



# Cybersecurity Standards Scorecard (2021 Edition)

## Problem Statement – Cybersecurity Standards

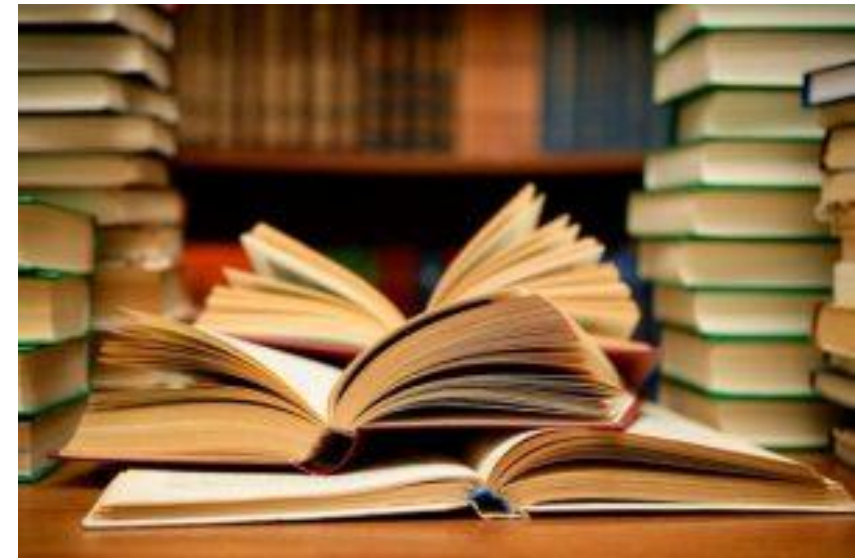
- At the present time there are dozens of cybersecurity standards and regulations around the world
- There is a general belief that all standards are basically the same – *this could not be further from the truth*
- Organizations tend to choose a cybersecurity standard based on popularity or experience 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 2021 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
  - PCI DSS (v3.2)
  - HIPAA
  - COBIT (v5)
  - MITRE Enterprise Mitigations
  - Collective Control Catalog (v2021)



# 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 2000 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



## Control Frameworks Mapped to the Control Systems (v1.0g)



Framework	Recommendation	Description	Control Category	Control System
CMMC (v1)	SI.1.212	Update malicious code protection mechanisms when new releases are available.	System Protection	Endpoint Protection System
CMMC (v1)	SI.1.213	Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	System Protection	Endpoint Protection System
CMMC (v1)	SI.2.214	Monitor system security alerts and advisories and take action in response.	System Protection	Vulnerability Management System
CMMC (v1)	SI.2.216	Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	Boundary Protection	Boundary Filtering System
CMMC (v1)	SI.2.217	Identify unauthorized use of organizational systems.	System Monitoring	Log Management System
CMMC (v1)	SI.3.218	Employ spam protection mechanisms at information system access entry and exit points.	Boundary Protection	Email Filtering System
CMMC (v1)	SI.3.219	Implement email forgery protections.	Boundary Protection	Email Filtering System
CMMC (v1)	SI.3.220	Utilize sandboxing to detect or block potentially malicious email.	Boundary Protection	Email Filtering System
CMMC (v1)	SI.4.221	Use threat indicator information relevant to the information and systems being protected and effective mitigations obtained from external organizations to inform intrusion detection and threat hunting.	System Monitoring	Log Management System
CMMC (v1)	SI.5.222	Analyze system behavior to detect and mitigate execution of normal system commands and scripts that indicate malicious actions.	System Monitoring	Log Management System
CMMC (v1)	SI.5.223	Monitor individuals and system components on an ongoing basis for anomalous or suspicious behavior.	System Monitoring	Log Management System
COBIT (v5)	EDM01	Ensure Governance Framework Setting and Maintenance	Security Program Governance	Cybersecurity Governance Program
COBIT (v5)	EDM02	Ensure Benefits Delivery	Security Program Governance	Cybersecurity Governance Program
COBIT (v5)	EDM03	Ensure Risk Optimization	Security Program Governance	Cybersecurity Governance Program



# Collective Control Catalog: Normalizing and Mapping

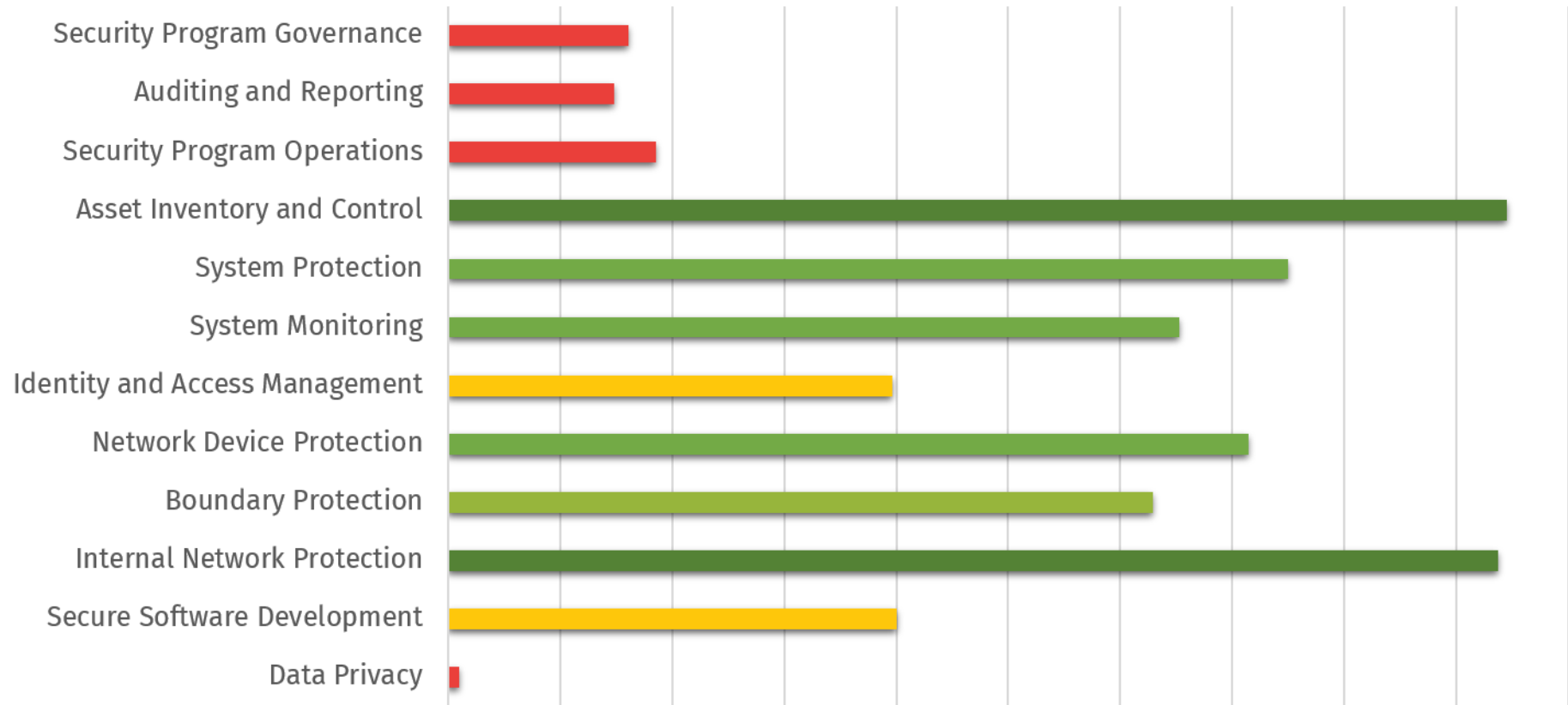


## Common Control Library (v1.0g)

Control Reference ID #	Control Description	CIS Control (v7.1)	NIST CSF (v1.1)	NIST CSF (v1.0)	ISO 27002:2013	NIST 800-171	NIST Privacy (v1.0)	Australian DSD35	CMMC (v1)
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	A.12.1.3 A.17.2.1		ID.BE-P2 PR.DS-P4		
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.								
GOV-05	Define additional leadership roles and responsibilities for the organization's information security program and committee.								
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			ID.DE-P1 GV.PO-P6 GV.RM-P1 GV.RM-P2 GV.RM-P3		
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		GV.PO-P5		

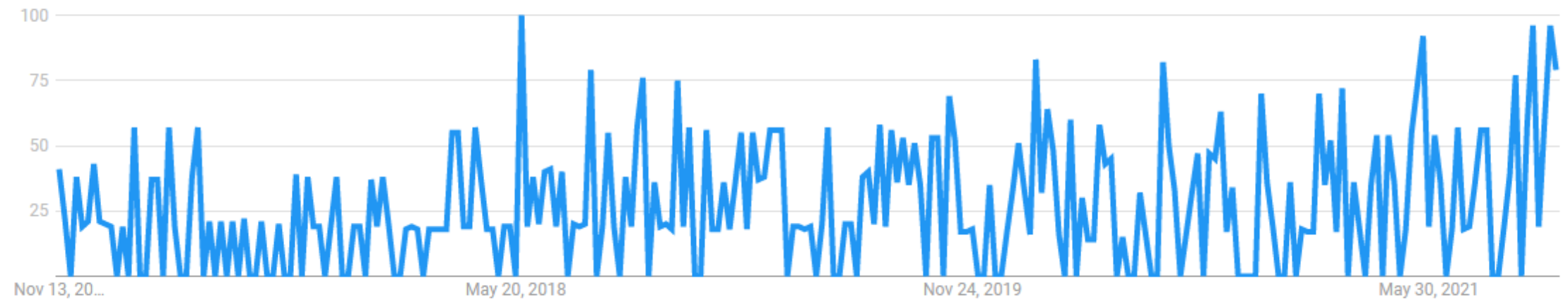
# Collective Control Catalog Coverage (CIS v7.1)

## Center for Internet Security (CIS) Controls v7.1



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

Interest over time 

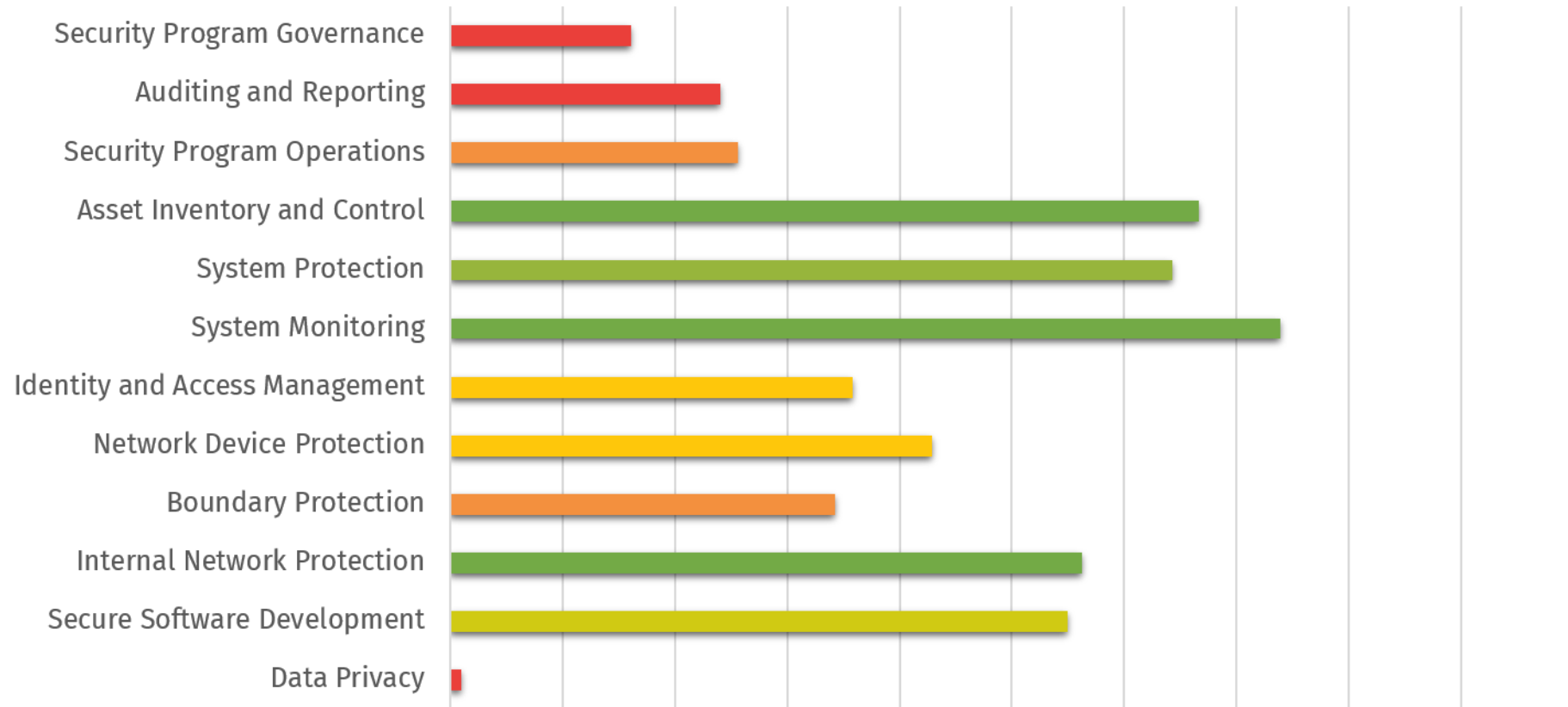


# Cybersecurity Scorecard – CIS Controls v7.1

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	B
Controls Updated Recently	B
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
<b>Overall Score</b>	<b>B</b>

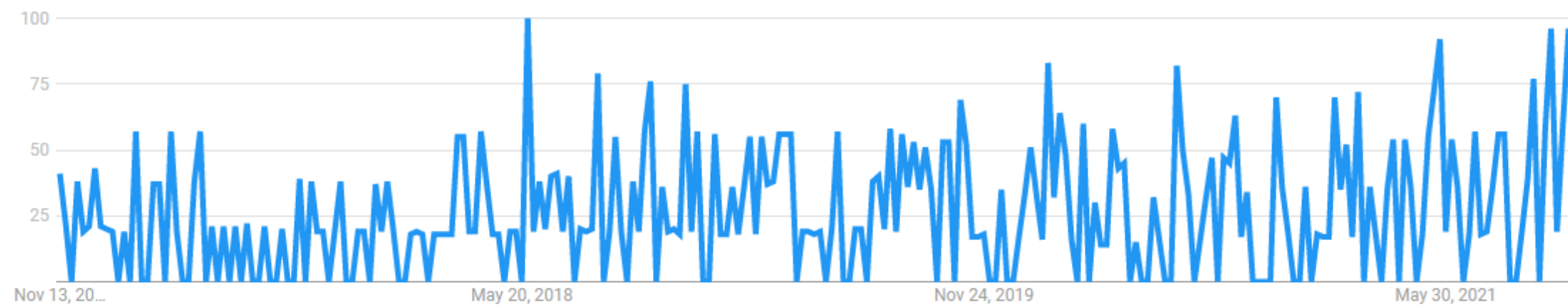
# Collective Control Catalog Coverage (CIS v8.0)

## Center for Internet Security (CIS) Controls v8.0



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

Interest over time 

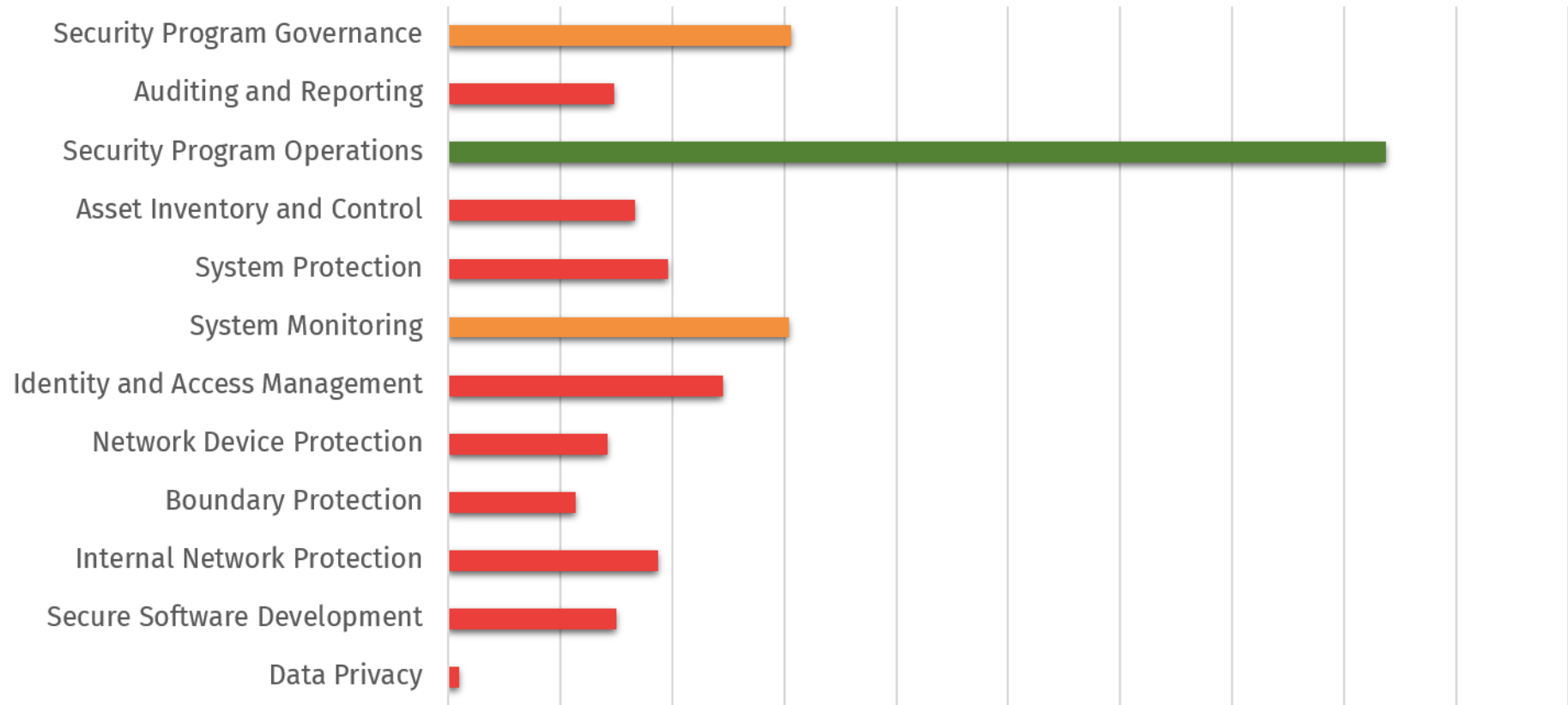


# Cybersecurity Scorecard – CIS Controls v8.0

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	A
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
<b>Overall Score</b>	<b>C+</b>

# Collective Control Catalog Coverage (NIST CSF)

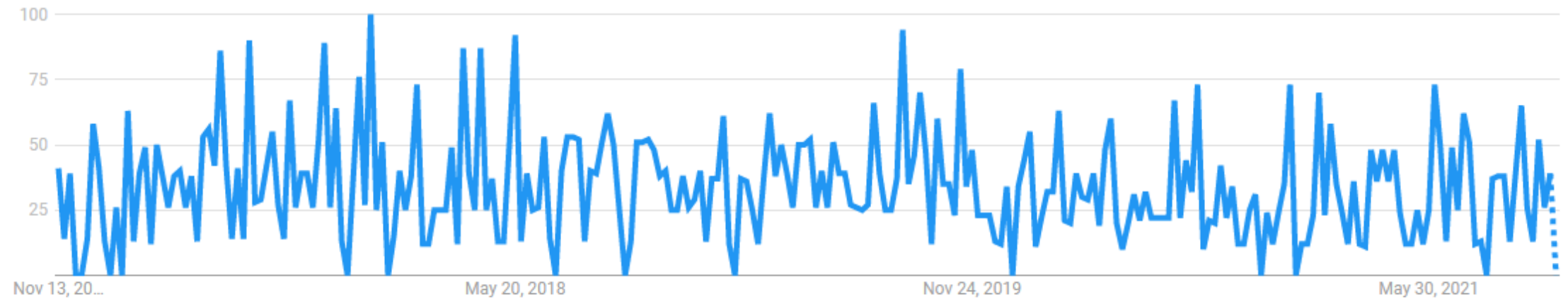
## NIST Cybersecurity Framework (CSF v1.1)





# Google Trends – Past 5 Years (NIST CSF)

Interest over time ?

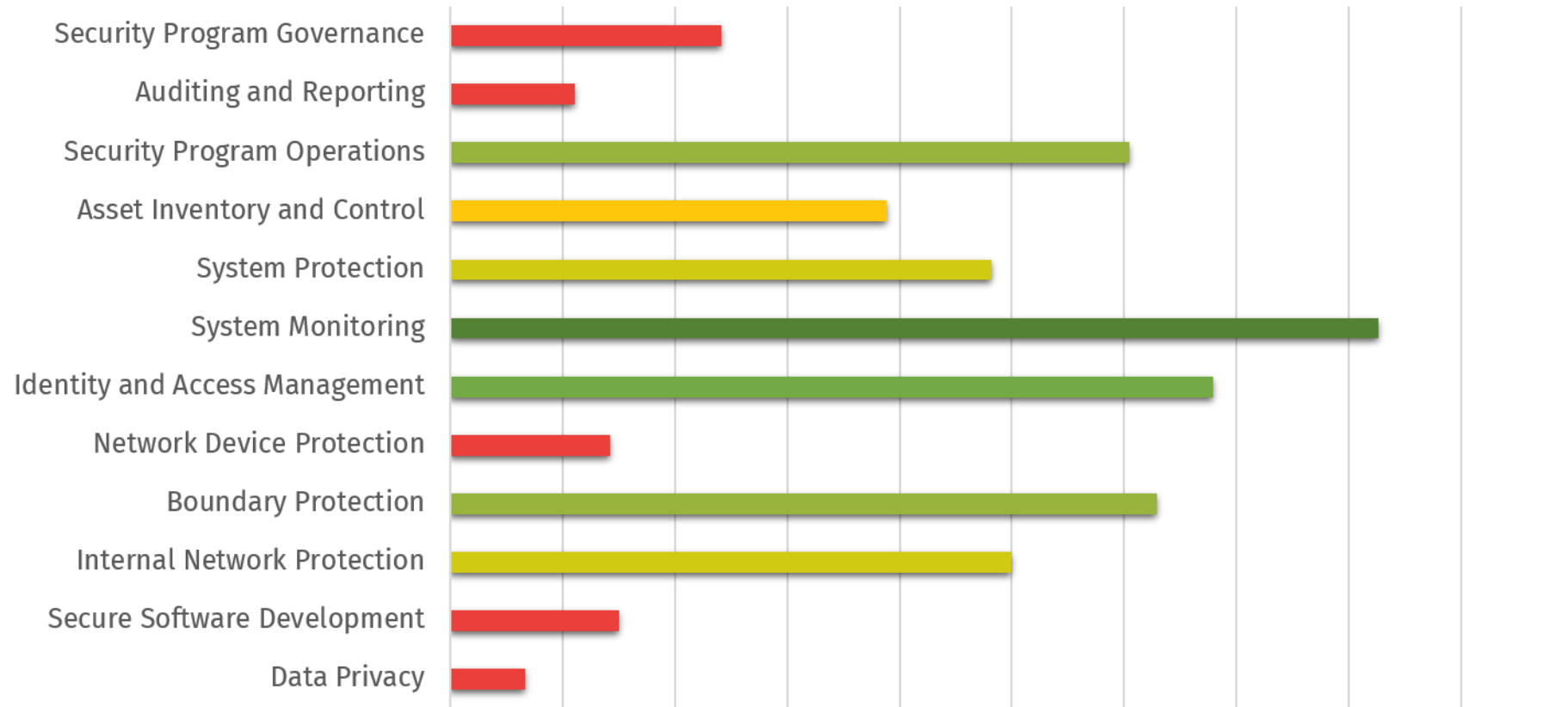


# Cybersecurity Scorecard – NIST CSF (v1.1)

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
<b>Overall Score</b>	<b>D+</b>

# Collective Control Catalog Coverage (CMMC)

## Cybersecurity Maturity Model Certification (v1.02)



# Google Trends – Past 5 Years (CMMC)

Interest over time ?



# 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	A
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
<b>Overall Score</b>	<b>C</b>

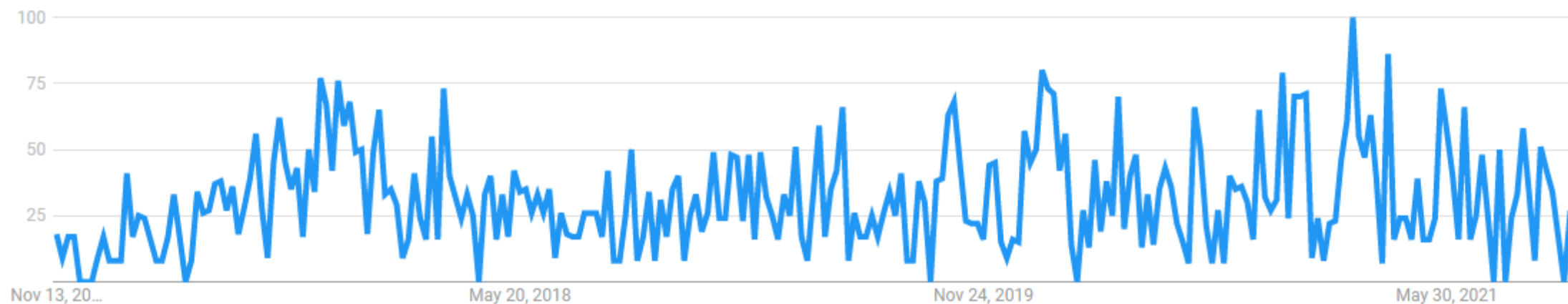
# Collective Control Catalog Coverage (NIST 800-171)

## NIST 800-171 (rev2)



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

Interest over time ?



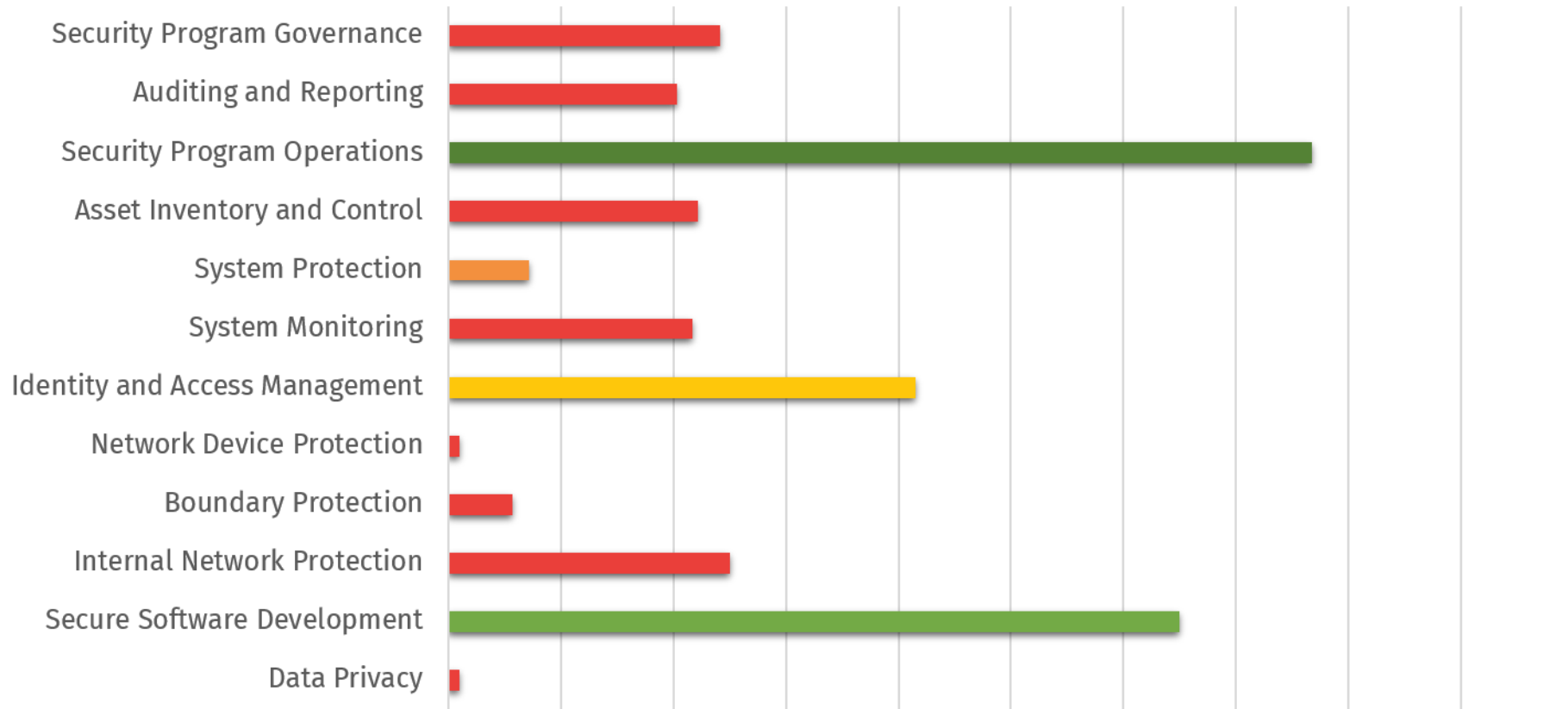
# Cybersecurity Scorecard – NIST 800-171 (rev2)

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	D
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	A
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
<b>Overall Score</b>	<b>C-</b>



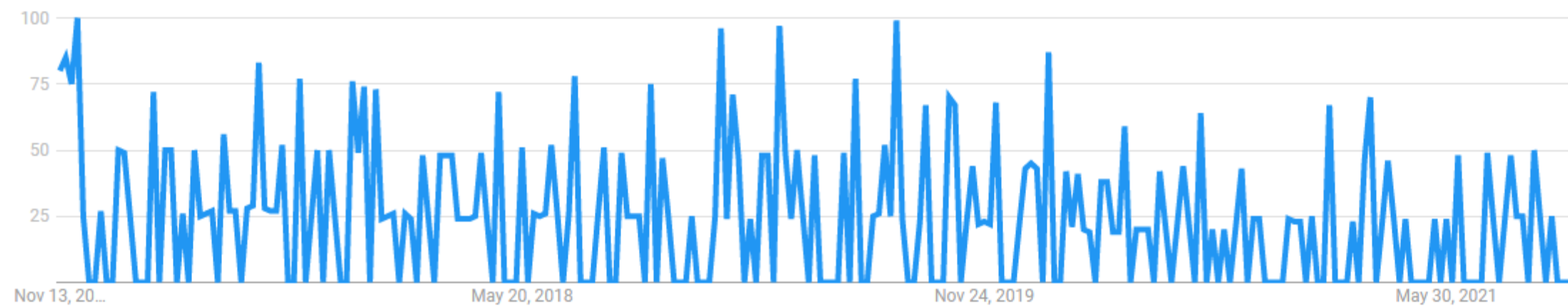
# Collective Control Catalog Coverage (ISO 27002)

## ISO 27002:2013



# Google Trends – Past 5 Years (ISO 27002)

Interest over time 

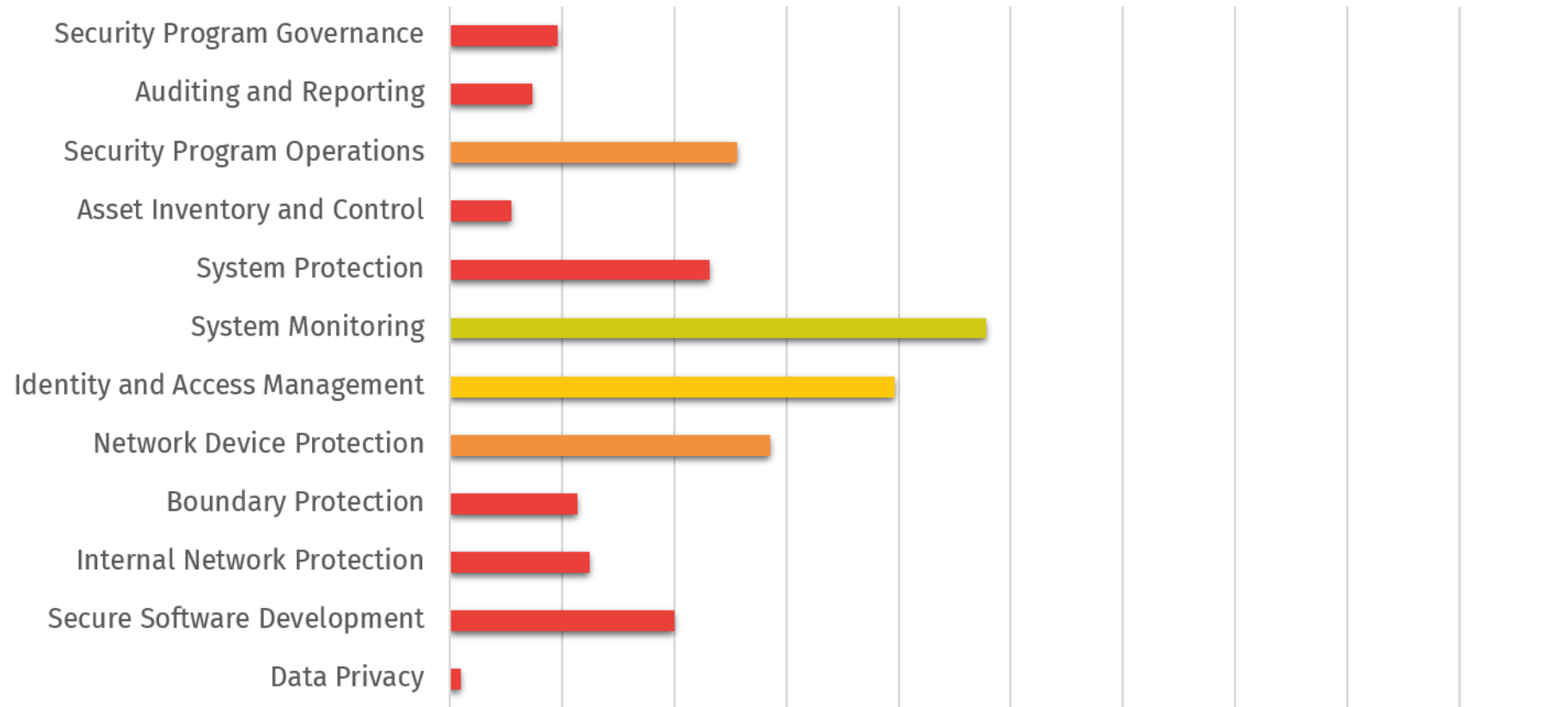


# Cybersecurity Scorecard – ISO 27002:2013

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	C
Operational Controls Addressed	B
Privacy Controls Addressed	F
Technical Controls Addressed	C
Controls Updated Recently	F
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
<b>Overall Score</b>	<b>C-</b>

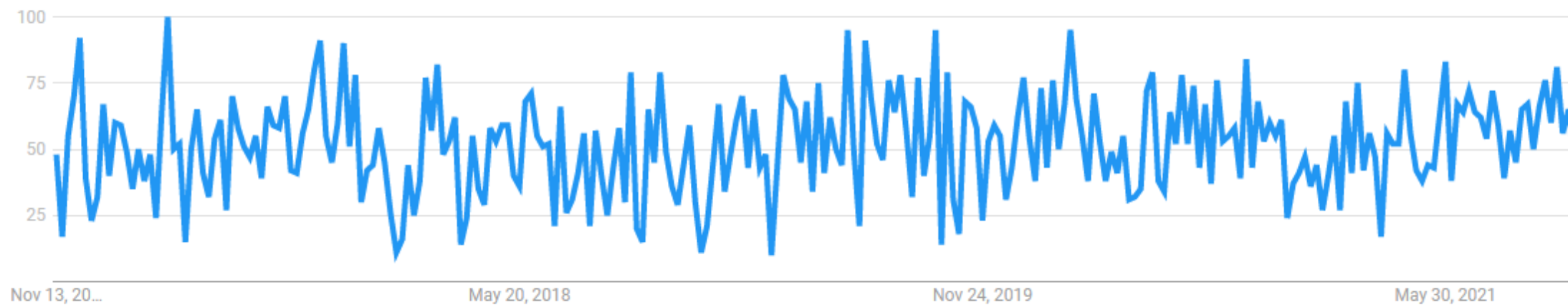
# Collective Control Catalog Coverage (PCI DSS v3.2)

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



# Google Trends – Past 5 Years (PCI DSS)

Interest over time 

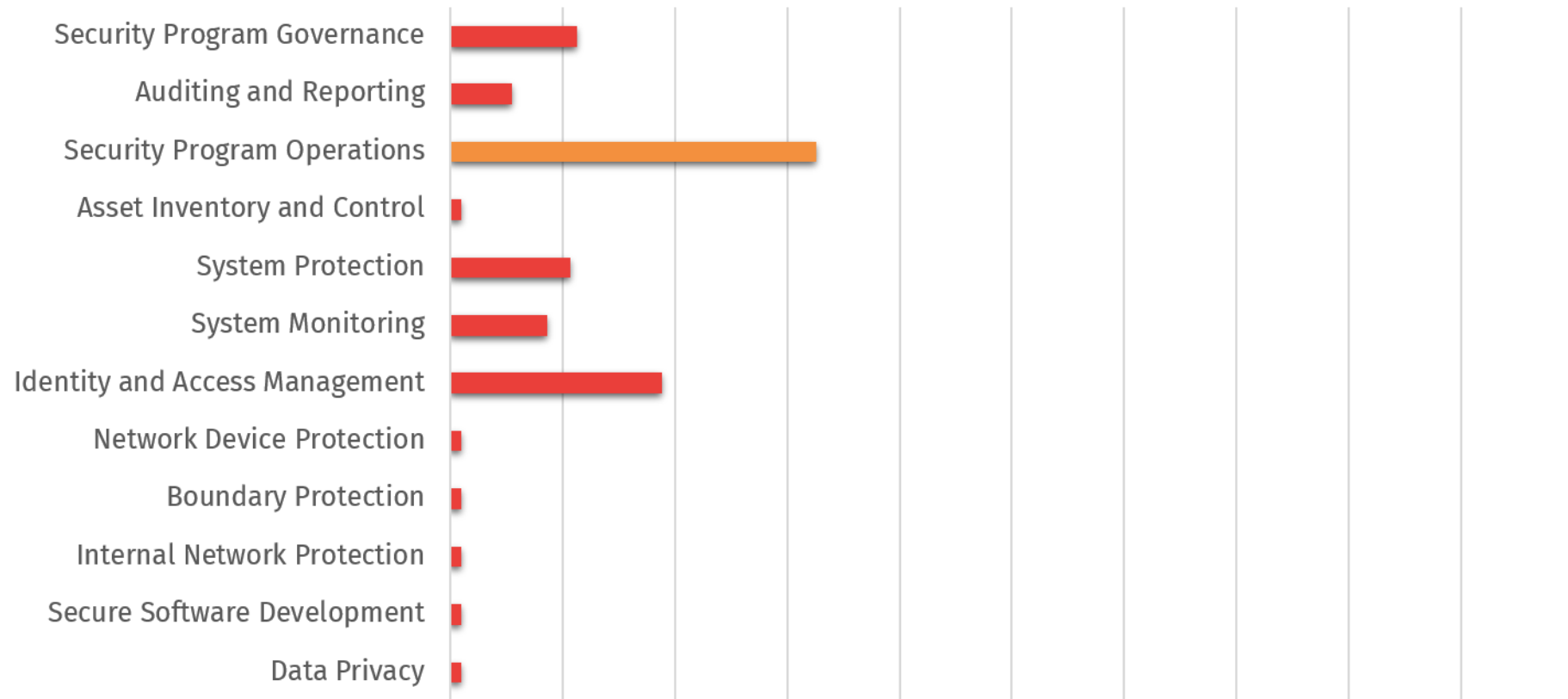


# Cybersecurity Scorecard – PCI DSS (v3.2)

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	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
<b>Overall Score</b>	<b>C-</b>

# Collective Control Catalog Coverage (HIPAA)

## HIPAA Security Rule



# Google Trends – Past 5 Years (HIPAA)

Interest over time 



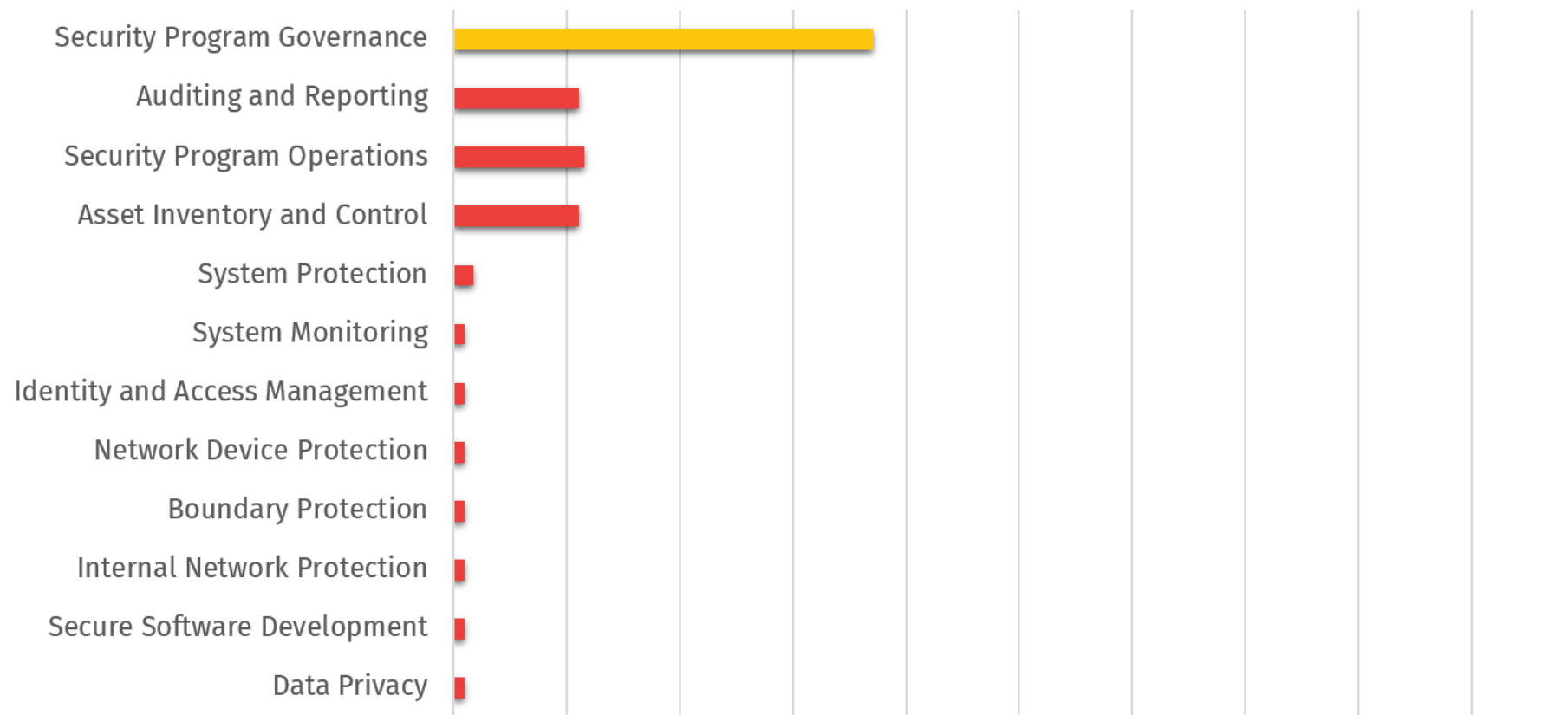


# Cybersecurity Scorecard – HIPAA


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
<b>Overall Score</b>	<b>D</b>

# Collective Control Catalog Coverage (COBIT)

## COBIT (v5)



# Google Trends – Past 5 Years (COBIT)

Interest over time 

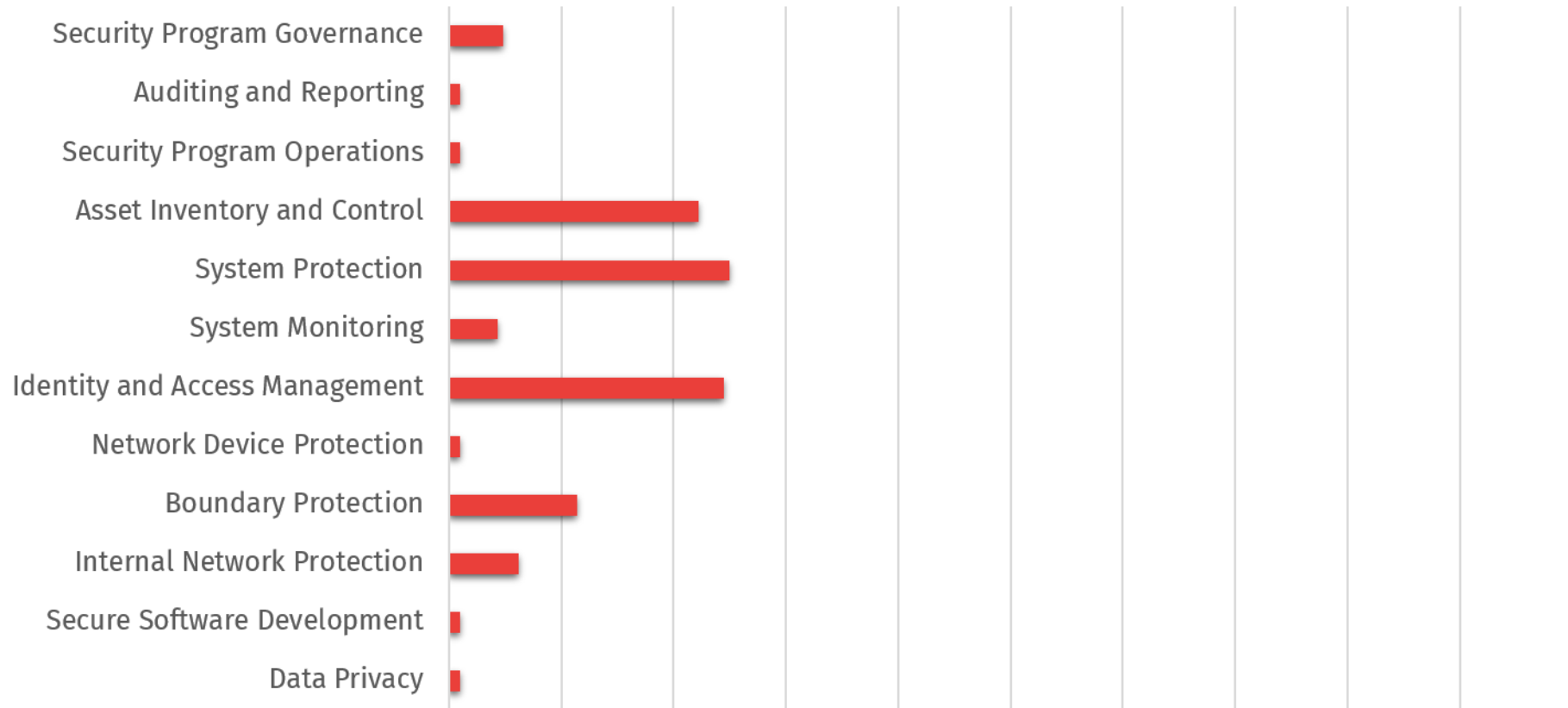


# Cybersecurity Scorecard – COBIT

Cybersecurity Standard Characteristic	Score
Governance Controls Addressed	C
Operational Controls Addressed	D
Privacy Controls Addressed	F
Technical Controls Addressed	F
Controls Updated Recently	D
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
<b>Overall Score</b>	<b>D</b>

# Collective Control Catalog Coverage (MITRE)

## MITRE Enterprise Mitigations



# Google Trends – Past 5 Years (MITRE)

Interest over time 



Hmm, your search doesn't have  
enough data to show here.

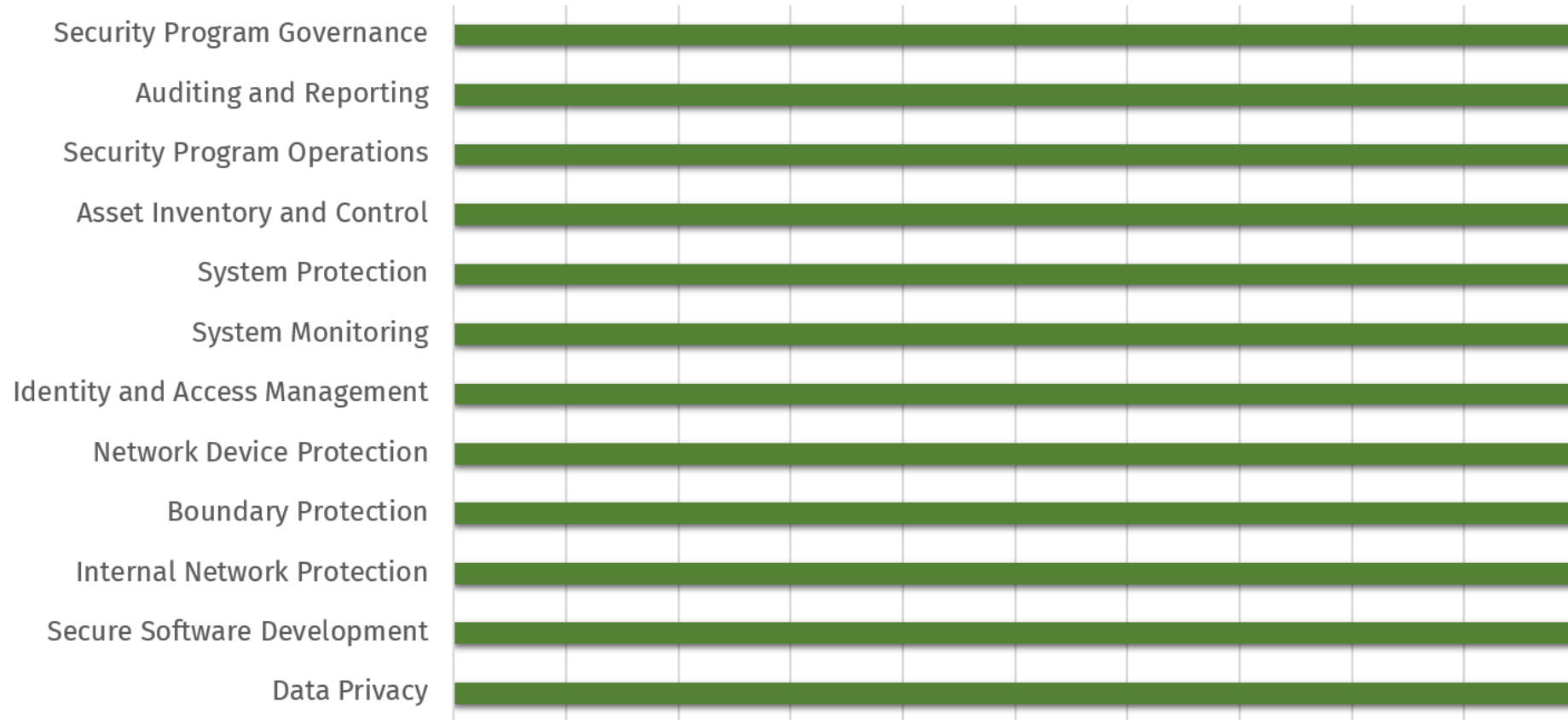
Please make sure everything is spelled correctly, or  
try a more general term.

# 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
<b>Overall Score</b>	<b>C-</b>

# Collective Control Catalog Coverage (CCC)

## Collective Control Catalog (v2021)





# Google Trends – Past 5 Years (CCC)

Interest over time 



Hmm, your search doesn't have  
enough data to show here.

Please make sure everything is spelled correctly, or  
try a more general term.

# 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)	F
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	F
<b>Overall Score</b>	<b>B+</b>

# 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 27002:2013	C-
PCI DSS (v3.2)	C-
HIPAA	D
COBIT (v5)	D
MITRE Enterprise Mitigations	C-
Collective Control Catalog (v2021)	B+

# Collective Control Catalog: Prioritization and Tagging

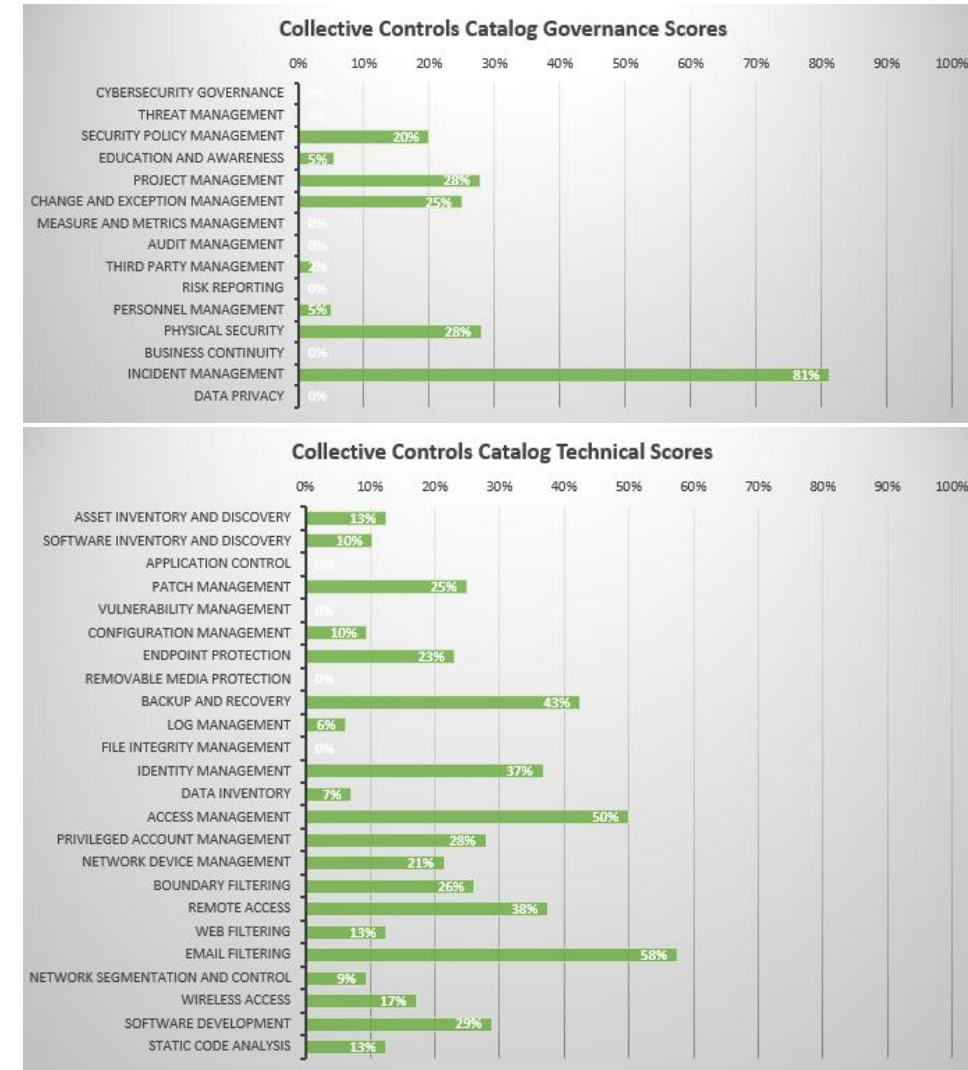


## Control Library Tagging (v1.0g)

Reference ID #	Description	Development Control	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	

# 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
- Ideally each year, more and more cybersecurity professional will donate their time to refining and explaining this approach
- Ideally each year, more and more resources and templates will be available to make it easier for organization to process the body of knowledge

## 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

### JAMESTARALA

Principal Consultant at Enclave Security

[james.tarala@enclavesecurity.com](mailto: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