySP80053
(3.1) qryCSF
(3.2) qryCSF_Pivo
Ready
100%