SANS

Cybersecurity Standards Scorecard (2022 Edition)

Problem Statement – Cybersecurity Standards

- At the present time there are dozens of cybersecurity standards and regulations around the world
- There is a general belief that all standards are basically the same – *this could not be further from the truth*

- Organizations tend to choose a cybersecurity standard based on popularity or experience with a given standard
- Very few organizations have an objective methodology for comparing or evaluating the standards themselves

Goal for this Webcast Series

- The goal for this webcast is for this to be an annual research study
- Each year we will evaluate the most popular cybersecurity standards
- Each year we will reconsider the evaluation criteria based on community feedback and suggestions

- The goal is also to present a potential methodology for evaluating standards
- Different organizations may have different goals and may want to score according to their organizational needs

- Ultimately, we want to help organizations to make an intelligent decision regarding how to choose how to defend themselves

Cybersecurity Standards Evaluated

- Dozens of standards could have been considered for this study
- However, only the following were considered in the 2022 study:
  - CIS Controls (v7.1)
  - CIS Controls (v8.0)
  - NIST CyberSecurity Framework (v1.1)
  - Cybersecurity Maturity Model Certification (v1.02)
  - NIST SP 800-171 (rev2)
  - ISO 27002:2013 & 27002:2022
  - PCI DSS (v3.2 & v4.0)
  - HIPAA
  - COBIT (v5)
  - MITRE Enterprise Mitigations
  - Collective Control Catalog (v2022)

Criteria Used to Compare Standards

- Each standard was evaluated on against a set of characteristics determined to be the baseline for a well-rounded cybersecurity standard
- The criteria used to evaluate each standard includes:
  - Operational Controls Addressed
  - Privacy Controls Addressed
  - Technical Controls Addressed
  - Controls Updated Recently
  - Community Driven / Open Development
  - Popularity of Standard (Google Trends)
  - Maps Threats to Controls
  - Specifically Addresses Modern Threats
  - Maps Detailed Controls to Other Control Standards
  - Tagged for Applicability (Cloud, ICS, IoT, etc)
  - International Applicability / Implementation
  - Prioritizes Controls
  - Corresponding Measures / Metrics Guide

Grade	Score
A+	4.66
A	4.33
A-	4
B+	3.66
B	3.33
B-	3
C+	2.66
C	2.33
C-	2
D+	1.66
D	1.33
D-	1
F+	0.66
F	0.33
F-	0

Cybersecurity Control Baseline – Collective Control Catalog

- Developed by the same consortium of security practitioners that developed the CRM and CTM
- Open-source research project freely available to the community

- Started as a research project to normalize and compare existing cybersecurity standards and regulations
- Presently aggregates and analyzes control libraries from 35+ standards
- Normalizes roughly 2200 control statements to about 400 statements

- Also categorizes, tags, and prioritizes control statements to facilitate project planning and implementation efforts

Project Contributors / Reviewers

- There have been numerous contributors to this project over the last few years

- Some of the key contributors to this project include representatives from:
  - The SANS Institute
  - The Institute of Applied Network Security (IANS)
  - Enclave Security / AuditScripts
  - Black Hills Information Security (BHIS)
  - Individuals from a diverse set of international organizations (public and private)

Collective Control Catalog: Inventory

AuditScripts

Control Frameworks Mapped to the Control Systems (v2022a)

enclave SECURITY

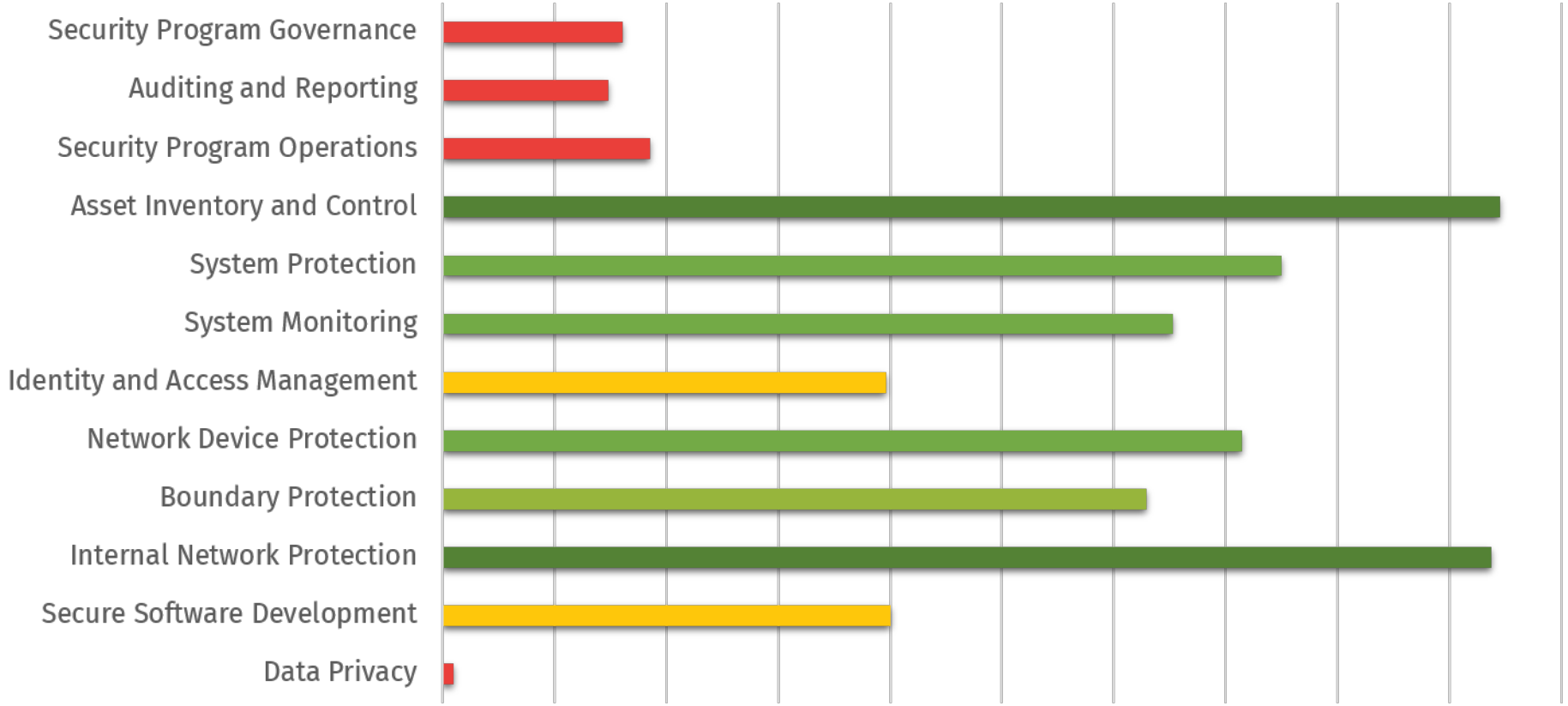
Framework	Recommendation	Description	Control Category	Control System
PCI DSS (v4.0)	1.1	Processes and mechanisms for installing and maintaining network security controls are defined and understood.	Network Device Protection	Network Device Management System
PCI DSS (v4.0)	1.2	Network security controls (NSCs) are configured and maintained.	Network Device Protection	Network Device Management System
PCI DSS (v4.0)	1.3	Network access to and from the cardholder data environment is restricted.	Internal Network Protection	Network Segmentation and Control System
PCI DSS (v4.0)	1.4	Network connections between trusted and untrusted networks are controlled.	Boundary Protection	Boundary Filtering System
PCI DSS (v4.0)	1.5	Risks to the CDE from computing devices that are able to connect to both untrusted networks and the CDE are mitigated.	Internal Network Protection	Network Segmentation and Control System
PCI DSS (v4.0)	2.1	Processes and mechanisms for applying secure configurations to all system components are defined and understood.	System Protection	Configuration Management System
PCI DSS (v4.0)	2.2	System components are configured and managed securely.	System Protection	Configuration Management System
PCI DSS (v4.0)	2.3	Wireless environments are configured and managed securely.	Internal Network Protection	Wireless Access System
PCI DSS (v4.0)	3.1	Processes and mechanisms for protecting stored account data are defined and understood.	Identity and Access Management	Access Management System
PCI DSS (v4.0)	3.2	Storage of account data is kept to a minimum.	Identity and Access Management	Data Inventory System
PCI DSS (v4.0)	3.3	Sensitive authentication data (SAD) is not stored after authorization.	Identity and Access Management	Identity Management System
PCI DSS (v4.0)	3.4	Access to displays of full PAN and ability to copy PAN is restricted.	Identity and Access Management	Access Management System
PCI DSS (v4.0)	3.5	Primary account number (PAN) is secured wherever it is stored.	Identity and Access Management	Access Management System
PCI DSS (v4.0)	3.6	Cryptographic keys used to protect stored account data are secured.	Identity and Access Management	Identity Management System
PCI DSS (v4.0)	3.7	Where cryptography is used to protect stored account data, key management processes and procedures covering all aspects of the key lifecycle are defined and implemented.	Identity and Access Management	Identity Management System

Collective Control Catalog: Normalizing and Mapping

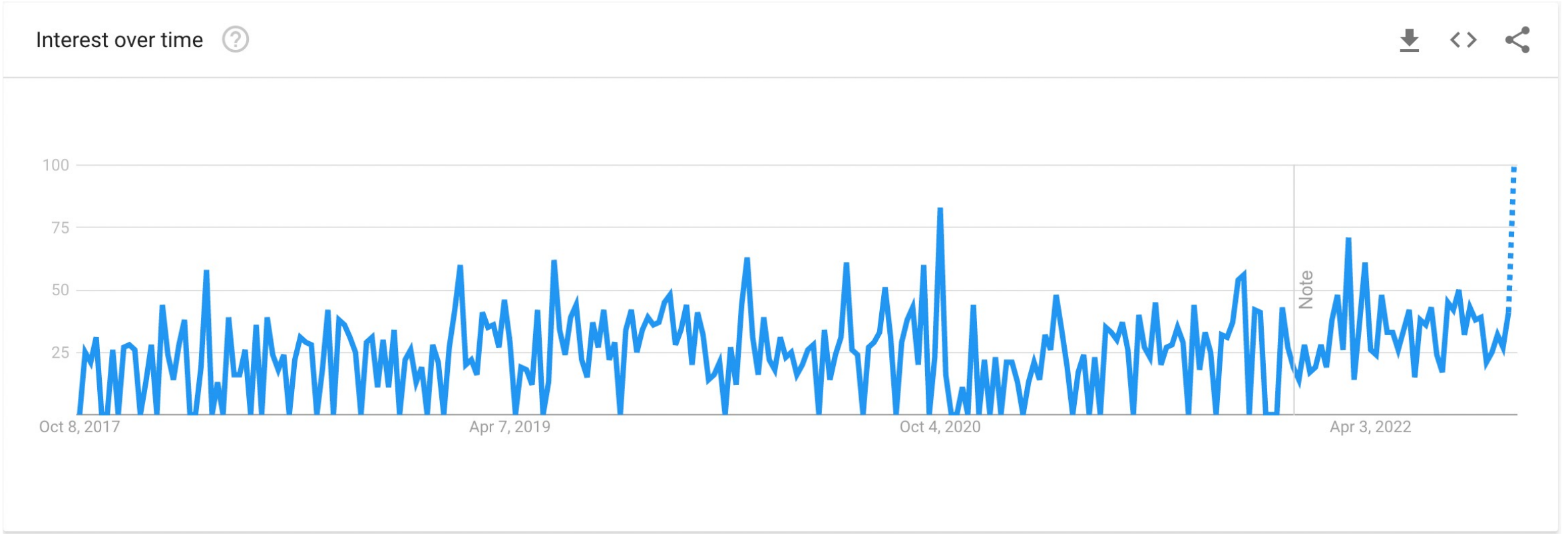
Collective Control Catalog (v2022a)							
Control Reference ID #	Control Description	CIS Control (v8.0)	CIS Control (v7.0 & 7.1	NIST CSF (v1.1)	NIST CSF (v1.0)	ISO 27002:2022	ISO 27002:2013
GOV-01	Create an information assurance charter that articulates the organization's commitment to data protection and its goals towards the confidentiality, integrity and availability of data.			ID.BE-3 PR.DS-4 PR.PT-5	ID.BE-3 PR.DS-4	8.6 8.14	A.12.1.3 A.17.2.1
GOV-02	Establish the authority of a committee to define the organization's information assurance program strategy and administer the program.						
GOV-03	Define the key stakeholders that will serve as members of the organization's information Assurance program committee.						
GOV-04	Establish that an senior executive leadership representative with authority will always be a member of this organization's committee.					5.4	
GOV-05	Define additional leadership roles and responsibilities for the organization's information security program and committee.					5.2	
GOV-06	Ensure that the organization's information security program committee is composed of key stakeholders from a cross-section of the organization, not simply technology workforce members.			ID.RM-1	ID.RM-1		
GOV-07	Ensure that the organization's information assurance program charter defines the organization's approach to addressing cyber security risk.			ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4	ID.RM-1 ID.RM-2 ID.RM-3 ID.GV-4 ID.RA-4		
GOV-08	Ensure that the organization's information assurance program charter defines the specific regulatory requirements, contractual requirements, and standards that the organization's assurance program shall achieve.			ID.BE-2 ID.GV-3 ID.RM-3	ID.BE-2 ID.GV-3 ID.RM-3		A.18.1.1 A.18.1.2
GOV-09	Define the frequency the information assurance program committee will meet, rules of order, rules for decision making, and other similar committee logistics.						

Collective Control Catalog Coverage (CIS v7.1)

Center for Internet Security (CIS) Controls v7.1



Google Trends – Past 5 Years (CIS v7.1)

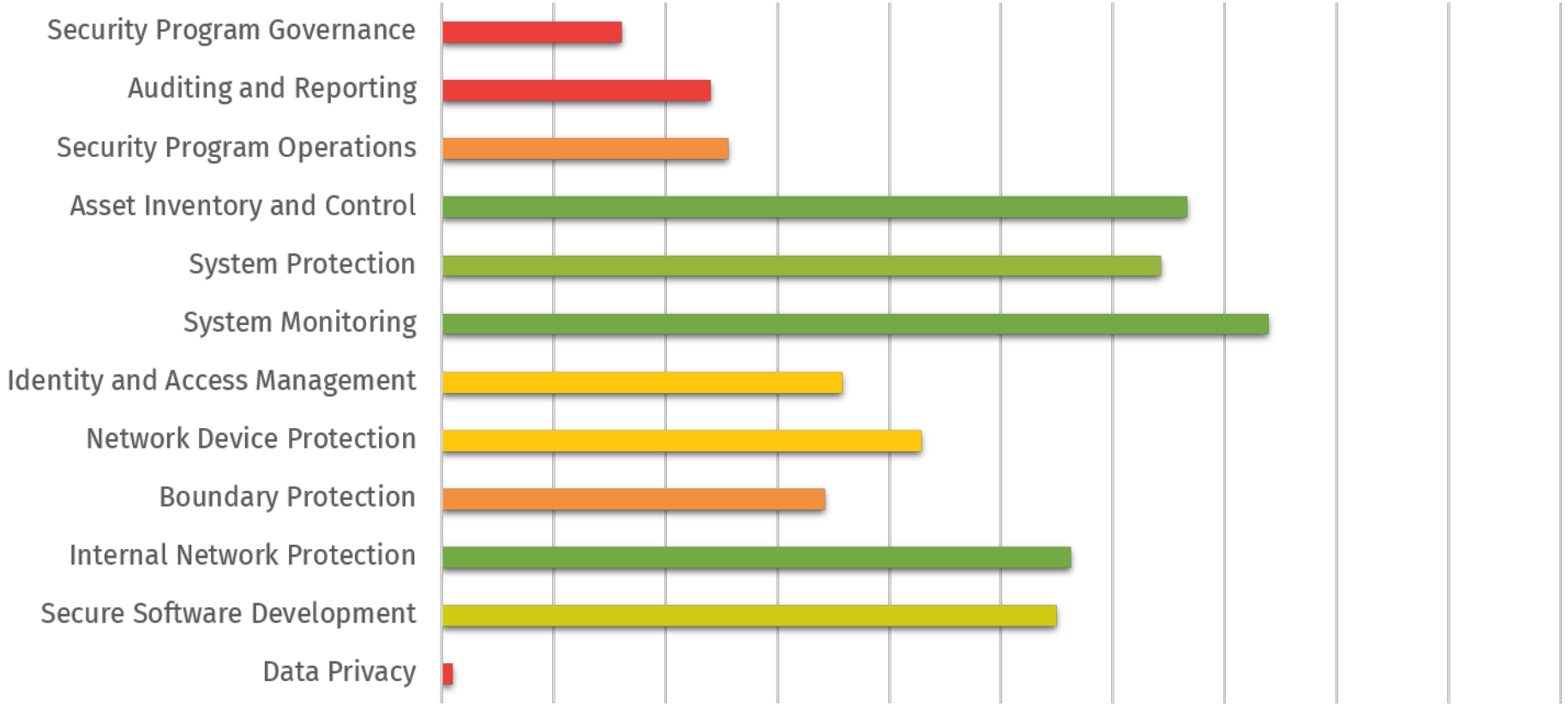


Cybersecurity Scorecard – CIS Controls v7.1

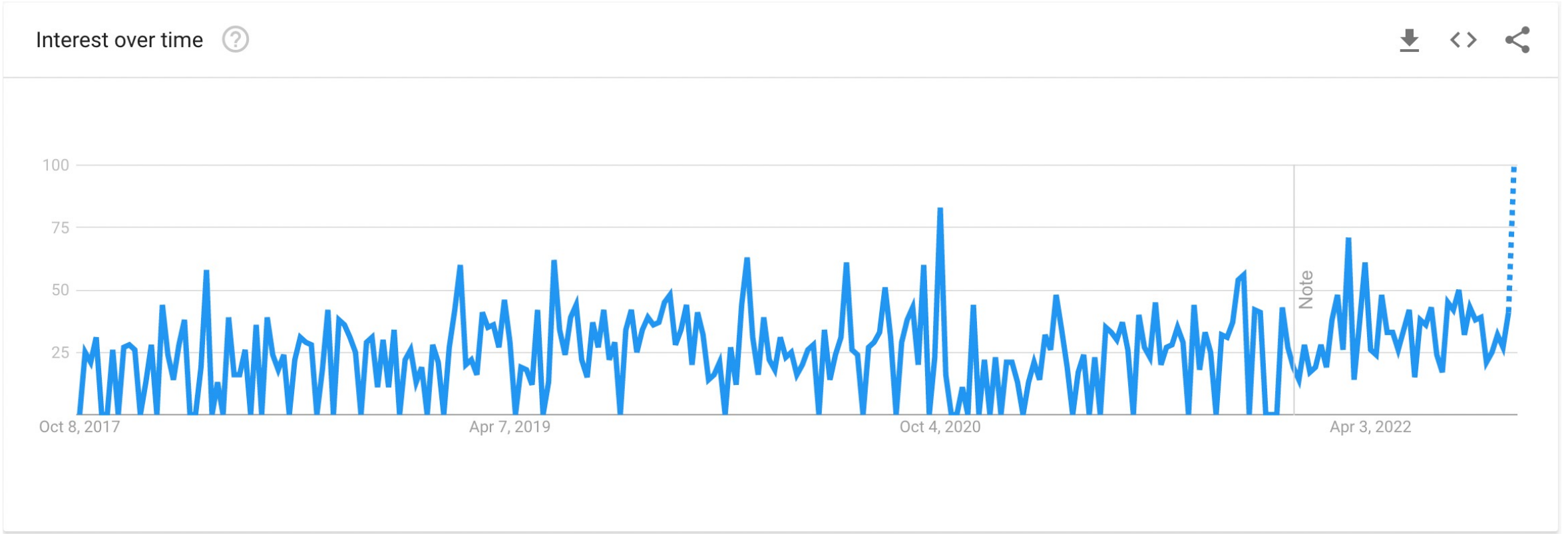
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	B
Controls Updated Recently	C
Community Driven / Open Development	A
Popularity of Standard (Google Trends)	B
Maps Threats to Controls	F
Specifically Addresses Modern Threats	B
Maps Detailed Controls to Other Control Standards	B
Tagged for Applicability (Cloud, ICS, IoT, etc)	C
International Applicability / Implementation	A
Prioritizes Controls	A
Corresponding Measures / Metrics Guide	A
Overall Score	**B**

Collective Control Catalog Coverage (CIS v8.0)

Center for Internet Security (CIS) Controls v8.0



Google Trends – Past 5 Years (CIS v8.0)

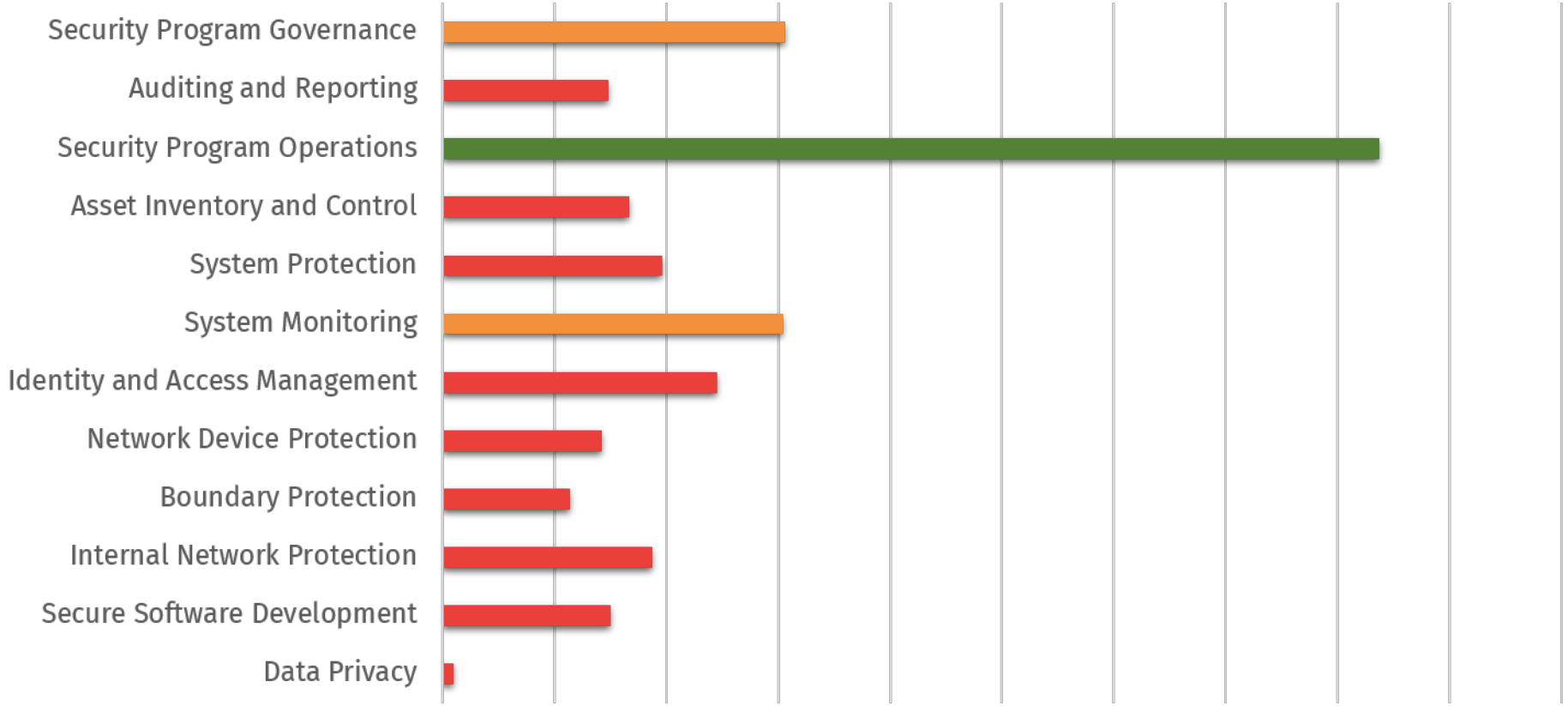


Cybersecurity Scorecard – CIS Controls v8.0

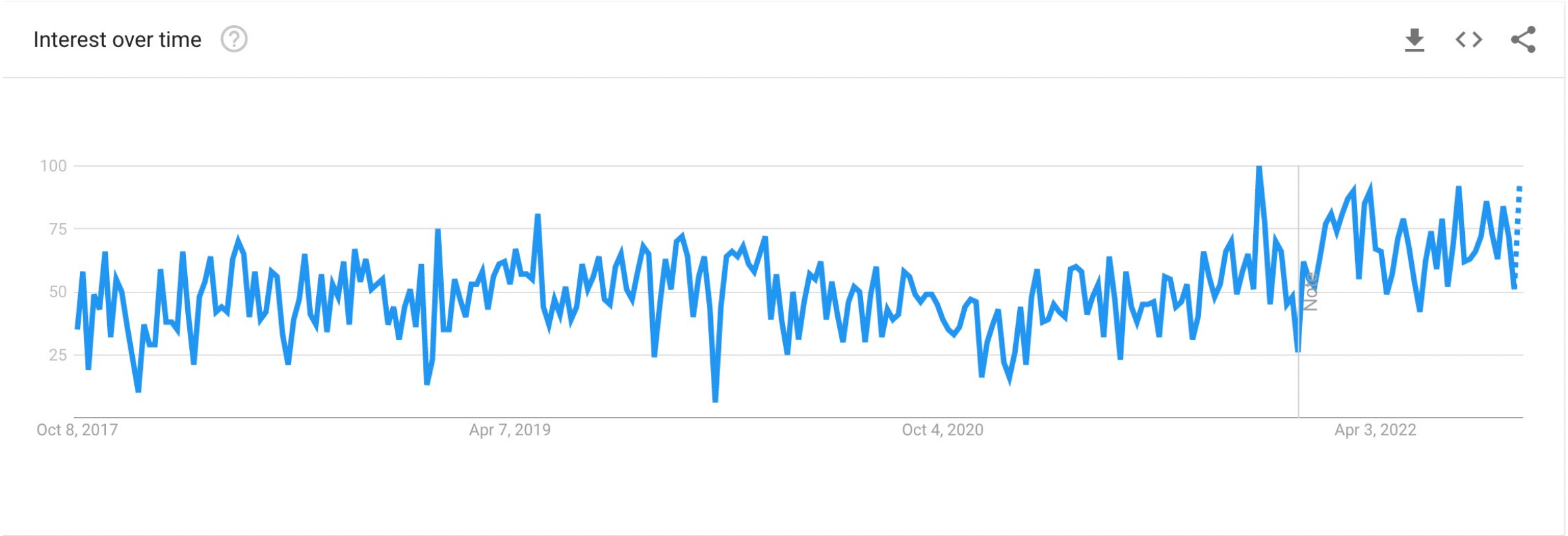
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	B
Community Driven / Open Development	B
Popularity of Standard (Google Trends)	B
Maps Threats to Controls	F
Specifically Addresses Modern Threats	B
Maps Detailed Controls to Other Control Standards	C
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	A
Prioritizes Controls	B
Corresponding Measures / Metrics Guide	F
Overall Score	**C+**

Collective Control Catalog Coverage (NIST CSF)

NIST Cybersecurity Framework (CSF v1.1)



Google Trends – Past 5 Years (NIST CSF)

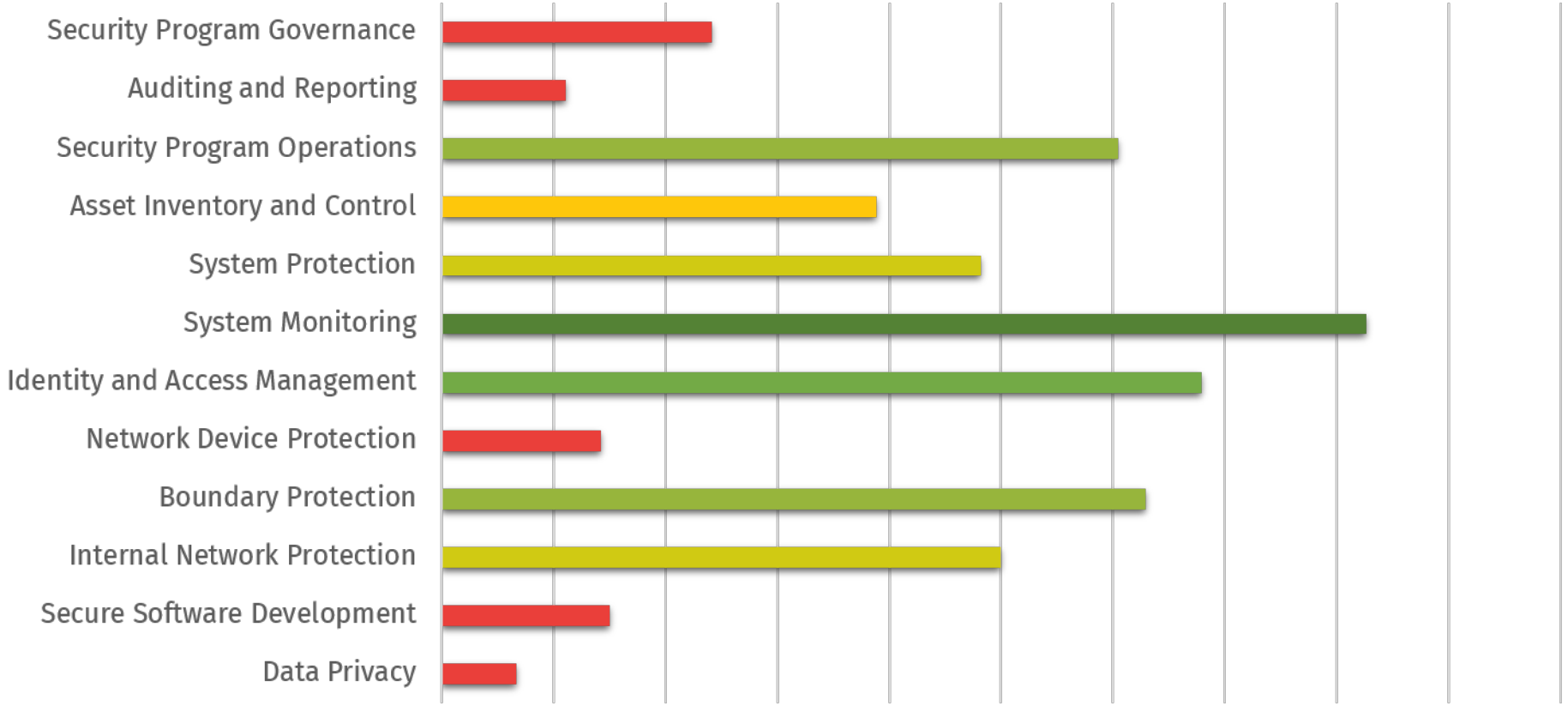


Cybersecurity Scorecard – NIST CSF (v1.1)

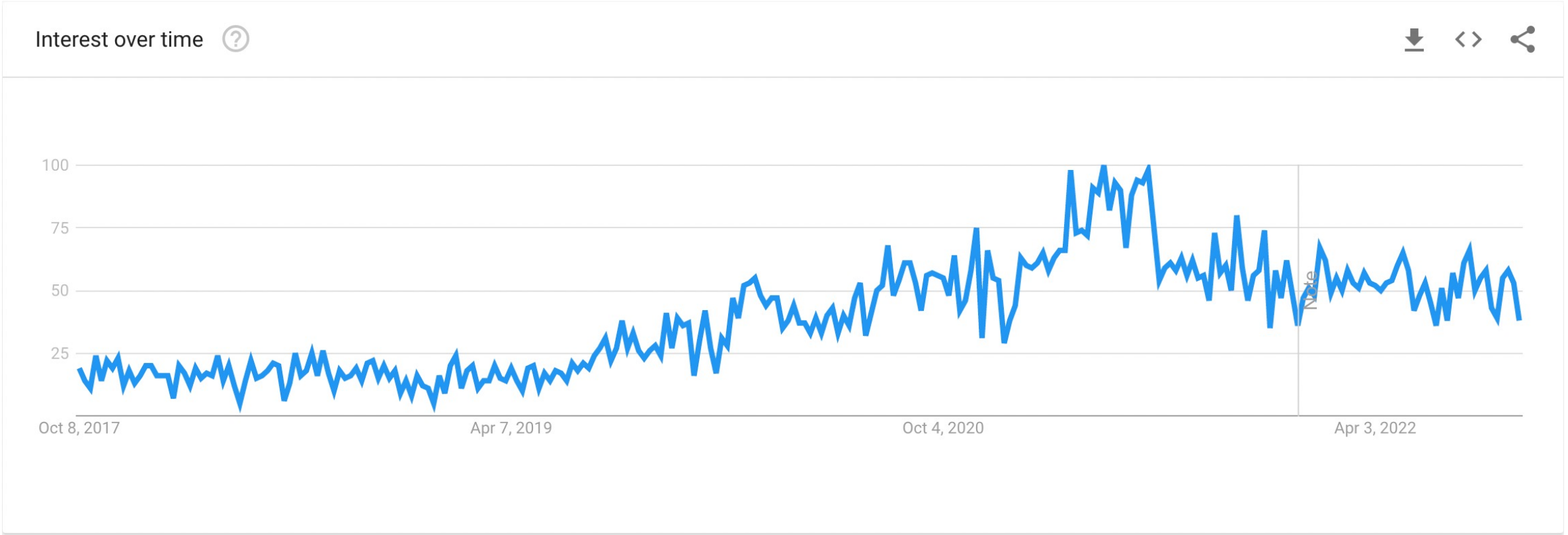
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	C
Privacy Controls Addressed	F
Technical Controls Addressed	D
Controls Updated Recently	D
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	C
Maps Threats to Controls	F
Specifically Addresses Modern Threats	F
Maps Detailed Controls to Other Control Standards	C
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	D
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**D+**

Collective Control Catalog Coverage (CMMC)

Cybersecurity Maturity Model Certification (v1.02)



Google Trends – Past 5 Years (CMMC)

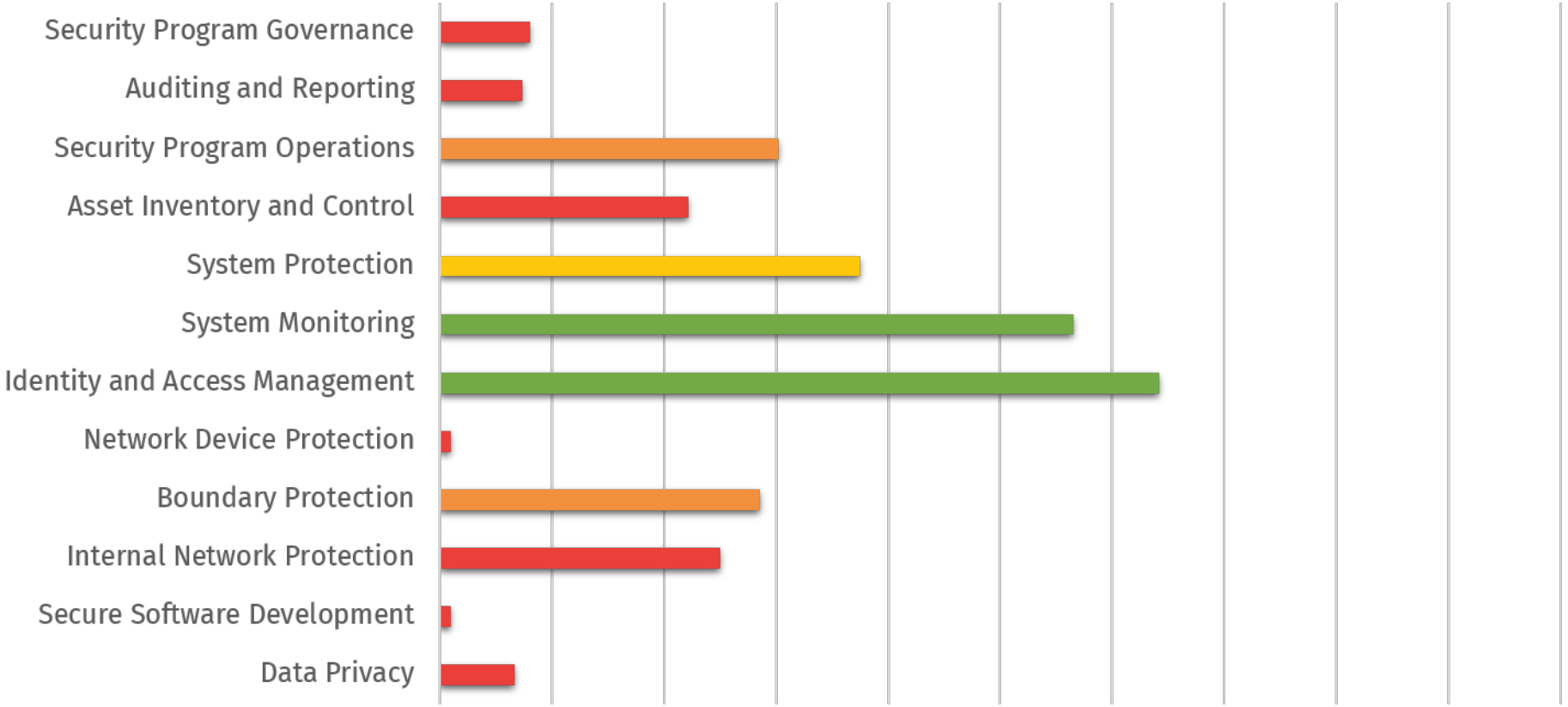


Cybersecurity Scorecard – CMMC (v1.02)

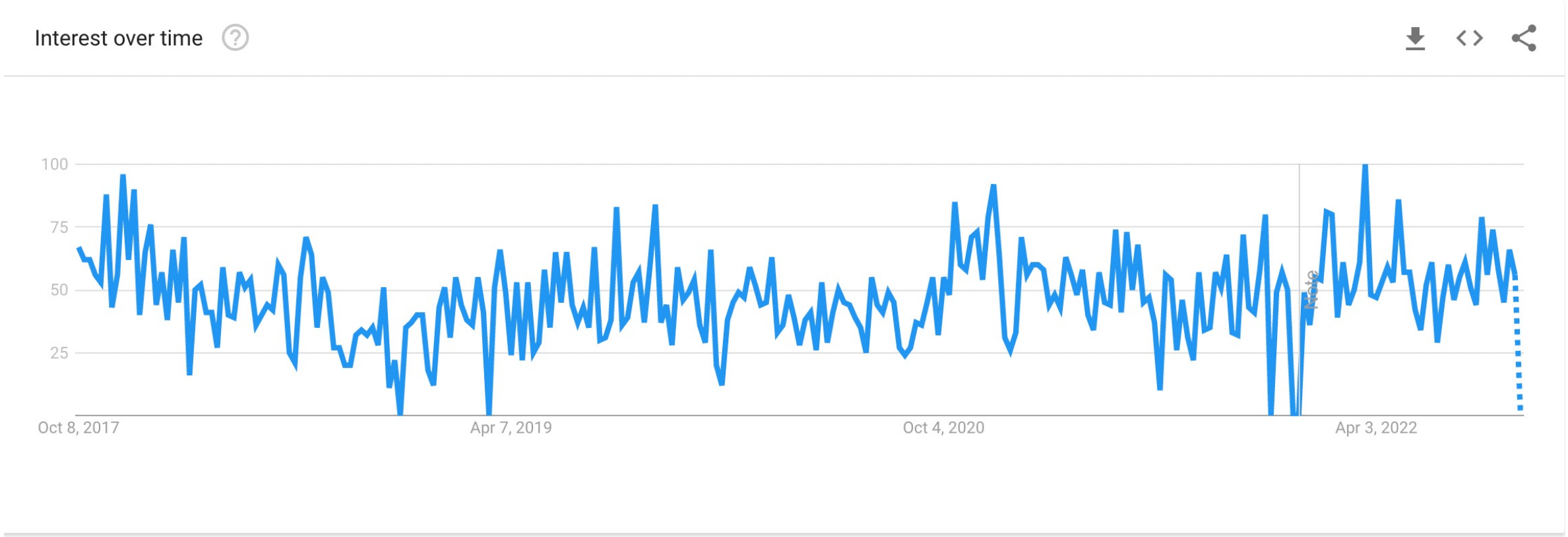
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	C
Privacy Controls Addressed	F
Technical Controls Addressed	B
Controls Updated Recently	B
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	C
Maps Threats to Controls	F
Specifically Addresses Modern Threats	B
Maps Detailed Controls to Other Control Standards	C
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	D
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**C**

Collective Control Catalog Coverage (NIST 800-171)

NIST 800-171 (rev2)



Google Trends – Past 5 Years (NIST 800-171)



Cybersecurity Scorecard – NIST 800-171 (rev2)

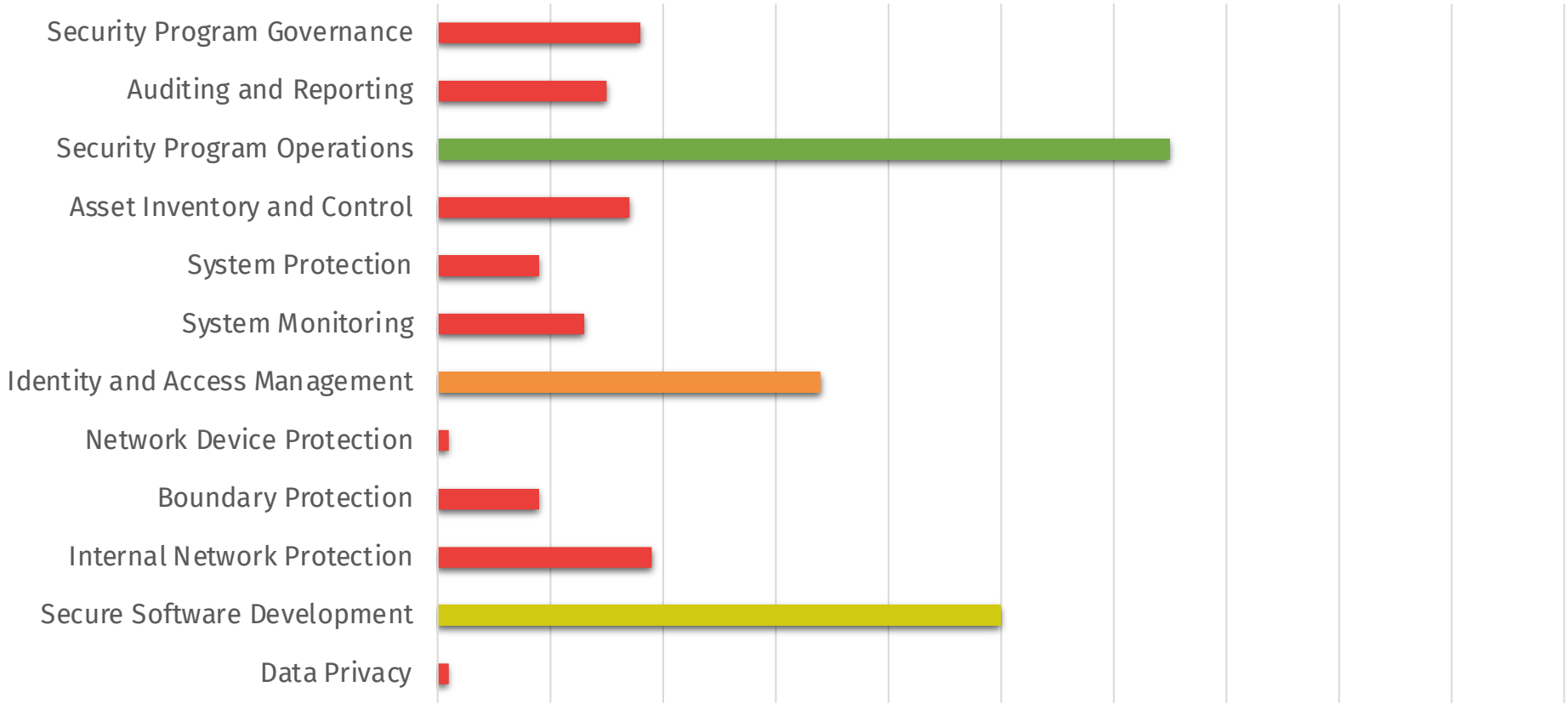
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	B
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	C
Maps Threats to Controls	F
Specifically Addresses Modern Threats	C
Maps Detailed Controls to Other Control Standards	D
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	D
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**C-**

Collective Control Catalog Coverage (ISO 27002)

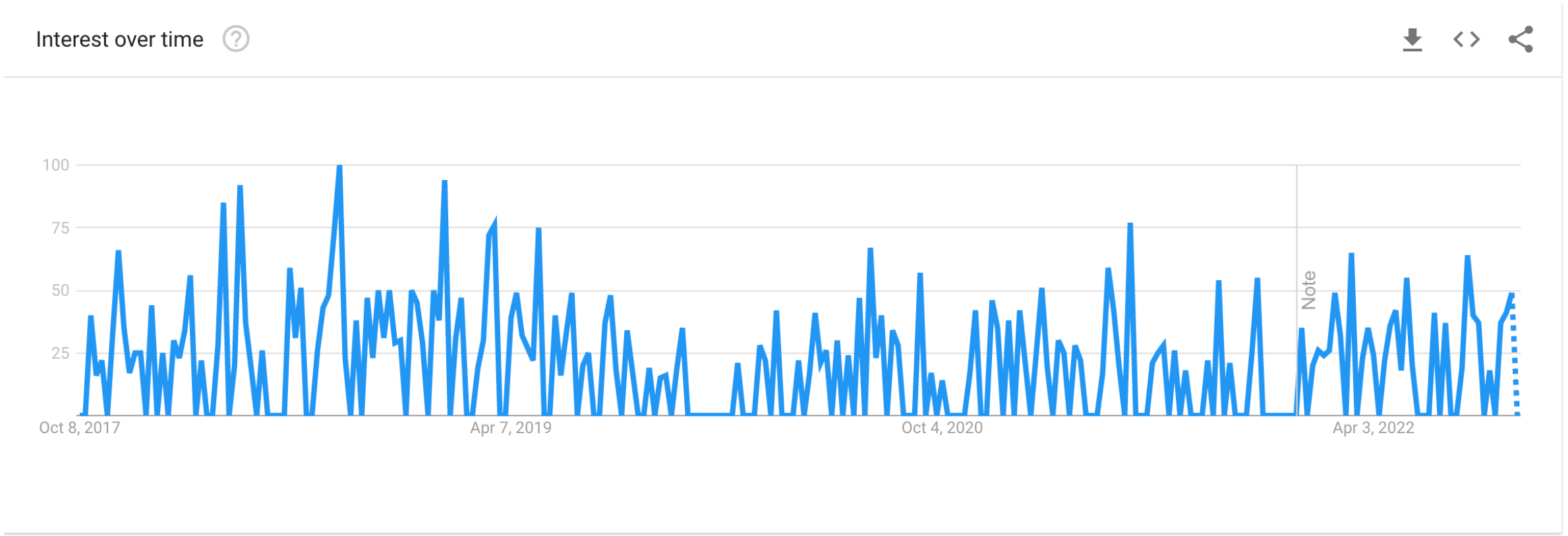
ISO 27002:2013

Collective Control Catalog Coverage (ISO 27002)

ISO 27002:2022



Google Trends – Past 5 Years (ISO 27002)

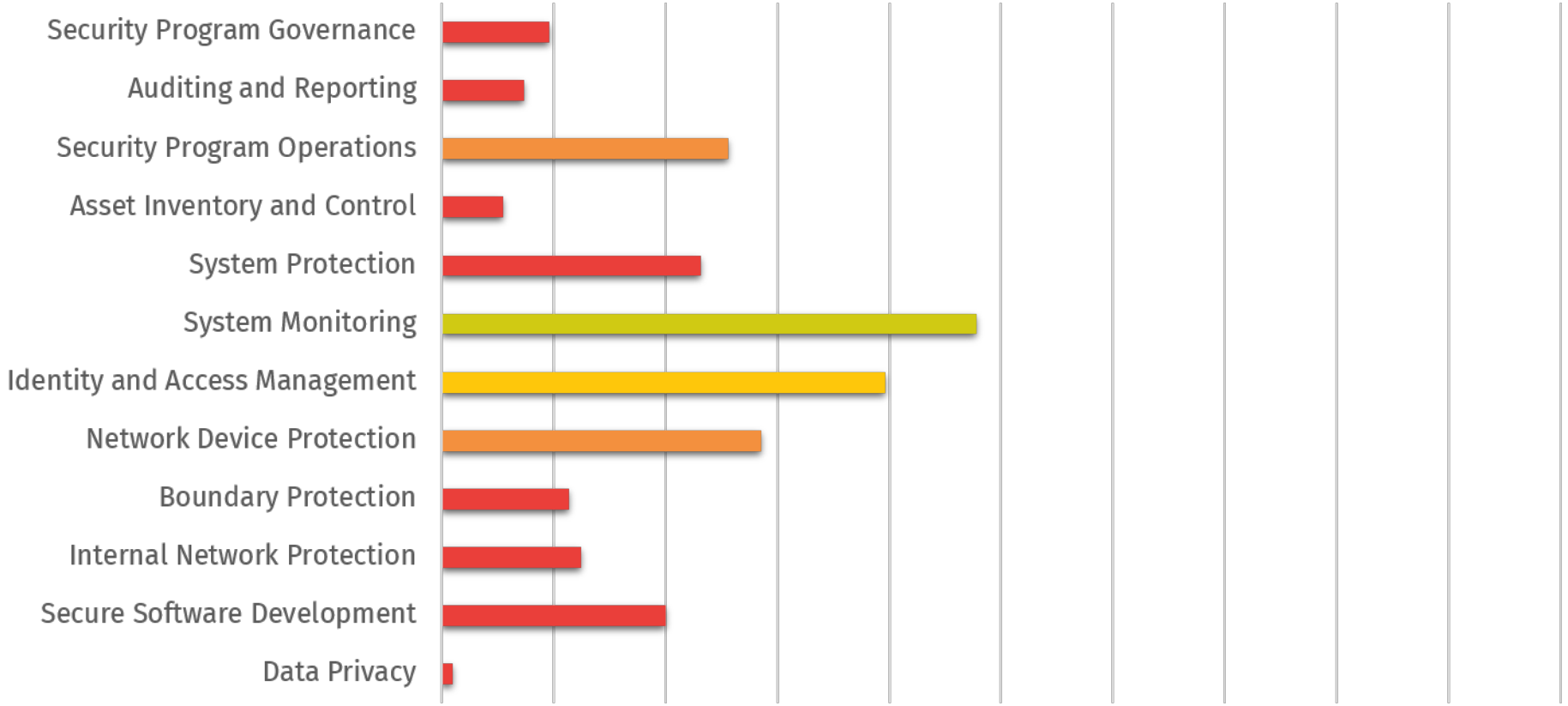


Cybersecurity Scorecard – ISO 27002:2022

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	C
Operational Controls Addressed	B
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	A
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	C
Maps Threats to Controls	F
Specifically Addresses Modern Threats	F
Maps Detailed Controls to Other Control Standards	D
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	A
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	C
Overall Score	**C-**

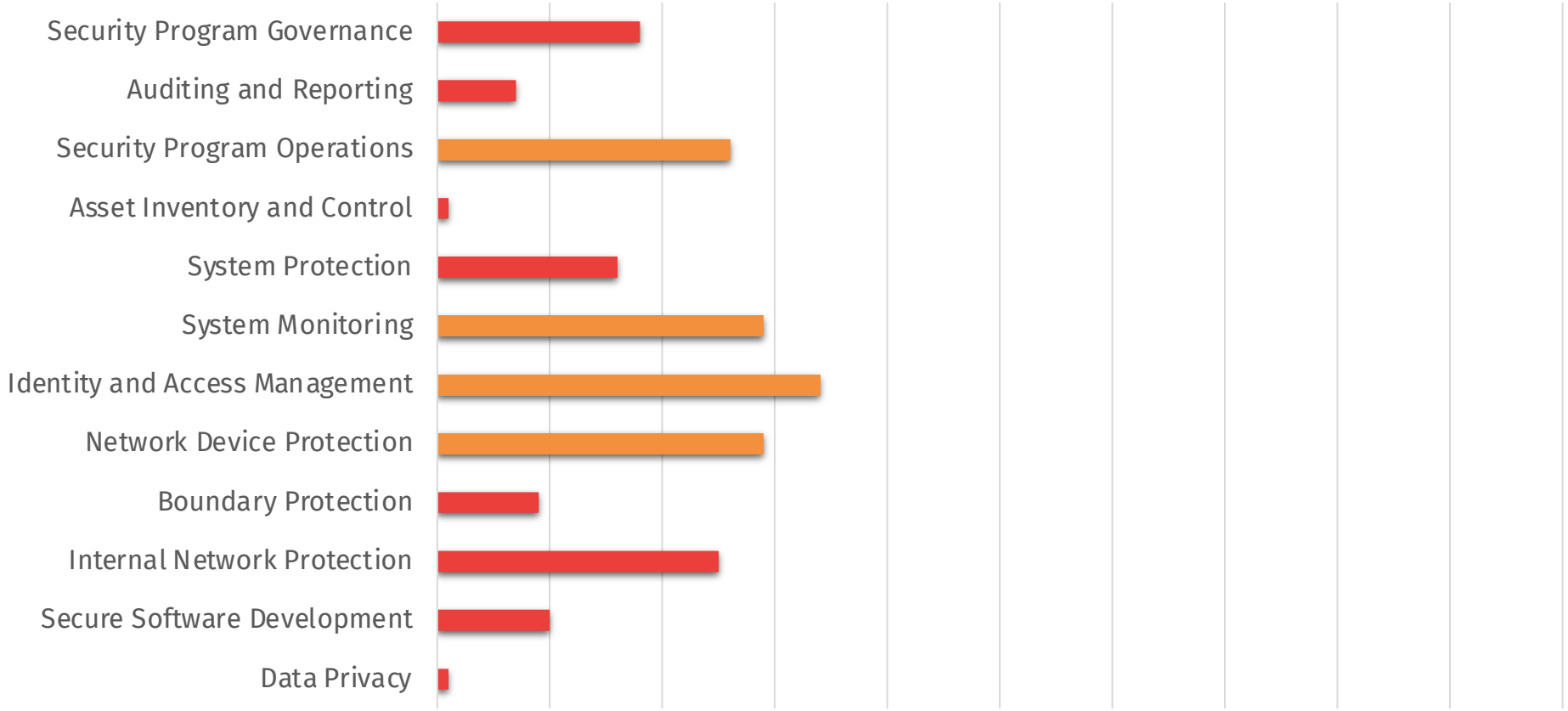
Collective Control Catalog Coverage (PCI DSS)

Payment Card International (PCI) Data Security Standard (v3.2)

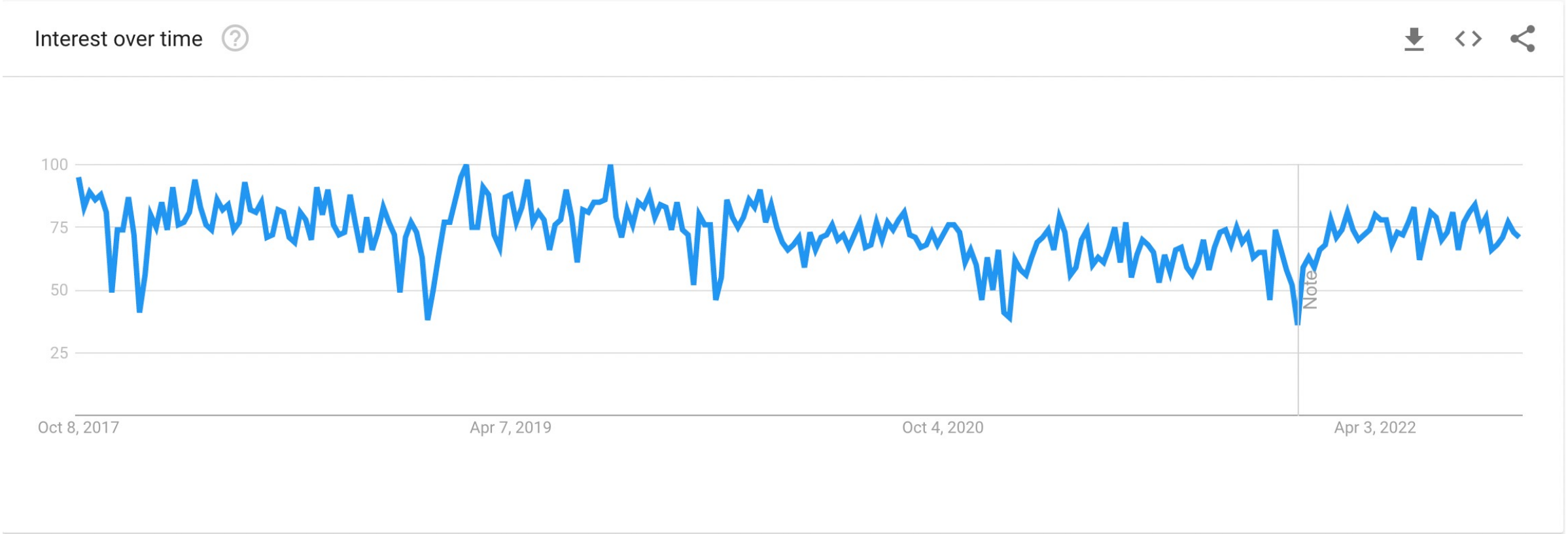


Collective Control Catalog Coverage (PCI DSS)

Payment Card International (PCI) Data Security Standard (v4.0)



Google Trends – Past 5 Years (PCI DSS)

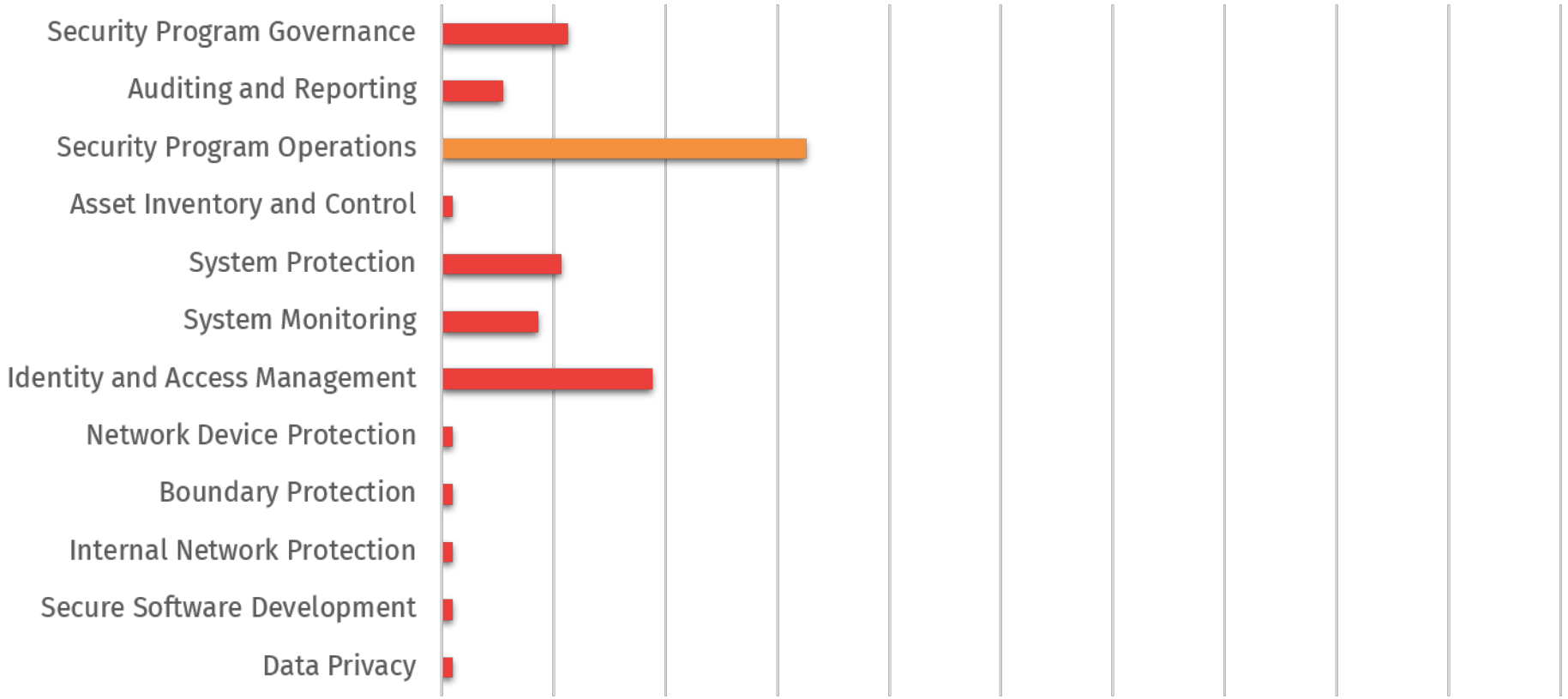


Cybersecurity Scorecard – PCI DSS (v4.0)

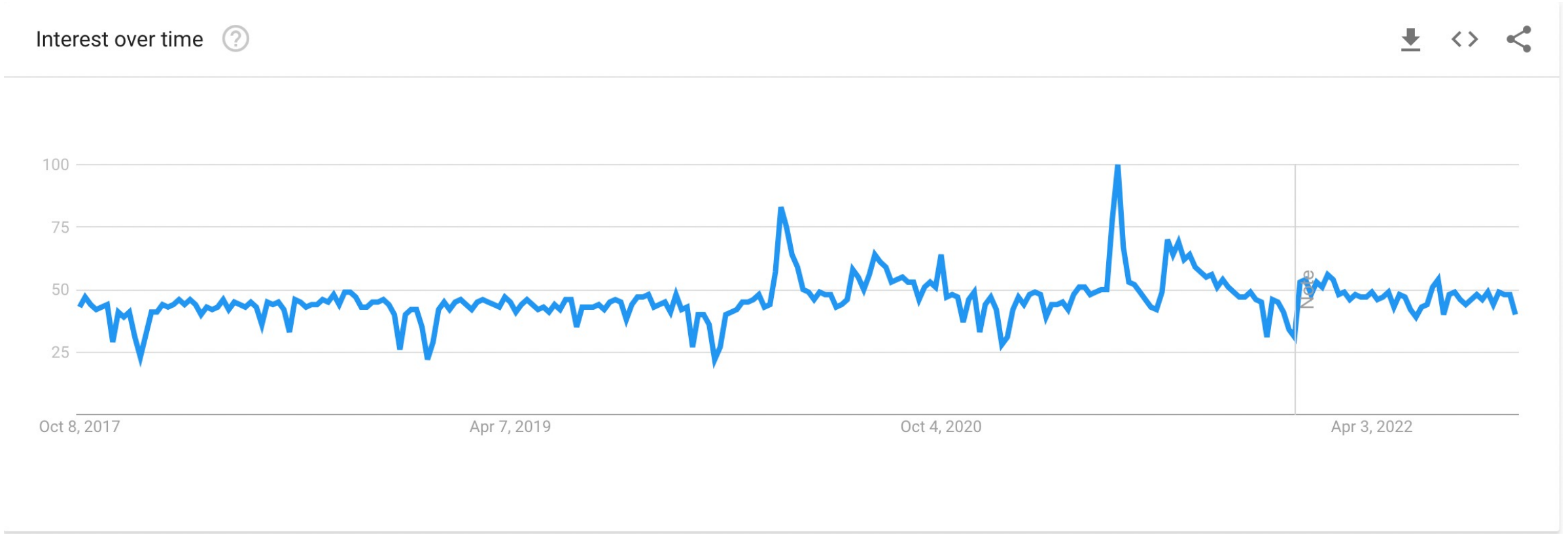
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	A
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	C
Maps Threats to Controls	F
Specifically Addresses Modern Threats	D
Maps Detailed Controls to Other Control Standards	D
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	B
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**C-**

Collective Control Catalog Coverage (HIPAA)

HIPAA Security Rule



Google Trends – Past 5 Years (HIPAA)

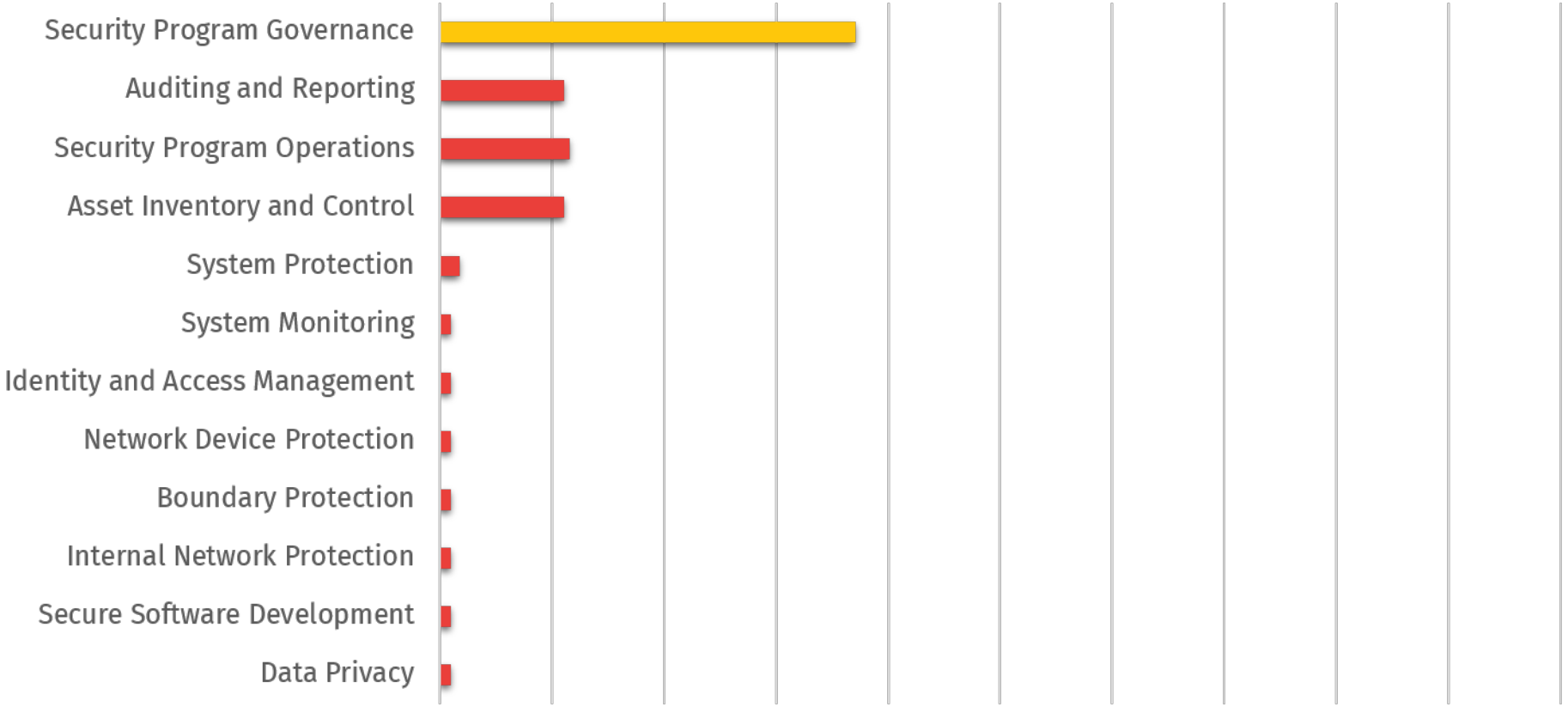


Cybersecurity Scorecard – HIPAA

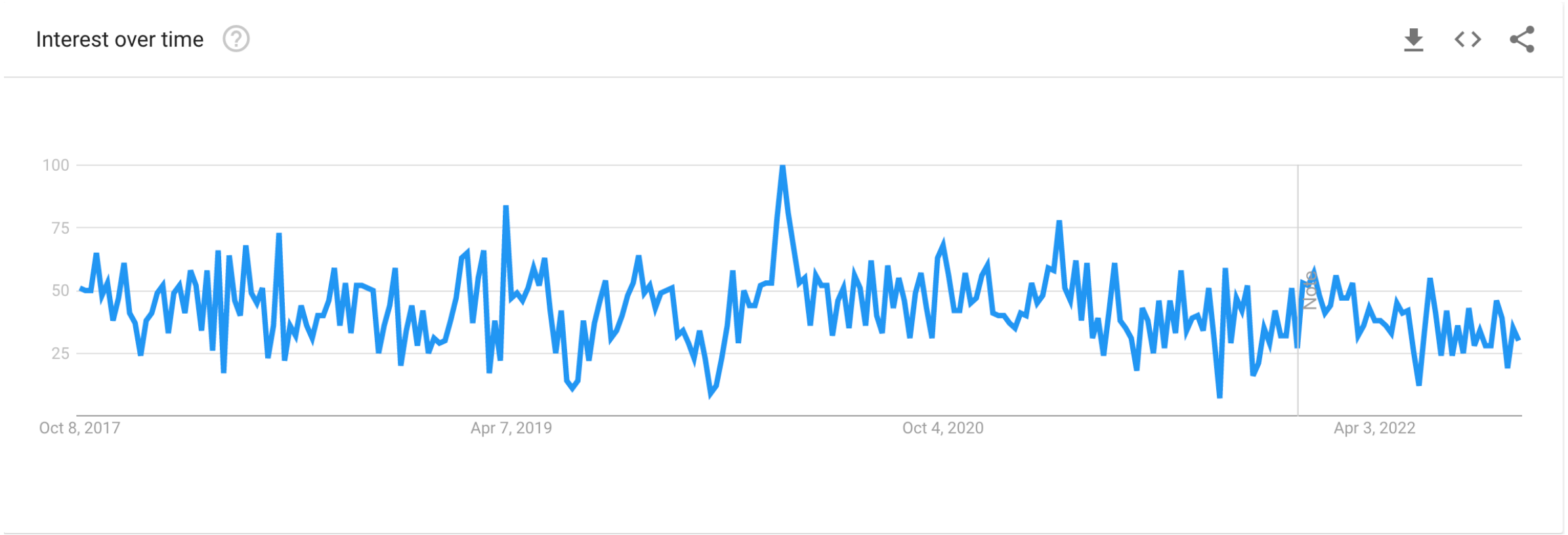
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	D
Controls Updated Recently	F
Community Driven / Open Development	F
Popularity of Standard (Google Trends)	D
Maps Threats to Controls	F
Specifically Addresses Modern Threats	F
Maps Detailed Controls to Other Control Standards	D
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	D
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**D**

Collective Control Catalog Coverage (COBIT)

COBIT (v5)



Google Trends – Past 5 Years (COBIT)

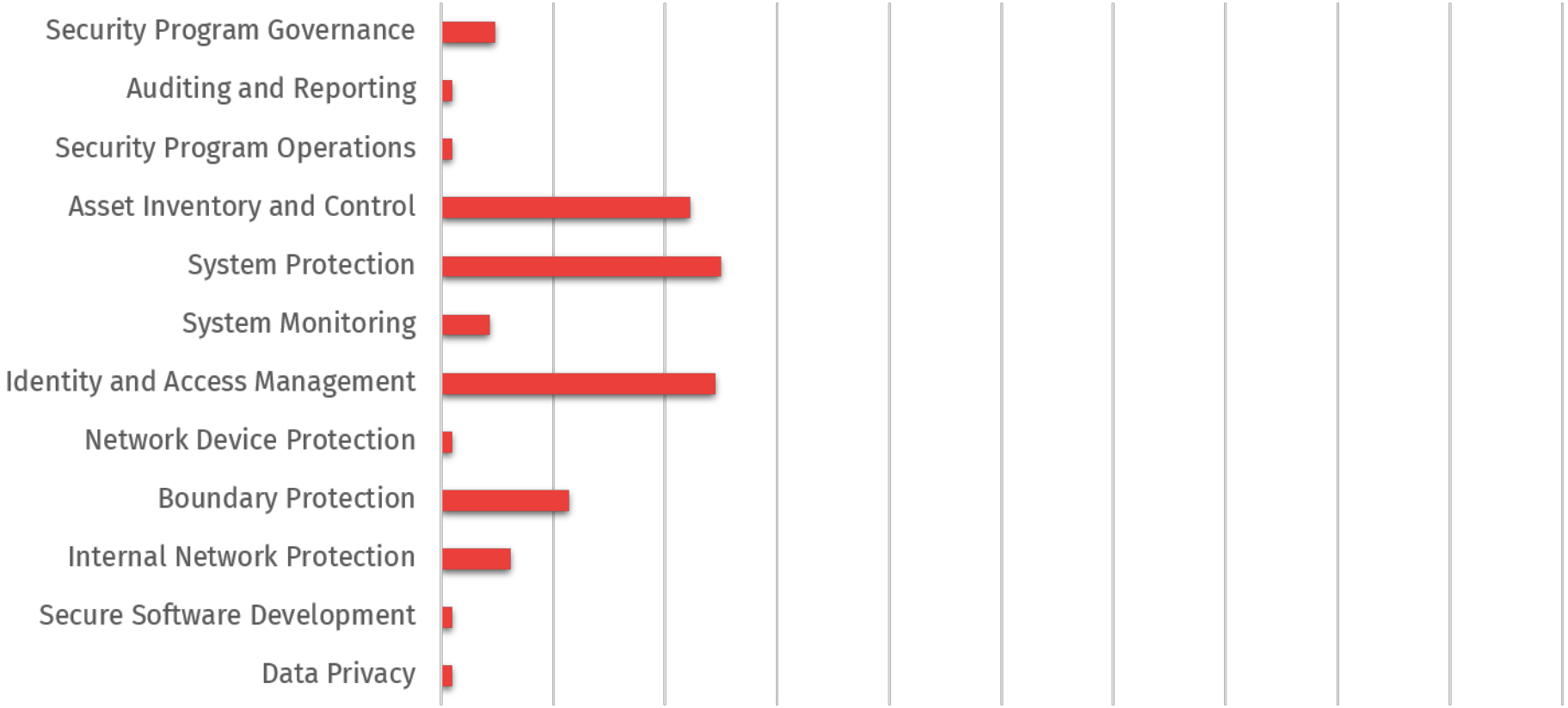


Cybersecurity Scorecard – COBIT

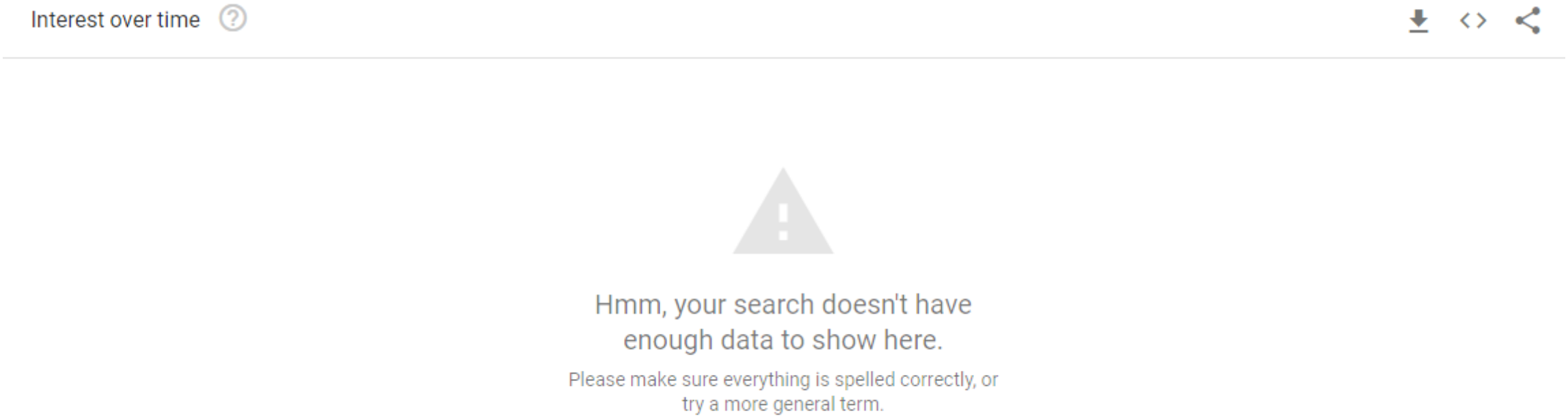
Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	C
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	F
Controls Updated Recently	F
Community Driven / Open Development	D
Popularity of Standard (Google Trends)	D
Maps Threats to Controls	F
Specifically Addresses Modern Threats	F
Maps Detailed Controls to Other Control Standards	F
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	C
Prioritizes Controls	F
Corresponding Measures / Metrics Guide	F
Overall Score	**D**

Collective Control Catalog Coverage (MITRE)

MITRE Enterprise Mitigations



Google Trends – Past 5 Years (MITRE)



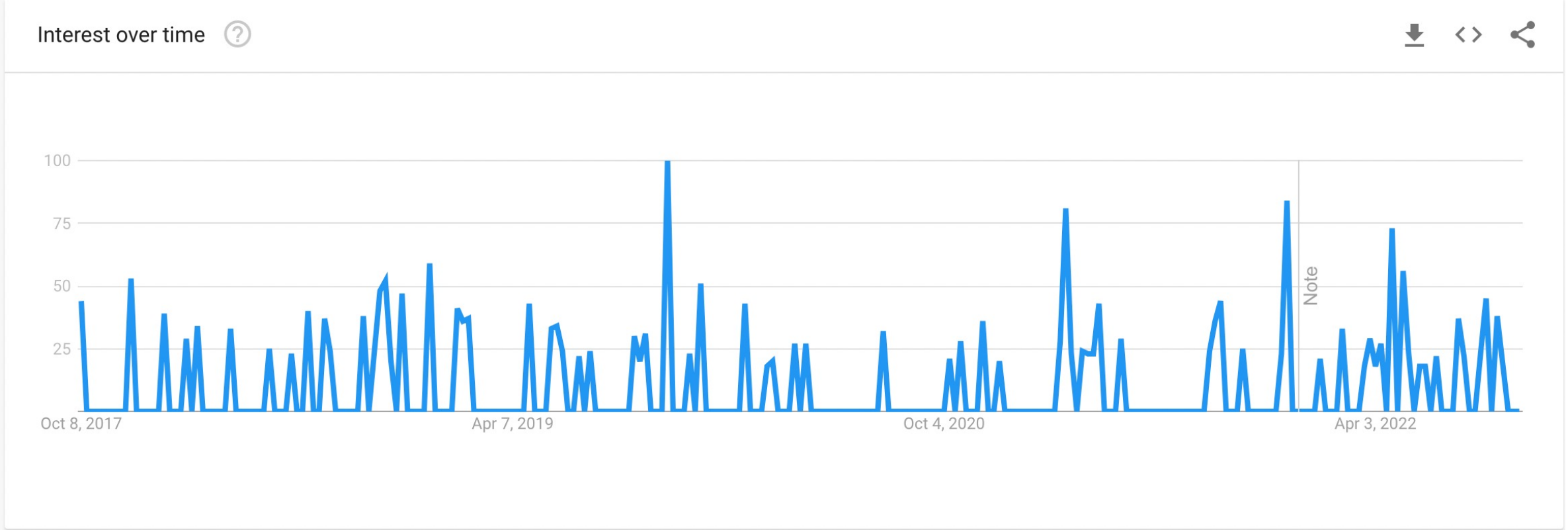
Cybersecurity Scorecard – MITRE Enterprise Mitigations

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	F
Operational Controls Addressed	F
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	B
Community Driven / Open Development	C
Popularity of Standard (Google Trends)	F
Maps Threats to Controls	A
Specifically Addresses Modern Threats	A
Maps Detailed Controls to Other Control Standards	F
Tagged for Applicability (Cloud, ICS, IoT, etc)	F
International Applicability / Implementation	C
Prioritizes Controls	D
Corresponding Measures / Metrics Guide	F
Overall Score	**C-**

Collective Control Catalog Coverage (CCC)

Collective Control Catalog (v2021)

Google Trends – Past 5 Years (CCC)



Cybersecurity Scorecard – CCC (v2021)

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	A
Operational Controls Addressed	B
Privacy Controls Addressed	B
Technical Controls Addressed	A
Controls Updated Recently	A
Community Driven / Open Development	B
Popularity of Standard (Google Trends)	D
Maps Threats to Controls	F
Specifically Addresses Modern Threats	A
Maps Detailed Controls to Other Control Standards	A
Tagged for Applicability (Cloud, ICS, IoT, etc)	B
International Applicability / Implementation	C
Prioritizes Controls	A
Corresponding Measures / Metrics Guide	A
Overall Score	**A-**

2021 Overall Cybersecurity Standards Scorecard

Cybersecurity Standard	Score (2021)
CIS Controls (v7.1)	B
CIS Controls (v8.0)	C+
NIST CyberSecurity Framework (v1.1)	D+
Cybersecurity Maturity Model Certification (v1.02)	C
NIST SP 800-171 (rev2)	C-
ISO 27002:2022	C-
PCI DSS (v4.0)	C-
HIPAA	D
COBIT (v5)	D
MITRE Enterprise Mitigations	C-
Collective Control Catalog (v2022)	A-

Collective Control Catalog: Prioritization and Tagging

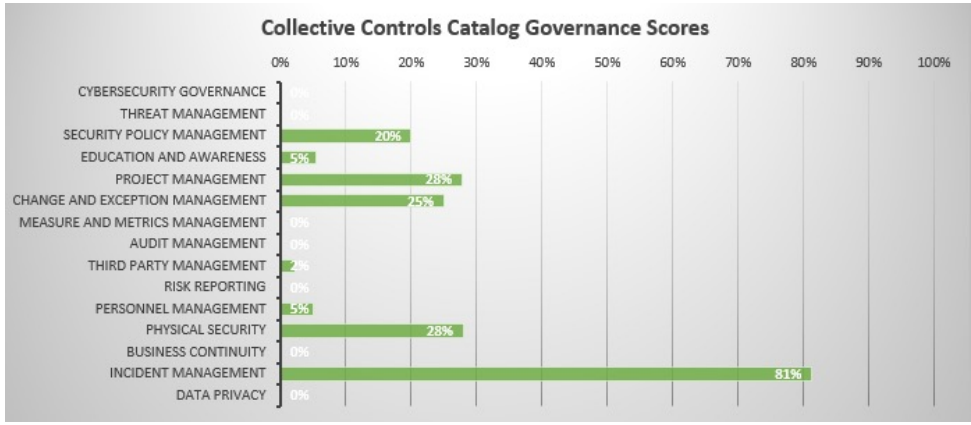
AuditScripts

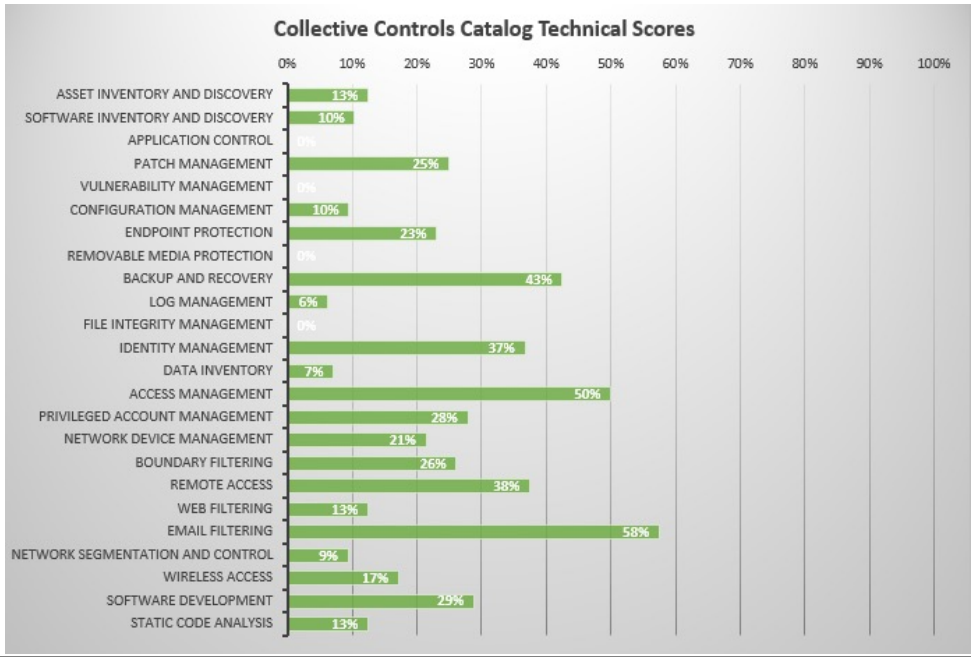
Collective Control Catalog Tagging (v2022a)

Reference ID #	Description	Initial Control (Priority 1)	Managed Control (Priority 2)	Defined Control (Priority 3)	Measured Control (Priority 4)
GOV-01	Create an information assurance charter that articulates the organization's commitment to data protection and its goals towards the confidentiality, integrity and availability of data.		X		
GOV-02	Establish the authority of a committee to define the organization's information assurance program strategy and administer the program.		X		
GOV-03	Define the key stakeholders that will serve as members of the organization's information Assurance program committee.		X		
GOV-04	Establish that an senior executive leadership representative with authority will always be a member of this organization's committee.		X		
GOV-05	Define additional leadership roles and responsibilities for the organization's information security program and committee.		X		
GOV-06	Ensure that the organization's information security program committee is composed of key stakeholders from a cross-section of the organization, not simply technology workforce members.		X		
GOV-07	Ensure that the organization's information assurance program charter defines the organization's approach to addressing cyber security risk.			X	
GOV-08	Ensure that the organization's information assurance program charter defines the specific regulatory requirements, contractual requirements, and standards that the organization's assurance program shall achieve.			X	
GOV-09	Define the frequency the information assurance program committee will meet, rules of order, rules for decision making, and other similar committee logistics.			X	
GOV-10	Define the program's scope and applicability to the individual business units, subsidiaries, or sites within the organization.			X	
GOV-11	Ensure that the senior levels of executive leadership formally approve the organization's information security program charter.			X	

Simple Sample Reporting Tool

- Microsoft Excel is still the most popular risk management tool available to cybersecurity practitioners
- Sometimes it is better not to be complicated
- The tool to the right is an example of using Microsoft Excel to score risk against an agreed upon set of controls
- In this case, using the free AuditScripts.com tool to measure against the Collective Controls Catalog (CCC)





Future of the Project

- The goal is to continue to develop this framework, with collective community support

- At least annually a new version of this framework, with supporting resources, will be released to the community for their consideration

- Specific Project Goals for 2023:
  - Include additional standards / mappings (ISO 27002, PCI, etc)
  - Include additional content for DevOps and serverless architectures
  - Document audit framework and template audit plan

Next Steps - Call for Action

As a cybersecurity professional, what comes next?

Learning from presentations such as this is wonderful, but action is better:

1. Has your organization's leadership formally chartered a program to address these issues?
2. Has your organization formally agreed on a common set of cybersecurity controls to help ensure you achieve your business objectives?
3. Has your organization been assessed against a common set of cybersecurity controls to better understand their present state?
4. Has your organization defined a plan to address the most critical cybersecurity control gaps that were identified in the assessment?

COURSE RESOURCES AND CONTACT INFORMATION

JAMES TARALA

Principal Consultant at Enclave Security

James.tarala@enclavesecurity.com

RESOURCES FOR FURTHER STUDY:

SANS Webcasts

AuditScripts.com Risk Resources

SANS MGT415: A Practical Introduction to Cyber Security Risk Management

SANS SEC566: Implementing and Auditing CIS Critical Controls