EVERYONE GETS A FRAMEWORK

https://www.linkedin.com/in/junell-felsburg/

ABOUT ME

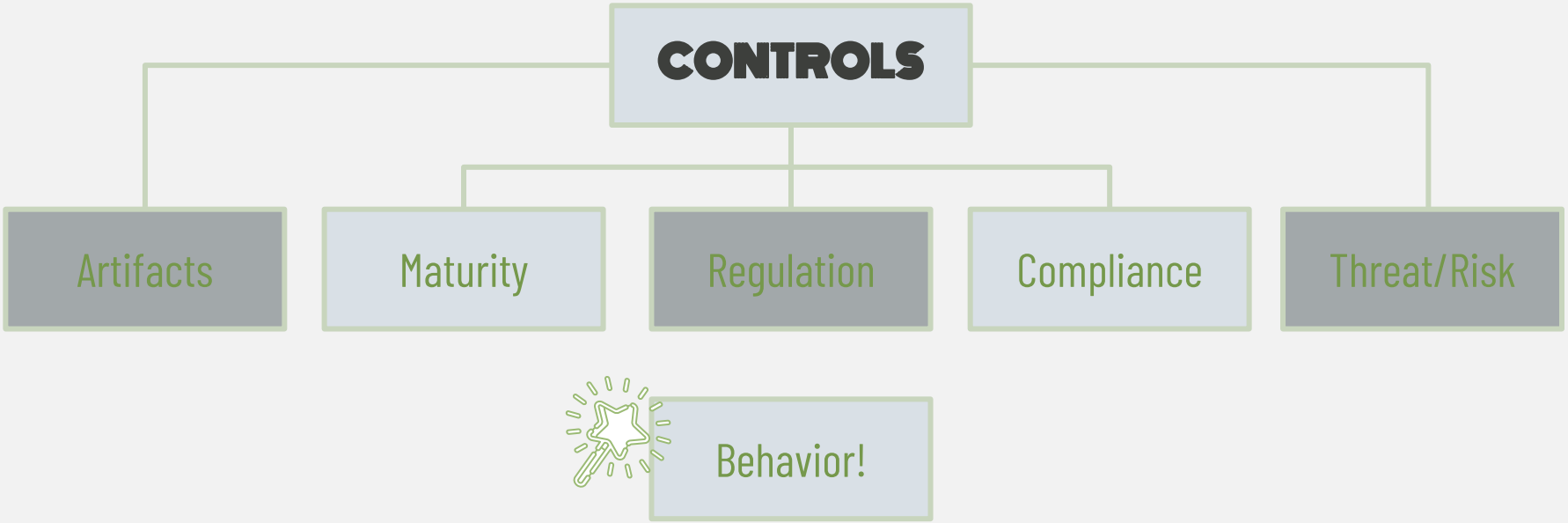
- Information Systems/Network
- Technology, GRC, People
- The Columbus Foundation
- Innovative Leadership Institute & IT Leaders
- Unplugged afterhours

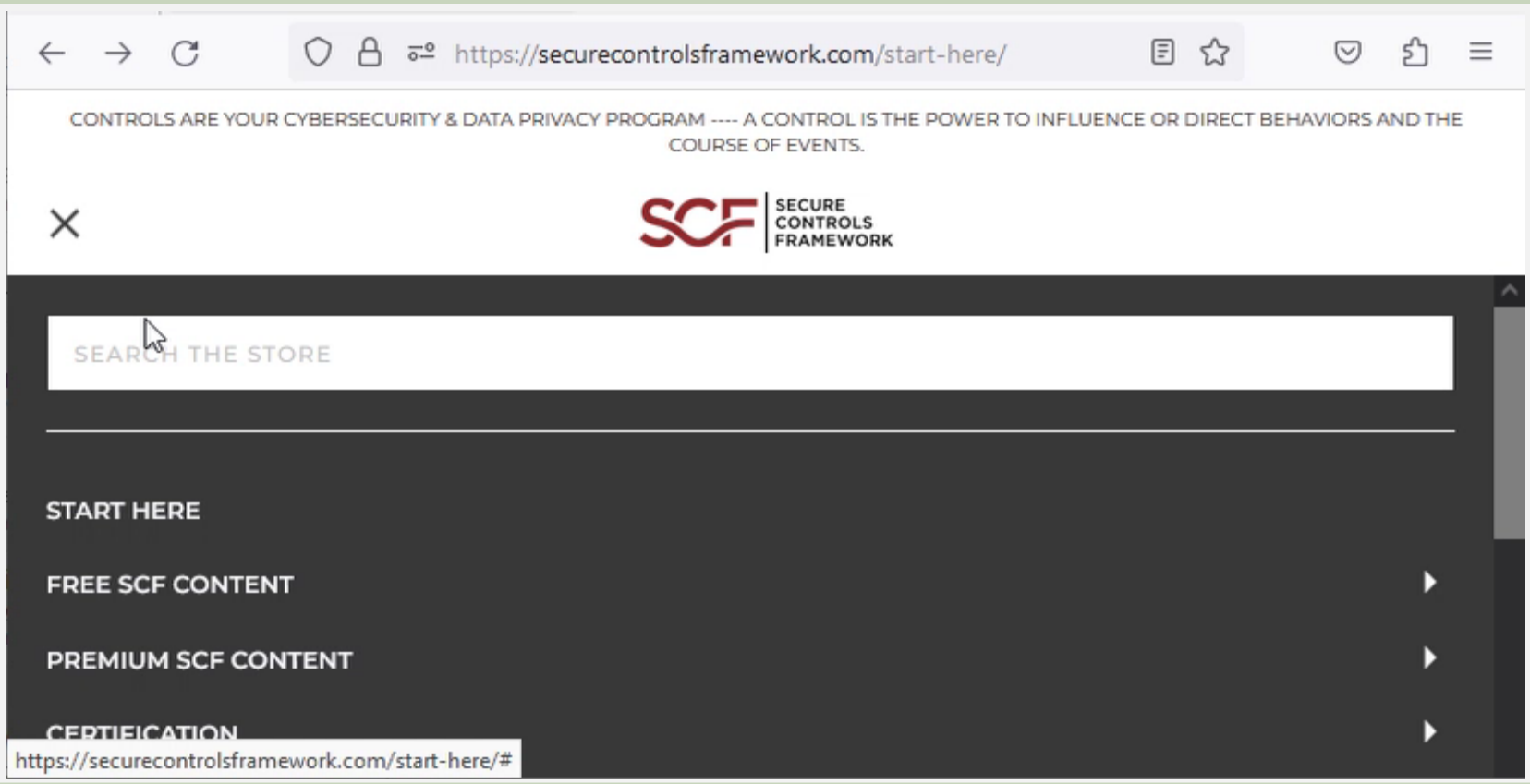
JUNELL FELSBURG

THE PROBLEM


SCF
SECURE
CONTROLS
FRAMEWORK

Another Framework???




https://securecontrolsframework.com/start-here/
CONTROLS ARE YOUR CYBERSECURITY & DATA PRIVACY PROGRAM ---- A CONTROL IS THE POWER TO INFLUENCE OR DIRECT BEHAVIORS AND THE COURSE OF EVENTS.
SCF
SECURE CONTROLS FRAMEWORK
SEARCH THE STORE
START HERE
FREE SCF CONTENT
PREMIUM SCF CONTENT
CERTIFICATION
https://securecontrolsframework.com/start-here/#

289

Columns

1169

Rows

MASSIVE

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Methods To Comp
Cybersecurity & Privacy Governance	Digital Security Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity and privacy governance controls.	- Steering committee - Digital Security Progra - Cybersecurity & Data (CDPP)
Cybersecurity & Privacy Governance	Steering Committee & Program Oversight	GOV-01.1	Mechanisms exist to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets formally and on a regular basis.	- Steering committee - Digital Security Progra - Cybersecurity & Data (CDPP)
Cybersecurity & Privacy Governance	Status Reporting To Governing Body	GOV-01.2	Mechanisms exist to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy program.	
Cybersecurity & Privacy Governance	Publishing Cybersecurity & Privacy Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	- Steering committee - Digital Security Progra - Cybersecurity & Data (CDPP)

THE PROCESS

Identify Sources

Plan

PLAN

A

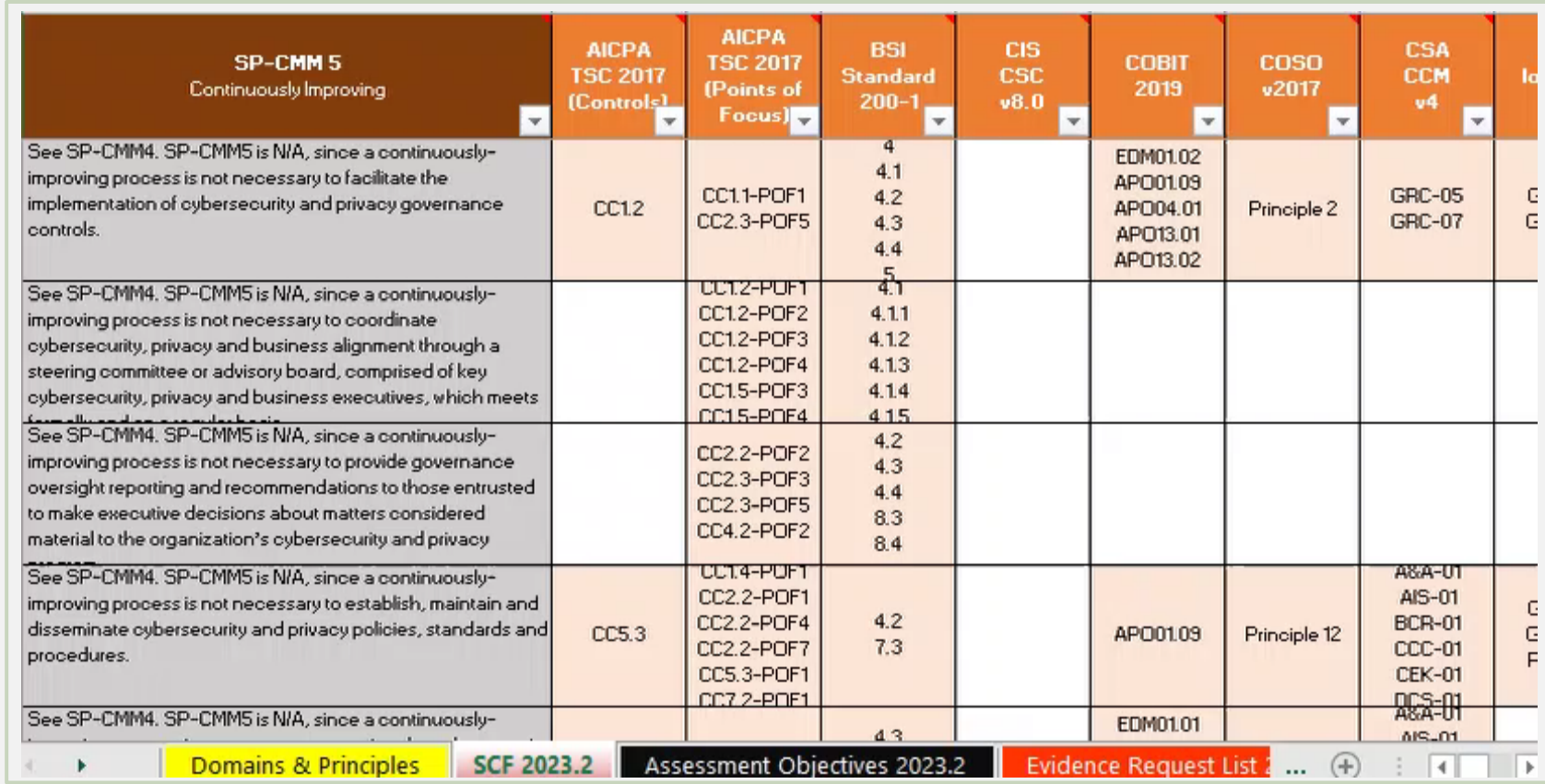
Hide all unneeded Source Columns (S:HK)

B

Minimum Compliance Controls & Discretionary Security Requirements

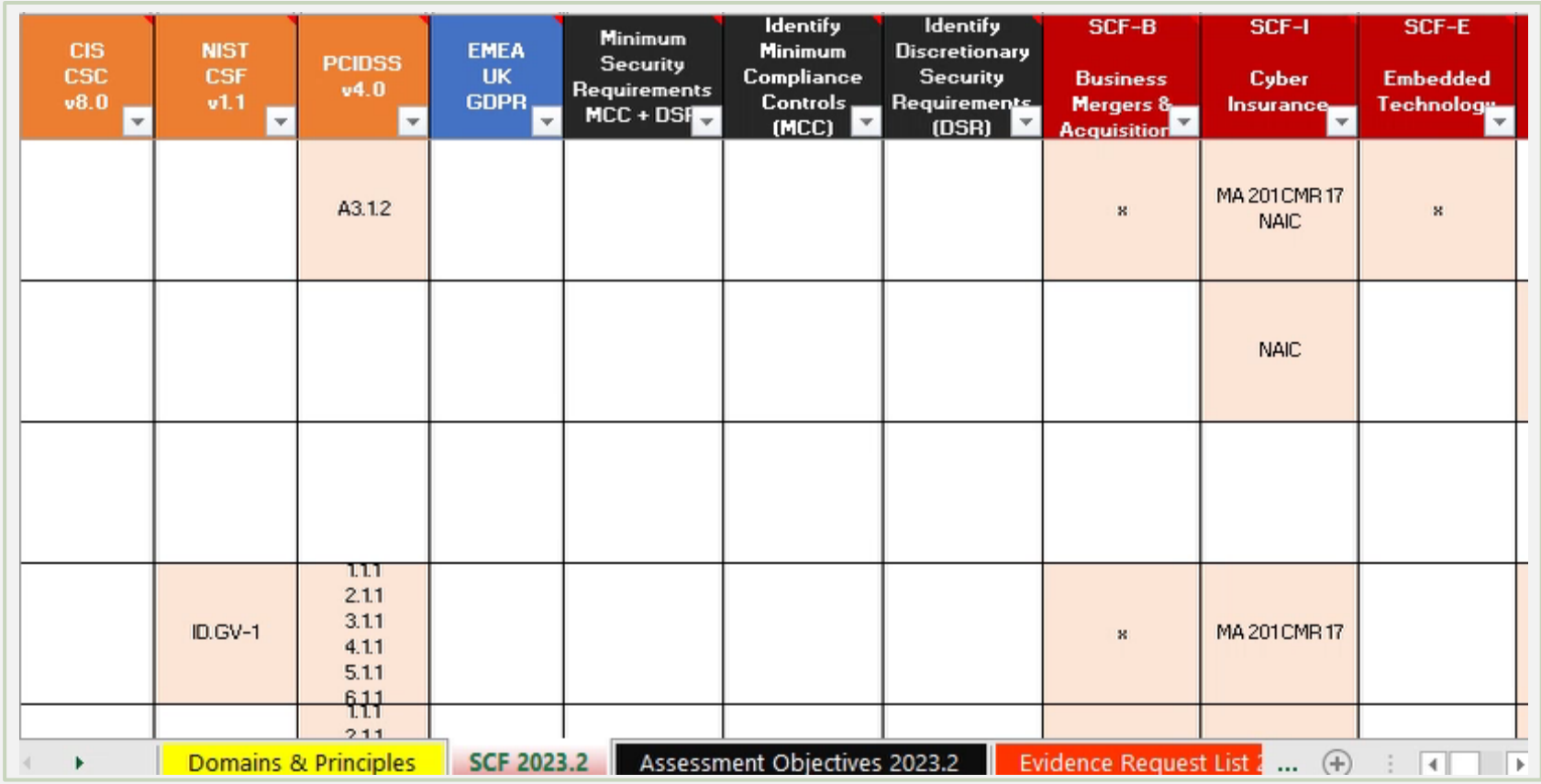
C

Hide (or delete) all unneeded Control Rows



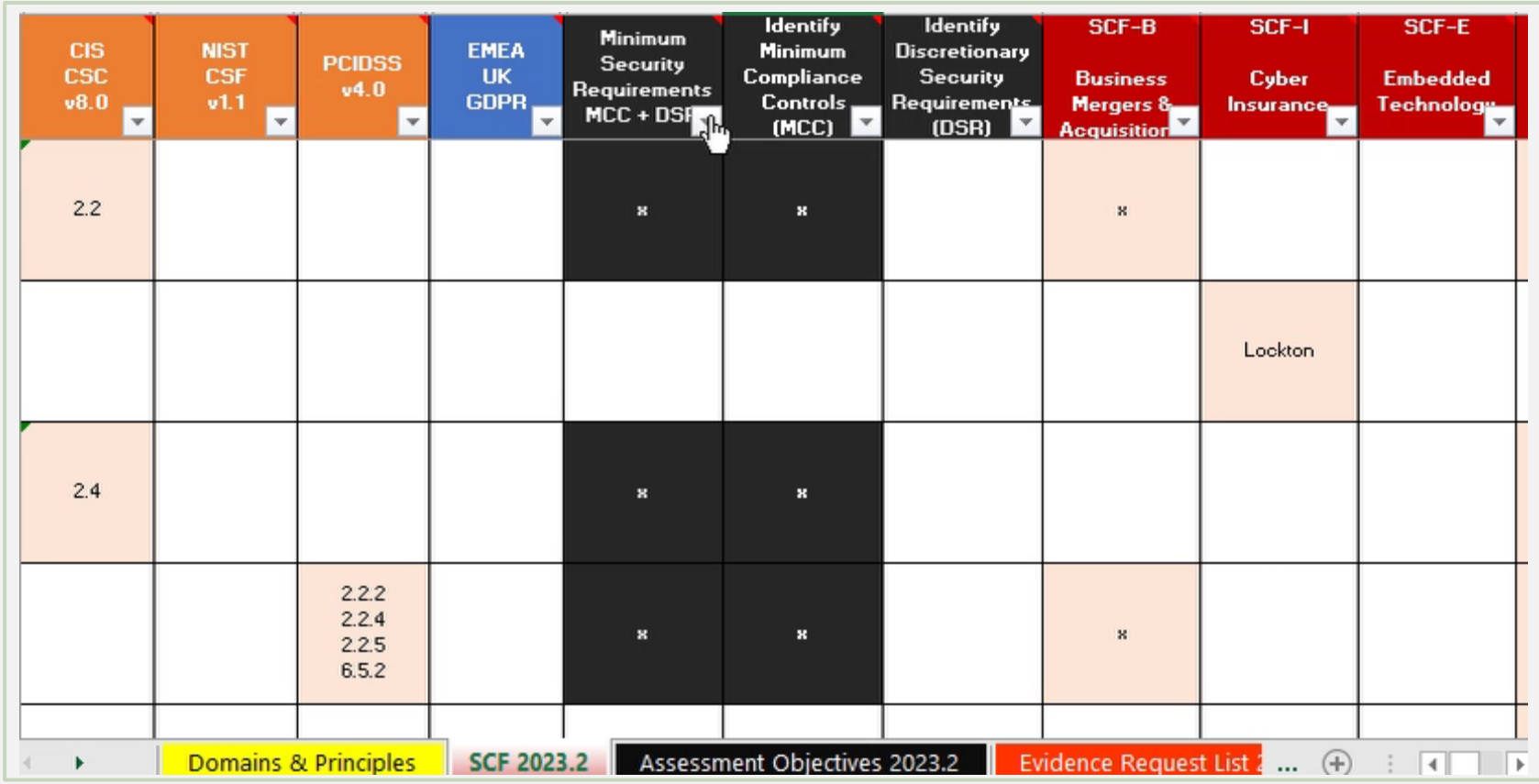
SP-CMM 5 Continuously Improving	AICPA TSC 2017 (Controls)	AICPA TSC 2017 (Points of Focus)	BSI Standard 200-1	CIS CSC v8.0	COBIT 2019	COSO v2017	CSA CCM v4	Io
See SP-CMM4. SP-CMM5 is N/A, since a continuously-improving process is not necessary to facilitate the implementation of cybersecurity and privacy governance controls.	CC1.2	CC1.1-POF1 CC2.3-POF5	4 4.1 4.2 4.3 4.4 5		EDM01.02 APO01.09 APO04.01 APO13.01 APO13.02	Principle 2	GRC-05 GRC-07	G G
See SP-CMM4. SP-CMM5 is N/A, since a continuously-improving process is not necessary to coordinate cybersecurity, privacy and business alignment through a steering committee or advisory board, comprised of key cybersecurity, privacy and business executives, which meets		CC1.2-POF1 CC1.2-POF2 CC1.2-POF3 CC1.2-POF4 CC1.5-POF3 CC1.5-POF4	4.1 4.1.1 4.1.2 4.1.3 4.1.4 4.1.5					
See SP-CMM4. SP-CMM5 is N/A, since a continuously-improving process is not necessary to provide governance oversight reporting and recommendations to those entrusted to make executive decisions about matters considered material to the organization's cybersecurity and privacy		CC2.2-POF2 CC2.3-POF3 CC2.3-POF5 CC4.2-POF2	4.2 4.3 4.4 8.3 8.4					
See SP-CMM4. SP-CMM5 is N/A, since a continuously-improving process is not necessary to establish, maintain and disseminate cybersecurity and privacy policies, standards and procedures.	CC5.3	CC1.4-POF1 CC2.2-POF1 CC2.2-POF4 CC2.2-POF7 CC5.3-POF1 CC7.2-POF1	4.2 7.3		APO01.09	Principle 12	A&A-01 AIS-01 BCR-01 CCC-01 CEK-01 DCS-01	G G P
See SP-CMM4. SP-CMM5 is N/A, since a continuously-			4.3		EDM01.01		A&A-01 AIS-01	

Domains & Principles | SCF 2023.2 | Assessment Objectives 2023.2 | Evidence Request List 2 ...



CIS CSC v8.0	NIST CSF v1.1	PCIDSS v4.0	EMEA UK GDPR	Minimum Security Requirements MCC + DSR	Identify Minimum Compliance Controls (MCC)	Identify Discretionary Security Requirements (DSR)	SCF-B Business Mergers & Acquisition	SCF-I Cyber Insurance	SCF-E Embedded Technology
		A3.1.2					x	MA 201 CMR 17 NAIC	x
								NAIC	
	ID.GV-1	1.1.1 2.1.1 3.1.1 4.1.1 5.1.1 6.1.1					x	MA 201 CMR 17	
		1.1.1 2.1.1							

Domains & Principles | SCF 2023.2 | Assessment Objectives 2023.2 | Evidence Request List 2 ...



CIS CSC v8.0	NIST CSF v1.1	PCIDSS v4.0	EMEA UK GDPR	Minimum Security Requirements MCC + DSR	Identify Minimum Compliance Controls (MCC)	Identify Discretionary Security Requirements (DSR)	SCF-B Business Mergers & Acquisition	SCF-I Cyber Insurance	SCF-E Embedded Technology
2.2				x	x		x		
								Lockton	
2.4				x	x				
		2.2.2 2.2.4 2.2.5 6.5.2		x	x		x		

Domains & Principles | SCF 2023.2 | Assessment Objectives 2023.2 | Evidence Request List 2 ...

STOP RIGHT THERE

You have a framework just for you!

Really?

Really, Really.

But I didn't do anything.

EVERYONE GETS A ~~FRAMEWORK~~ INFORMATION SECURITY PROGRAM ACTION, IMPLEMENTATION, AND MATURATION PLAN

PROCESS

Identify Sources

Plan

Do

Assessment

DO

A

Determine Priority

B

Ask the questions

C

Collect the Evidence

D

Assess Maturity

SCF Domain	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Methods To Comply With SCF Controls	Evidence Request List (ERL) #	
Asset Management	Asset Governance	AST-01	Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.	- Generally Accepted Accounting Principles (GAAP) - ITIL - Configuration Management Database (CMDB) - IT Asset Management (ITAM) program	E-AST-01	Does the o manager
Asset Management	Asset Inventories	AST-02	Mechanisms exist to perform inventories of technology assets that: • Accurately reflects the current systems, applications and services in use; • Identifies authorized software products, including business justification details; • Is at the level of granularity deemed necessary for tracking and reporting; • Includes organization-defined information deemed necessary to achieve	- ManageEngine AssetExplorer - LANDesk IT Asset Management Suite - ServiceNow (https://www.servicenow.com/) - Solarwinds (https://www.solarwinds.com/) - CrowdStrike	E-AST-04 E-AST-05 E-AST-07	Does the o • Accurat • Is at the reporting; • Include
Asset Management	Automated Unauthorized Component Detection	AST-02.2	Automated mechanisms exist to detect and alert upon the detection of unauthorized hardware, software and firmware components.	- CimTrak Integrity Suite (https://www.cimcor.com/cimtrak/) - DHCP logging - Active discovery tools - NNT Change Tracker		Does the o and alert and firmw
Asset Management	Component Duplication Avoidance	AST-02.3	Mechanisms exist to establish and maintain an authoritative source and repository to provide a trusted source and accountability for approved and implemented system components that prevents assets from being duplicated in other asset inventories.	- ITIL - Configuration Management Database (CMDB) - Manual or automated process		Does the o duplicate
Asset Management	Network Access Control (NAC)	AST-02.5	Automated mechanisms exist to employ Network Access Control (NAC), or a similar technology, that is capable of detecting unauthorized devices and disable network access to those unauthorized devices.	- Cisco NAC - Aruba Networks - Juniper NAC - Packet Fence - Symantec NAC		Does the o a similar te devices a devices?
Asset Management	Dynamic Host Configuration Protocol	AST-02.6	Mechanisms exist to enable Dynamic Host Configuration Protocol (DHCP) server logging to improve asset inventories and assist in detecting unknown systems.	- Splunk - Manual Process - Build Automation Tools	E-MON-04	Does the o Protocol (assist in d

Examples

AST-01

Mechanisms exist to facilitate an IT Asset Management (ITAM) program to implement and manage asset management controls.

How to Comply

Generally Accepted Accounting Principles (GAAP)
ITIL - Configuration Management Database (CMDB)
- IT Asset Management (ITAM) program

Questions to ask

Does the organization facilitate the implementation of asset management controls?

Evidence

Documented evidence of an IT Asset Management (ITAM) program.

Examples

DCH-24

Mechanisms exist to identify and document the location of information and the specific system components on which the information resides.

How to Comply

- Data Flow Diagram (DFD)

Questions to ask

Does the organization identify and document the location of information and the specific system components on which the information resides?

Evidence

Documented evidence of designated internal and third-party facilities where organizational data is stored, transmitted and/or processed.

SP-CM M 0

- Not Performed

SP-CM M 1

- Performed Informally

SP-CM M 2

- Planned & Tracked

SP-CM M 3

- Well Defined

SP-CM M 4

- Quantitative Controlled

SP-CM M 5

- Continuously Improving

PROCESS

Identify Sources

Analyze Results

Plan

Do

Check

Assessment

CHECK

A

Goal
Maturity

B

What can
be better

C

How are
you going
to get
there

80/20

Pareto Principle

PROCESS

Identify Sources

Plan

Do

Assessment

Analyze Results

Check

Adjust

Drive Change

ADJUST

A

Determine Priority

B

Ask the questions

C

Collect the Evidence

D

Assess Maturity

SEBDB - Behavior

Behaviours

SB063: Checks security credentials of unknown persons at work

Individuals should check the security credentials of unknown people they come into contact with in the workplace. ...

SB064: Prevents tailgating at security checkpoints

When passing through security checkpoints, people should check they are not being followed by others who do not ...

SB065: Does not share security passes or access tokens

Sharing security passes even with "trusted" contacts creates risk. People should only ever use security passes ...

SB066: Escorts visitors to ensure they follow security policies

Visitors should be escorted according to organisational policies. This reduces the risk of unauthorised access to ...

SB105: Uses a security key

Security keys are USB keys or dongles that work as an advanced form of multi-factor authentication. Using them ...

SB177: Does not lose device through theft or negligence

Losing devices containing sensitive information through theft or negligence increases the likelihood of cyber ...

SB177a: Does not lose mobile device through theft or negligence

Losing a mobile phone or tablet containing sensitive information through theft or negligence increases the ...

SB177b: Does not lose laptop/desktop through theft or negligence

Losing laptops/desktops containing sensitive information through theft or negligence increases the likelihood of ...

SB195: Completes policy attestation

Most organizations today have multiple compliance requirements and contractual obligations that require all ...

THANK YOU

Do you have any questions?

https://www.linkedin.com/in/junell-felsburg/
jfelsburg@columbusfoundation.org

CREDITS: This presentation template was created by Slidesgo, including icons by Flaticon, and infographics & images by Freepik.