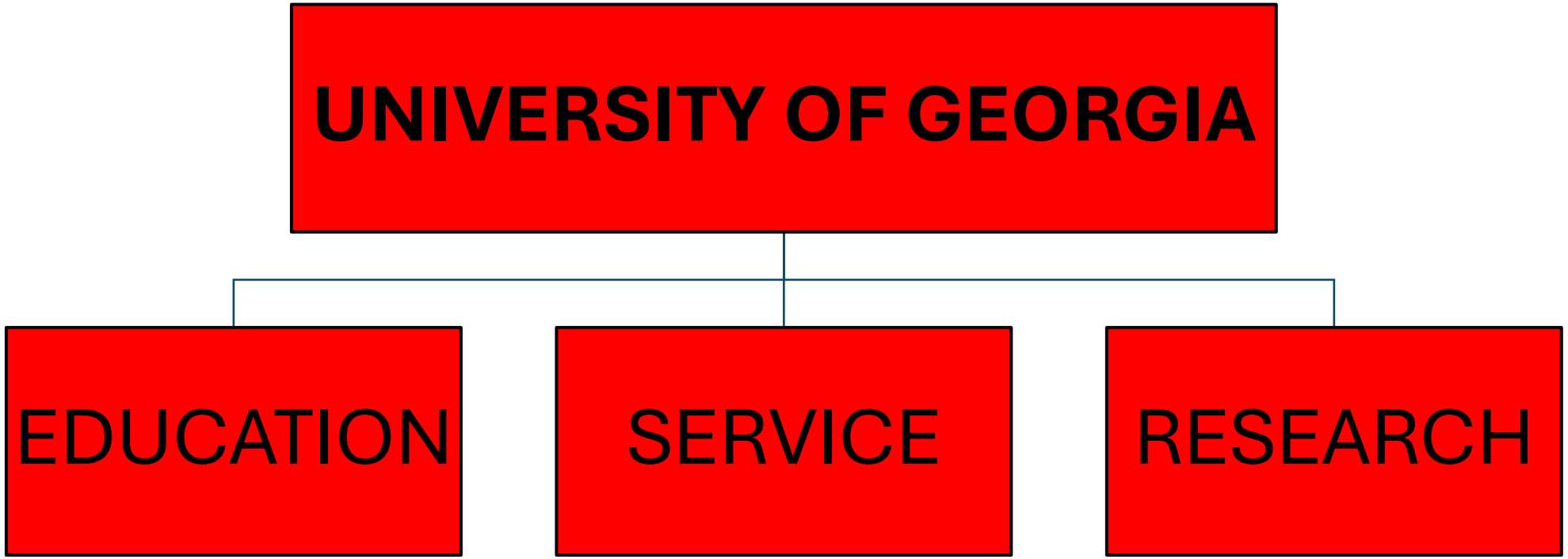
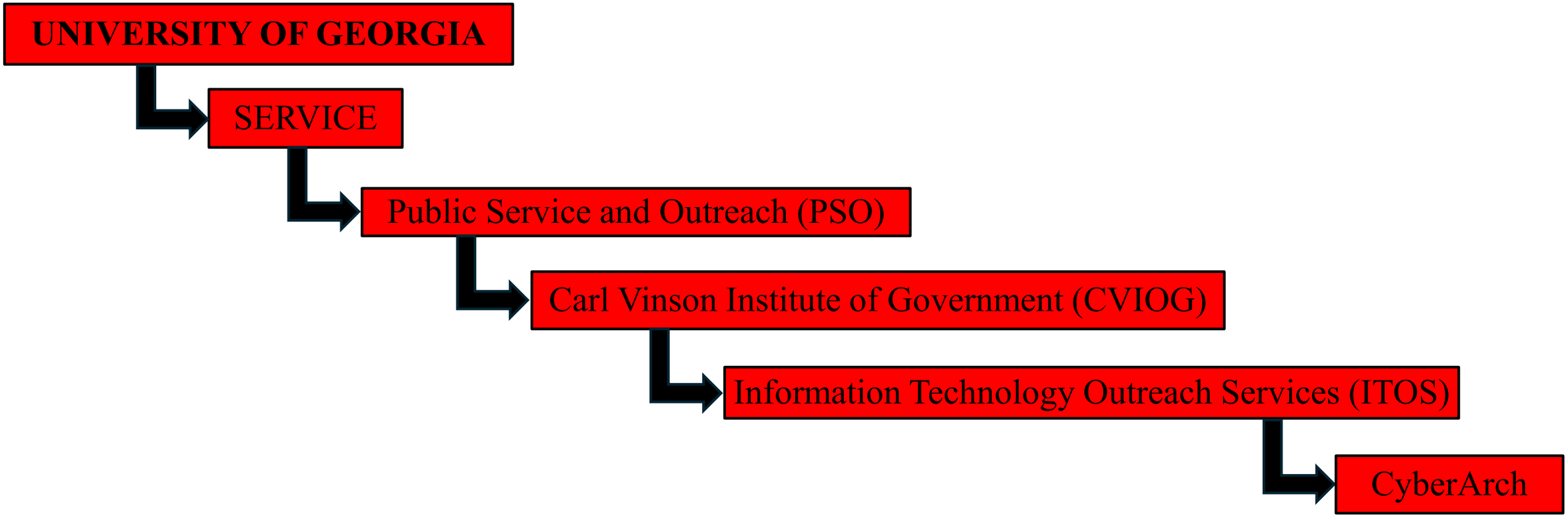
UNIVERSITY OF
GEORGIA
CyberArch

CyberArch Hierarchy

UGA Motto: “to teach, to serve, and to inquire into the nature of things”



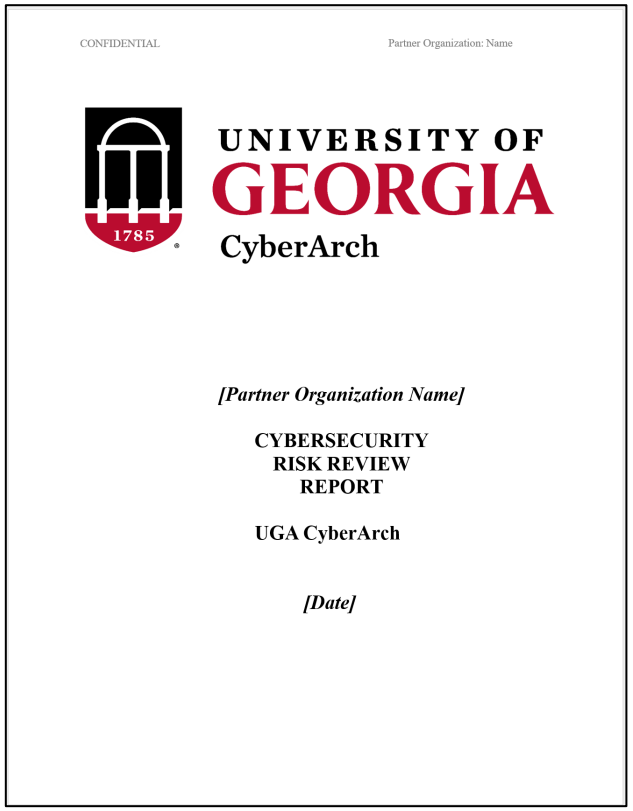
CyberArch Hierarchy



CyberArch Mission

Serve Georgia Organizations

- No-Cost Cybersecurity Risk Review Reports



CONFIDENTIAL

Partner Organization: Name

UNIVERSITY OF GEORGIA
CyberArch

[Partner Organization Name]

CYBERSECURITY RISK REVIEW REPORT

UGA CyberArch

[Date]

Produce the Next Generation of Cybersecurity Experts

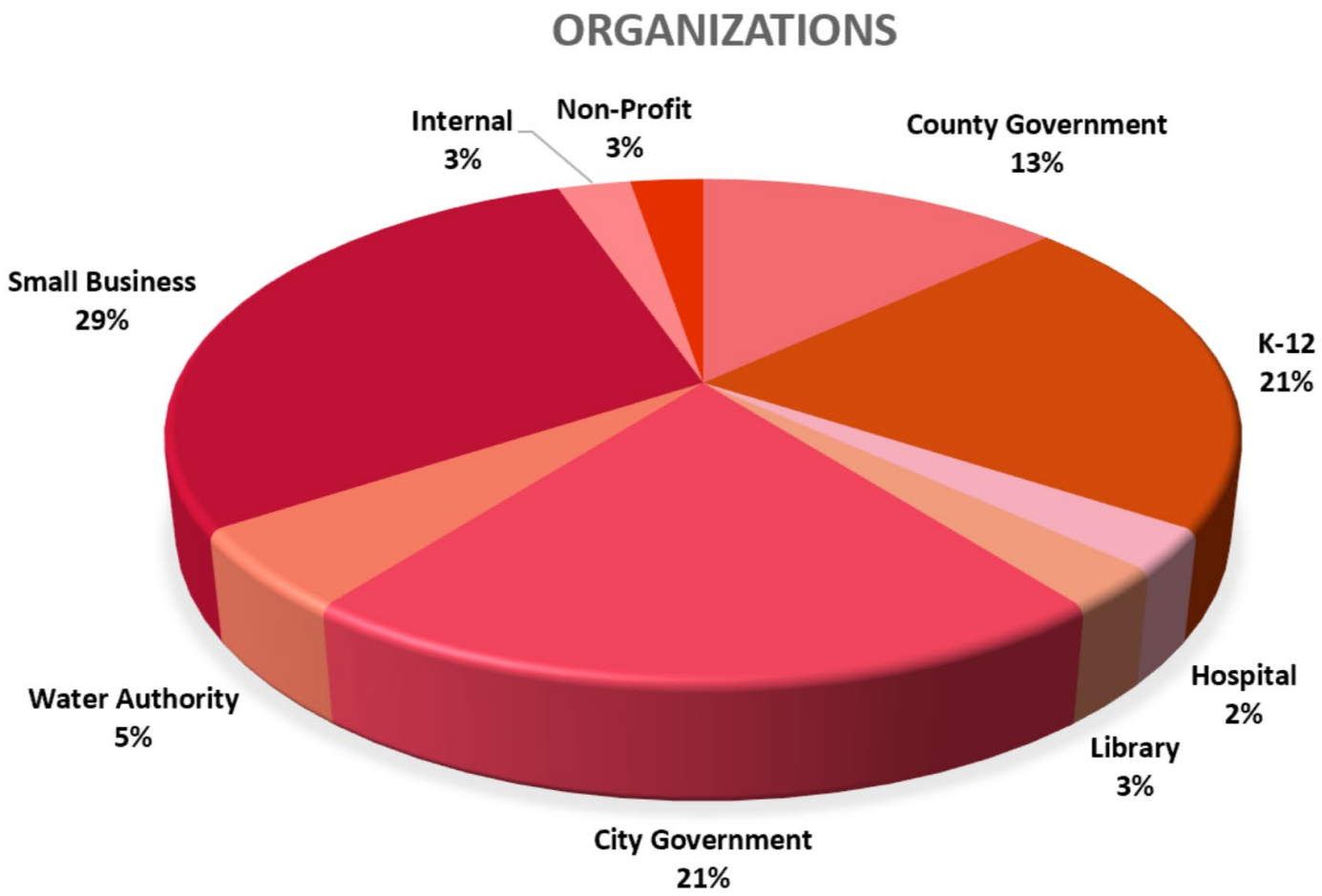
- Training: MIT, UTSA, and Google Cybersecurity courses.
- Experience: Intern teams meet with Partner Organizations, and produce Cybersecurity Risk Review Reports

CyberArch - Interns

- Graduate Assistants – 2 (one graduate student, one PhD candidate)
- Interns – 36 (undergraduate and graduate students)

- Training: Google Cybersecurity Course – 41
- Training: CyberArch Academy – 150

CyberArch – Partner Organizations



Cybersecurity Risk Review Report

Carl Vinson Institute of Government
UNIVERSITY OF GEORGIA

UNIVERSITY OF GEORGIA
CyberArch

Cybersecurity Risk Review Report - Components

Massachusetts Institute of Technology

CYBERSECURITY FOR CRITICAL URBAN INFRASTRUCTURE

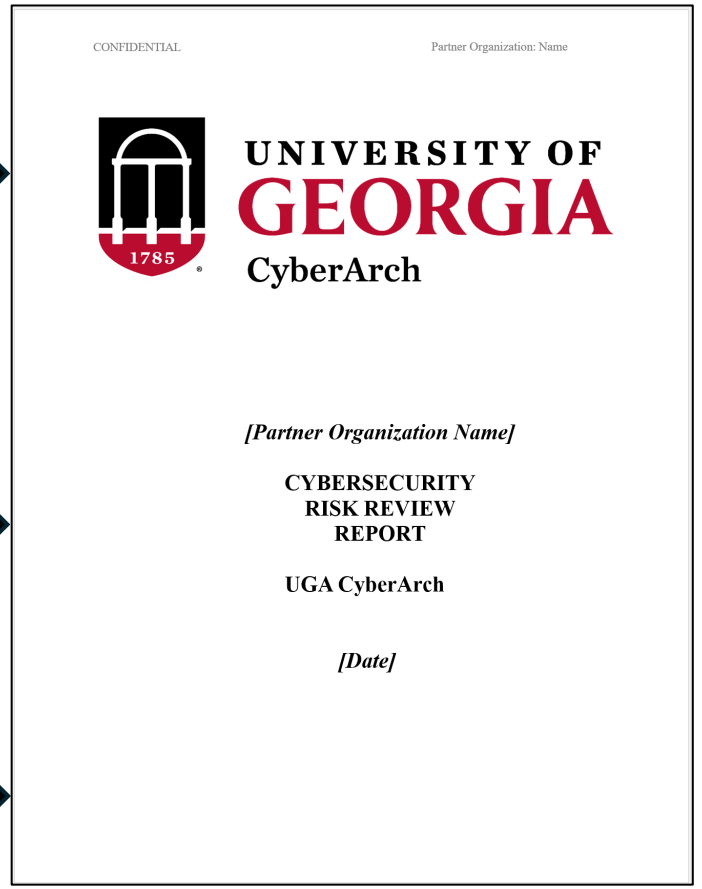
UTSA The University of Texas at San Antonio™

The Community Cyber Security Maturity Model

CIS

CIS Controls Implementation Group 1

56 Safeguards


CONFIDENTIAL

Partner Organization: Name

UNIVERSITY OF GEORGIA

CyberArch

[Partner Organization Name]

CYBERSECURITY RISK REVIEW REPORT

UGA CyberArch

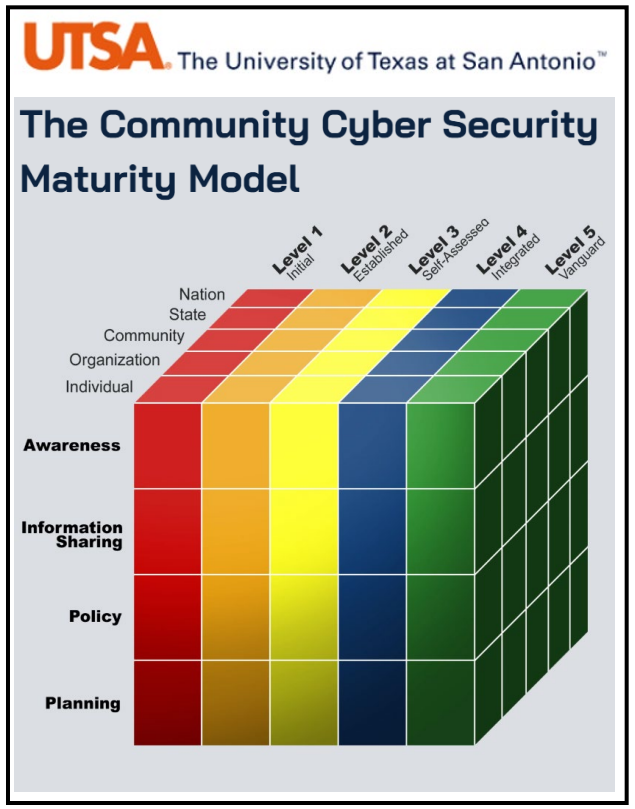
[Date]

MIT - Cybersecurity For Critical Urban Infrastructure

- Designed to prepare city officials, agency staff and a new generation of cybersecurity analysts to understand, help prevent and manage cyberattacks on vulnerable communities across America.
- Uses a questionnaire format to prepare a vulnerability assessment.
- Establishes rules of confidentiality to apply to studying cybersecurity breaches.
- **NOTE:** CyberArch uses MIT's questionnaire format and some of its questions to prepare its Cybersecurity Risk Review Reports.

SOURCE: https://mitxonline.mit.edu/courses/course-v1:MITxT+11.S198x/

University of Texas at San Antonio (UTSA) – Community Cybersecurity Maturity Model (CCSMM)



- A guide which helps communities establish a cybersecurity baseline at the local level.
- Builds a cybersecurity program focused on "whole community" preparedness and response to address a cyber incident or attack.
- It can also be used to communicate with individuals and communities about capabilities and improvement.
- **NOTE:** While the maturity levels used by CyberArch are inspired by the CCSMM, they are not identical.

SOURCE: https://cias.utsa.edu/research/maturity-model/

Center for Internet Security (CIS)

The Center for Internet Security, Inc. (CIS®) is a community-driven non-profit, responsible for globally recognized best practices for securing IT systems and data.

CIS leads a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats.

SOURCE: https://www.cisecurity.org/about-us

CIS – Implementation Groups

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

153 TOTAL SAFEGUARDS

IG3 IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks. **23** SAFEGUARDS

IG2 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity. **74** SAFEGUARDS

IG1 IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks. **56** SAFEGUARDS

SOURCE: https://www.cisecurity.org/controls

CIS Controls

- The CIS Critical Security Controls (CIS Controls) are a prescriptive, prioritized, and simplified set of best practices used to strengthen an organization's cybersecurity posture.
  - Simplify Approach to Threat Protection
  - Comply with Industry Regulations
  - Achieve Essential Cyber Hygiene
  - Translate Information into Action
  - Abide by the Law

CIS Control 1: Inventory and Control of Enterprise Assets

CIS Control 2: Inventory and Control of Software Assets

CIS Control 3: Data Protection

CIS Control 4: Secure Configuration of Enterprise Assets and Software

CIS Control 5: Account Management

CIS Control 6: Access Control Management

CIS Control 7: Continuous Vulnerability Management

CIS Control 8: Audit Log Management

CIS Control 9: Email and Web Browser Protections

CIS Control 10: Malware Defenses

CIS Control 11: Data Recovery

CIS Control 12: Network Infrastructure Management

CIS Control 13: Network Monitoring and Defense

CIS Control 14: Security Awareness and Skills Training

CIS Control 15: Service Provider Management

CIS Control 16: Application Software Security

CIS Control 17: Incident Response Management

CIS Control 18: Penetration Testing

SOURCE: https://www.cisecurity.org/controls

CIS Safeguards

Number	Control/Safeguard	IG1	IG2	IG3
01	**Inventory and Control of Enterprise Assets**			
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	●	●	●
1.2	Address Unauthorized Assets	●	●	●
1.3	Utilize an Active Discovery Tool		●	●
1.4	Use Dynamic Host Configuration Protocol (DHCP) Logging to Update Enterprise Asset Inventory		●	●
1.5	Use a Passive Asset Discovery Tool			●

Each control consists of multiple safeguards in sequential order of Implementation Group

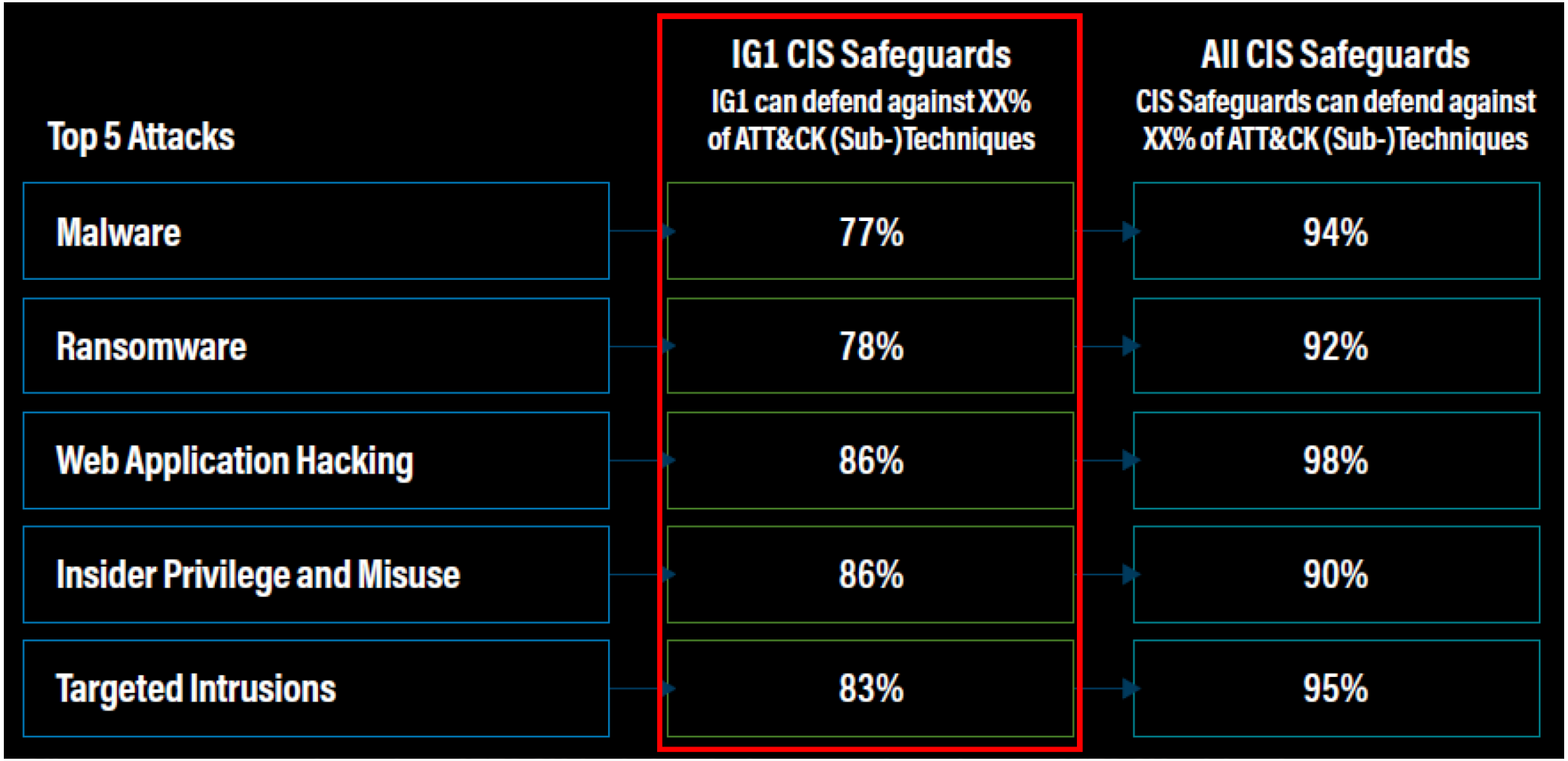
IMPLEMENTATION GROUPS
↓
CONTROLS
↓
SAFEGUARDS

Cybersecurity Risk Review Report – IG1 Summary

- Essential cyber hygiene.
- Minimum standard of information security for all enterprises.
- Utilizes 15 of the 18 CIS Controls.
- 56 Safeguards.

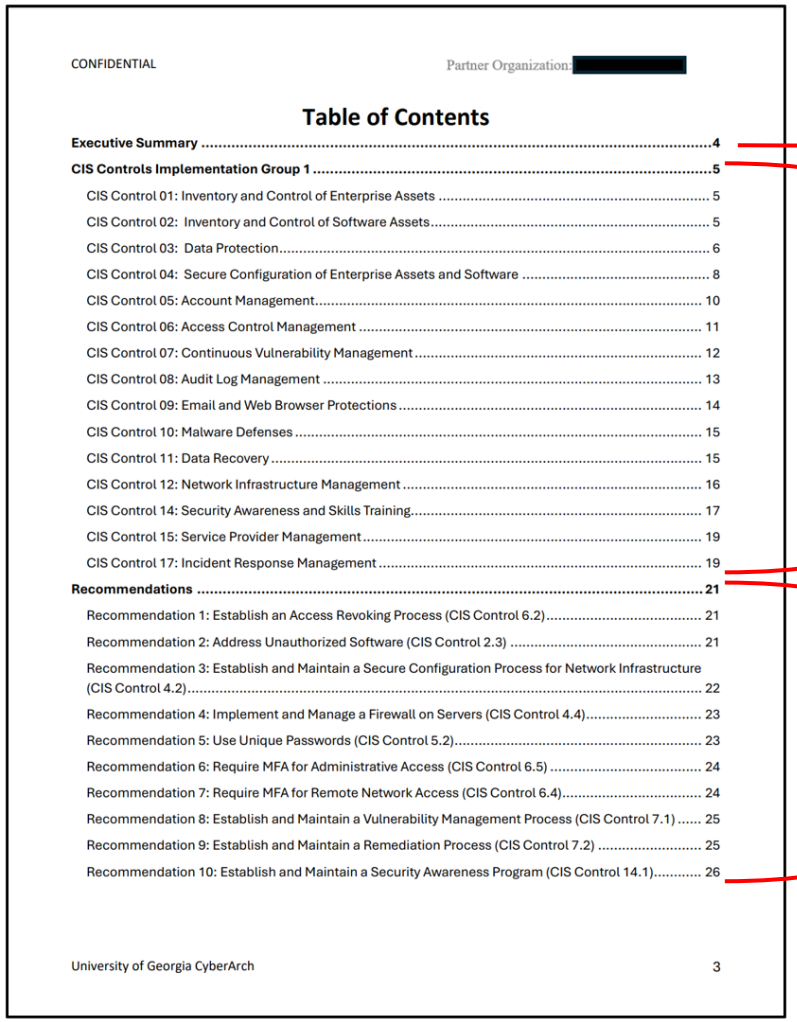
✔ CIS Control 1: Inventory and Control of Enterprise Assets	✔ CIS Control 10: Malware Defenses
✔ CIS Control 2: Inventory and Control of Software Assets	✔ CIS Control 11: Data Recovery
✔ CIS Control 3: Data Protection	✔ CIS Control 12: Network Infrastructure Management
✔ CIS Control 4: Secure Configuration of Enterprise Assets and Software	CIS Control 13: Network Monitoring and Defense
✔ CIS Control 5: Account Management	✔ CIS Control 14: Security Awareness and Skills Training
✔ CIS Control 6: Access Control Management	✔ CIS Control 15: Service Provider Management
✔ CIS Control 7: Continuous Vulnerability Management	CIS Control 16: Application Software Security
✔ CIS Control 8: Audit Log Management	✔ CIS Control 17: Incident Response Management
✔ CIS Control 9: Email and Web Browser Protections	CIS Control 18: Penetration Testing

IG1 Effectiveness



SOURCE: CIS Community Defense Model 2.0

Cybersecurity Risk Review Report - Components



CONFIDENTIAL

Partner Organization: [redacted]

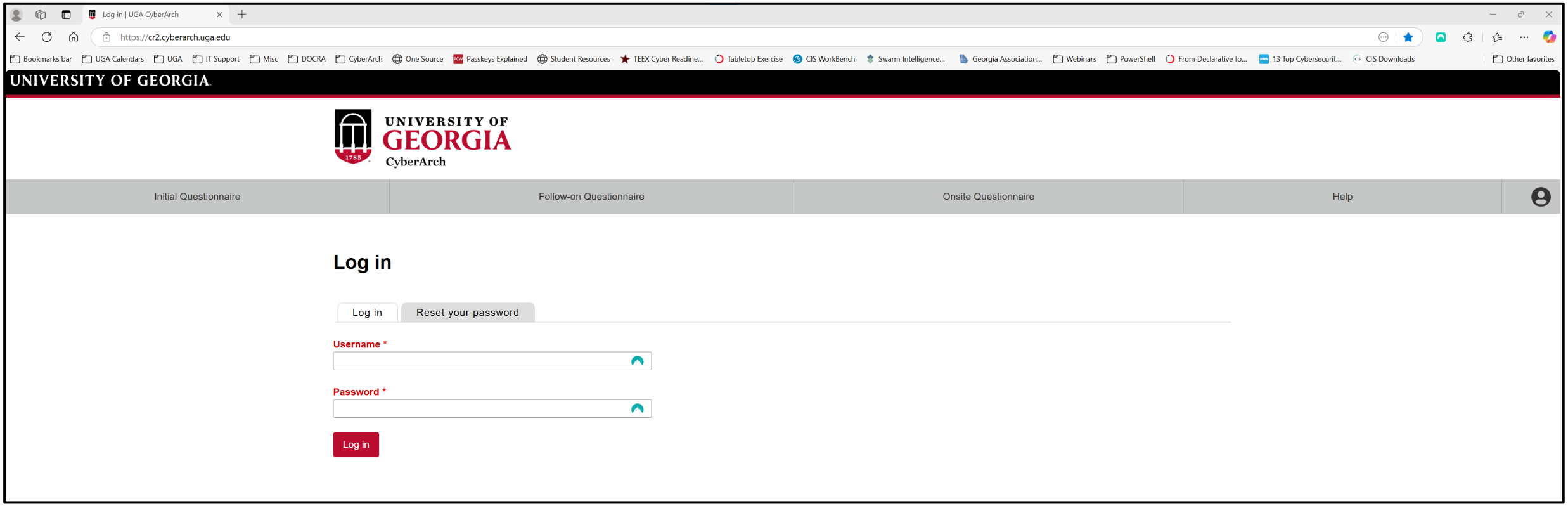
Table of Contents

Executive Summary

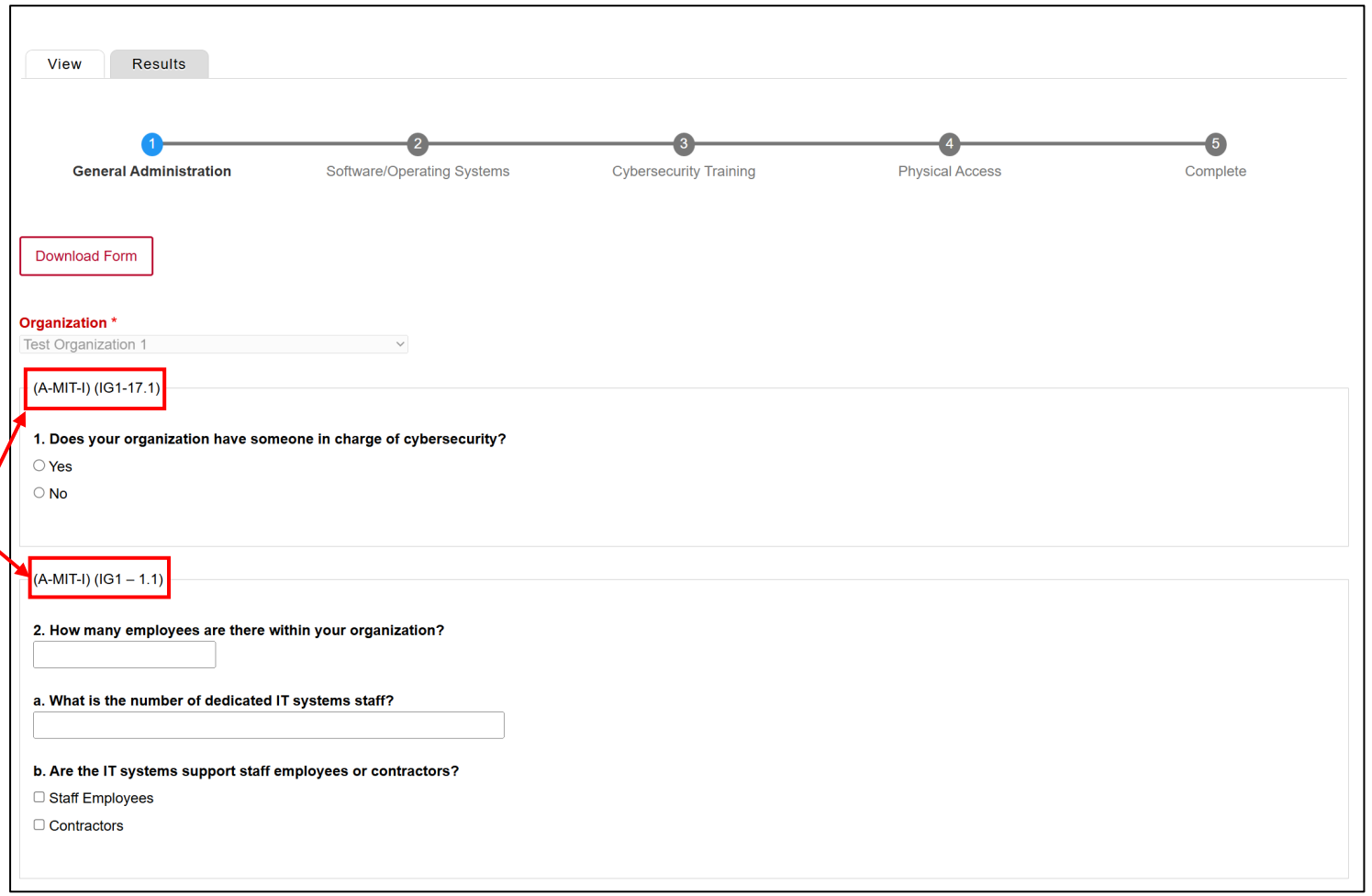
CIS Implementation Group 1 (IG1) Summary

Recommendations

Cybersecurity Risk Review (CR2) – Account Set Up



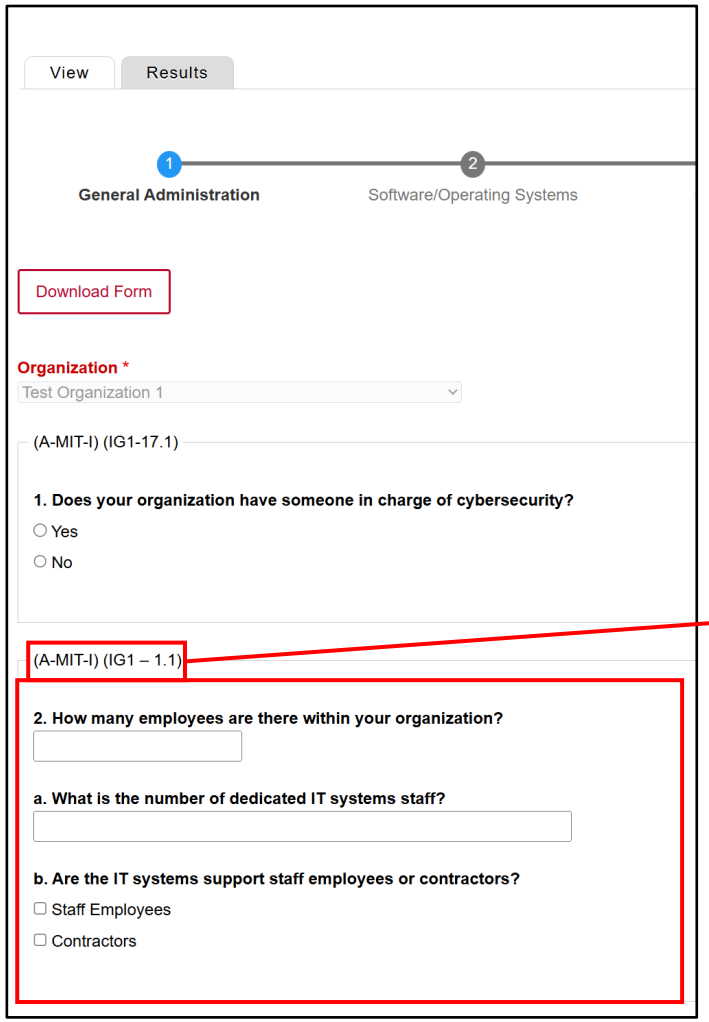
IG1 Summary - Questionnaire

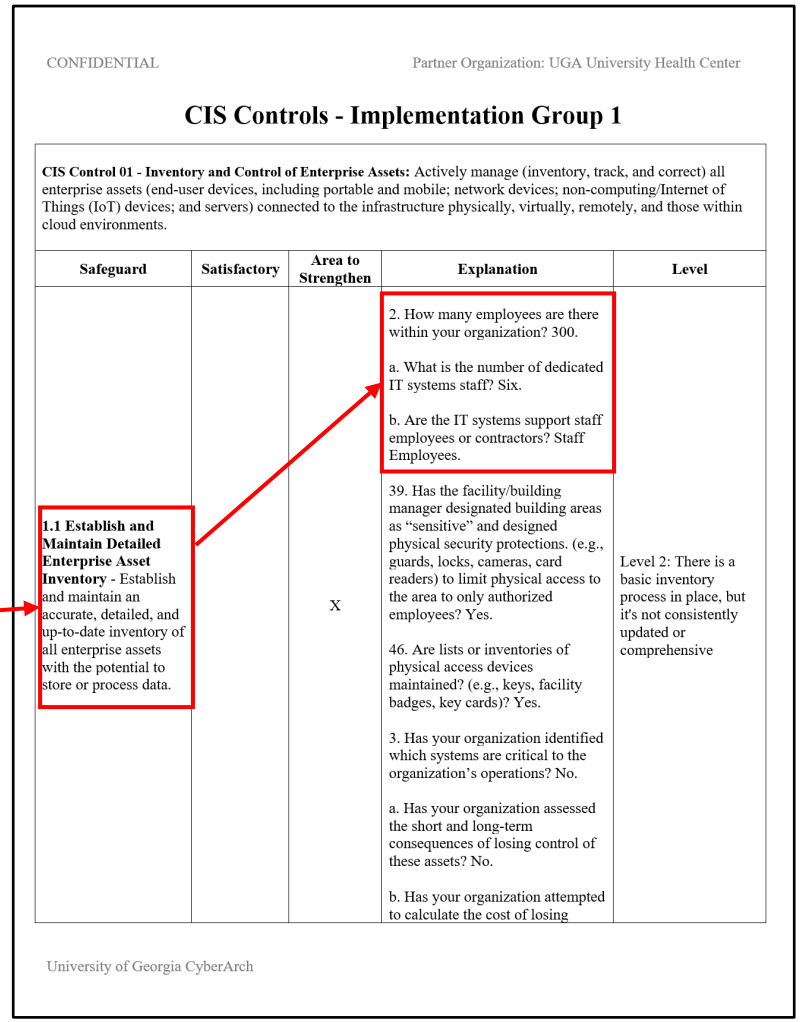


Questions inspired by MIT model and CIS Controls

Questionnaire format inspired by MIT model.

IG1 Summary – Auto Mapping





CONFIDENTIAL

Partner Organization: UGA University Health Center

CIS Controls - Implementation Group 1

CIS Control 01 - Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

Safeguard	Satisfactory	Area to Strengthen	Explanation	Level
1.1 Establish and Maintain Detailed Enterprise Asset Inventory - Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data.		X	2. How many employees are there within your organization? 300. a. What is the number of dedicated IT systems staff? Six. b. Are the IT systems support staff employees or contractors? Staff Employees. 39. Has the facility/building manager designated building areas as "sensitive" and designed physical security protections. (e.g., guards, locks, cameras, card readers) to limit physical access to the area to only authorized employees? Yes. 46. Are lists or inventories of physical access devices maintained? (e.g., keys, facility badges, key cards)? Yes. 3. Has your organization identified which systems are critical to the organization's operations? No. a. Has your organization assessed the short and long-term consequences of losing control of these assets? No. b. Has your organization attempted to calculate the cost of losing	Level 2: There is a basic inventory process in place, but it's not consistently updated or comprehensive

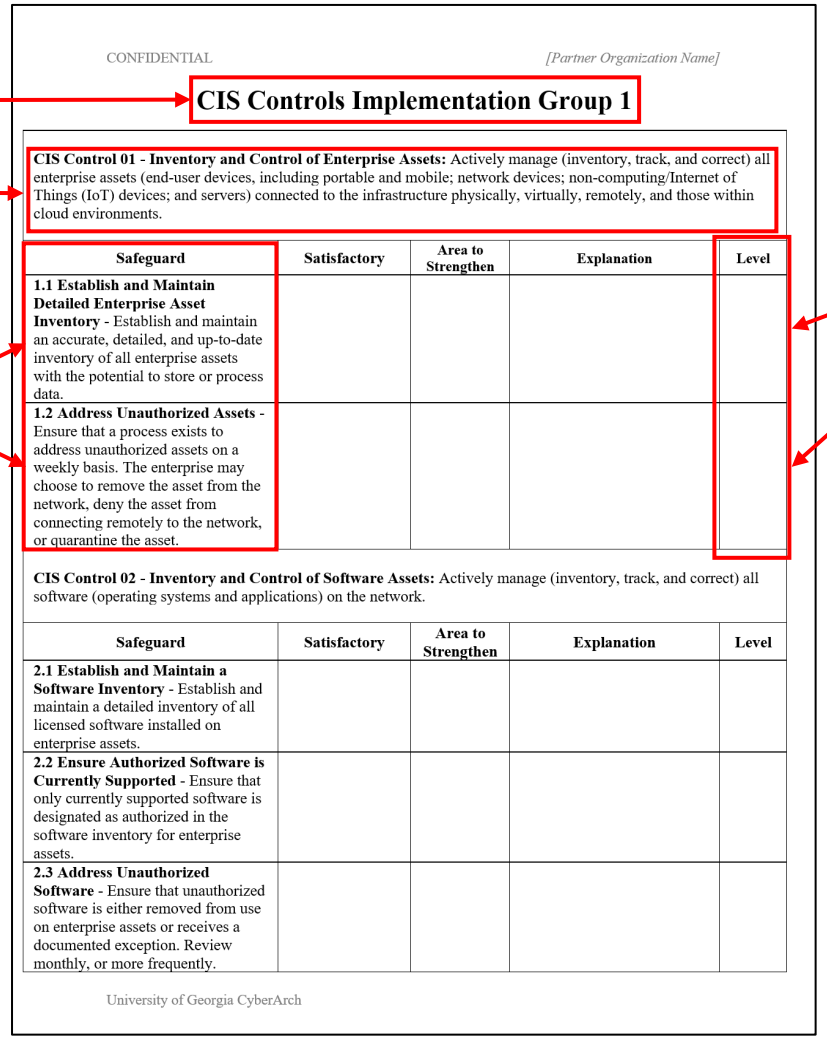
University of Georgia CyberArch

IG1 Summary – Components

CIS: Implementation Group 1

CIS Controls

CIS Safeguards



CONFIDENTIAL *[Partner Organization Name]*

CIS Controls Implementation Group 1

CIS Control 01 - Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

Safeguard	Satisfactory	Area to Strengthen	Explanation	Level
1.1 Establish and Maintain Detailed Enterprise Asset Inventory - Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data.				
1.2 Address Unauthorized Assets - Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.				

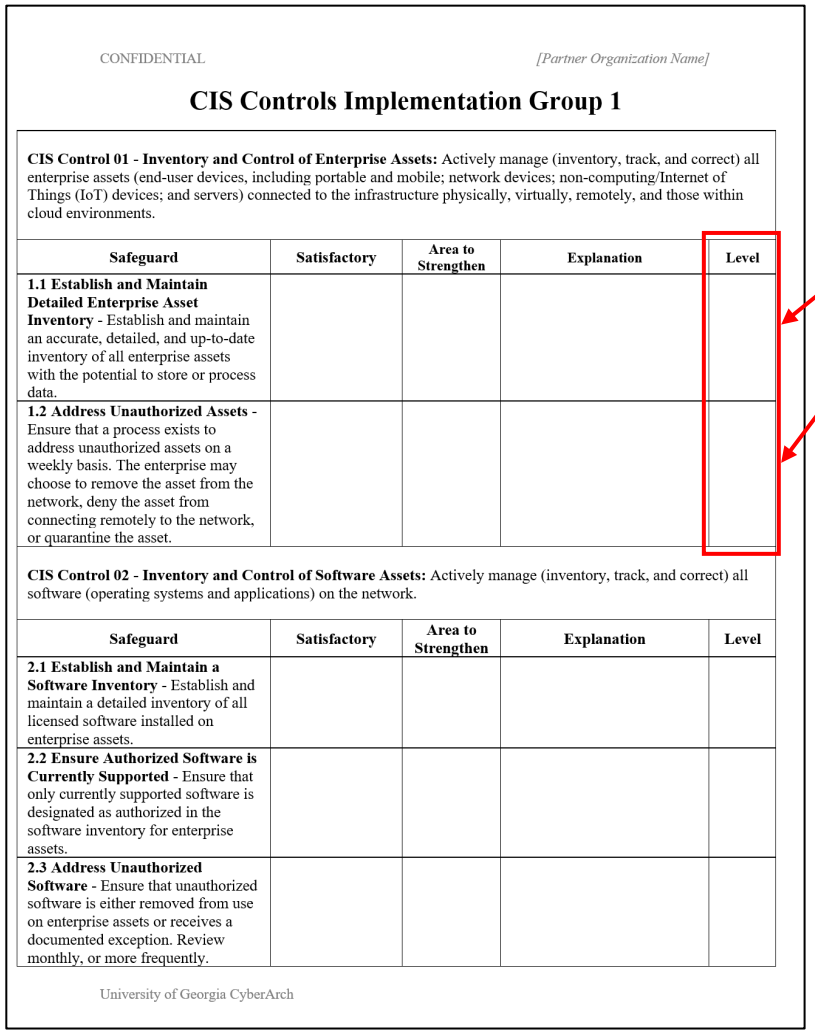
CIS Control 02 - Inventory and Control of Software Assets: Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network.

Safeguard	Satisfactory	Area to Strengthen	Explanation	Level
2.1 Establish and Maintain a Software Inventory - Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.				
2.2 Ensure Authorized Software is Currently Supported - Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.				
2.3 Address Unauthorized Software - Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.				

University of Georgia CyberArch

Inspired by UTSA Community Cybersecurity Maturity Model (CCSMM) Levels

IG1 Summary – Components



CONFIDENTIAL [Partner Organization Name]

CIS Controls Implementation Group 1

CIS Control 01 - Inventory and Control of Enterprise Assets: Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments.

Safeguard	Satisfactory	Area to Strengthen	Explanation	Level
1.1 Establish and Maintain Detailed Enterprise Asset Inventory - Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data.				
1.2 Address Unauthorized Assets - Ensure that a process exists to address unauthorized assets on a weekly basis. The enterprise may choose to remove the asset from the network, deny the asset from connecting remotely to the network, or quarantine the asset.				

CIS Control 02 - Inventory and Control of Software Assets: Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network.

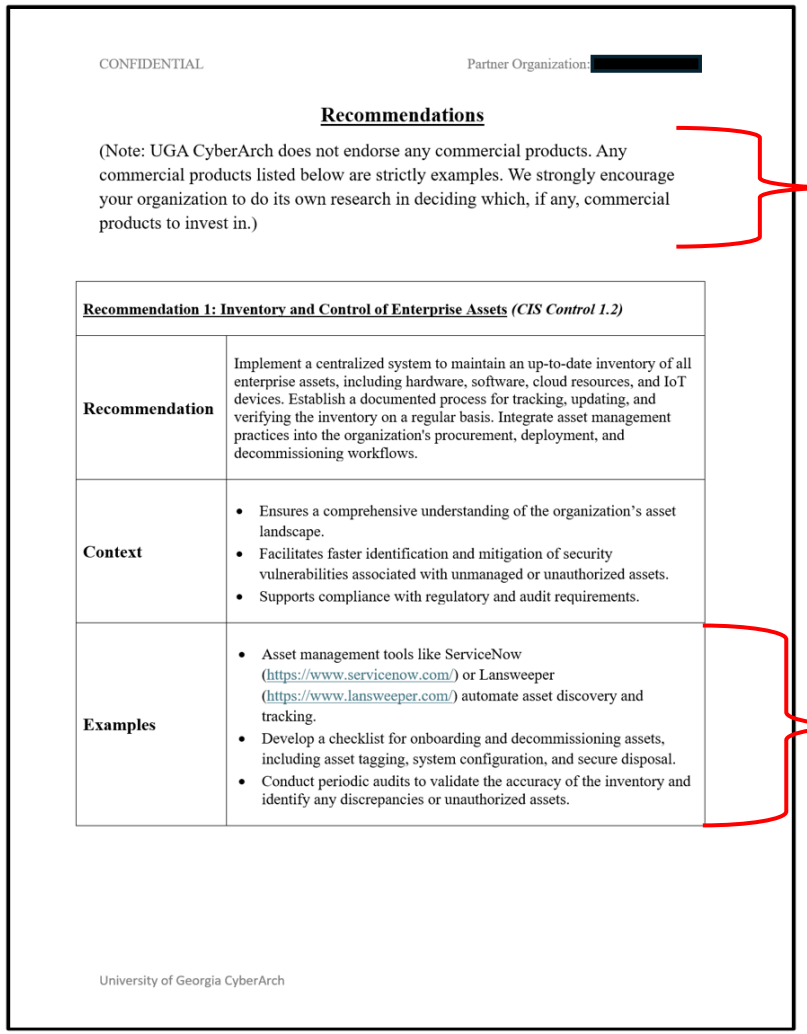
Safeguard	Satisfactory	Area to Strengthen	Explanation	Level
2.1 Establish and Maintain a Software Inventory - Establish and maintain a detailed inventory of all licensed software installed on enterprise assets.				
2.2 Ensure Authorized Software is Currently Supported - Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets.				
2.3 Address Unauthorized Software - Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.				

University of Georgia CyberArch

Maturity Levels

Level 5: Continuous improvement, advanced automation, real-time monitoring.
Level 4: Mature process, regularly reviewed and updated.
Level 3: Well-defined process, consistently applied.
Level 2: Process in place, but inconsistent.
Level 1: No formal process.
Level 0: Not implemented.

Cybersecurity Risk Review Report – Recommendations



CONFIDENTIAL Partner Organization: [redacted]

Recommendations

(Note: UGA CyberArch does not endorse any commercial products. Any commercial products listed below are strictly examples. We strongly encourage your organization to do its own research in deciding which, if any, commercial products to invest in.)

Recommendation 1: Inventory and Control of Enterprise Assets *(CIS Control 1.2)*	
Recommendation	Implement a centralized system to maintain an up-to-date inventory of all enterprise assets, including hardware, software, cloud resources, and IoT devices. Establish a documented process for tracking, updating, and verifying the inventory on a regular basis. Integrate asset management practices into the organization's procurement, deployment, and decommissioning workflows.
Context	• Ensures a comprehensive understanding of the organization's asset landscape. • Facilitates faster identification and mitigation of security vulnerabilities associated with unmanaged or unauthorized assets. • Supports compliance with regulatory and audit requirements.
Examples	• Asset management tools like ServiceNow (https://www.servicenow.com/) or Lansweeper (https://www.lansweeper.com/) automate asset discovery and tracking. • Develop a checklist for onboarding and decommissioning assets, including asset tagging, system configuration, and secure disposal. • Conduct periodic audits to validate the accuracy of the inventory and identify any discrepancies or unauthorized assets.

University of Georgia CyberArch

- CyberArch does not endorse any commercial products.
- Any commercial products listed are strictly examples.
- We strongly encourage your organization to do its own research in deciding which, if any, commercial products to invest in.)

Cybersecurity Risk Review Report – Recommendations

Recommendation

Examples of Possible Solutions

Recommendation 1: Inventory and Control of Enterprise Assets *(CIS Control 1.2)*	
Recommendation	Implement a centralized system to maintain an up-to-date inventory of all enterprise assets, including hardware, software, cloud resources, and IoT devices. Establish a documented process for tracking, updating, and verifying the inventory on a regular basis. Integrate asset management practices into the organization's procurement, deployment, and decommissioning workflows.
Context	• Ensures a comprehensive understanding of the organization's asset landscape. • Facilitates faster identification and mitigation of security vulnerabilities associated with unmanaged or unauthorized assets. • Supports compliance with regulatory and audit requirements.
Examples	• Asset management tools like ServiceNow (https://www.servicenow.com/) or Lansweeper (https://www.lansweeper.com/) automate asset discovery and tracking. • Develop a checklist for onboarding and decommissioning assets, including asset tagging, system configuration, and secure disposal. • Conduct periodic audits to validate the accuracy of the inventory and identify any discrepancies or unauthorized assets.

Context:

- **What the recommendation means.**
- **The benefits of implementing.**
- **The risks of not implementing.**

IG1 Recommendation Support

- Deep dive into more detailed suggestions on how best to implement recommendations.
- Provide further analysis into possible commercial solutions (feature comparison, cost analysis, etc.)
- Reminder: CyberArch does not recommend any specific commercial solution but can research options and provide information for you and/or your leadership to make the best possible decision for your organization.

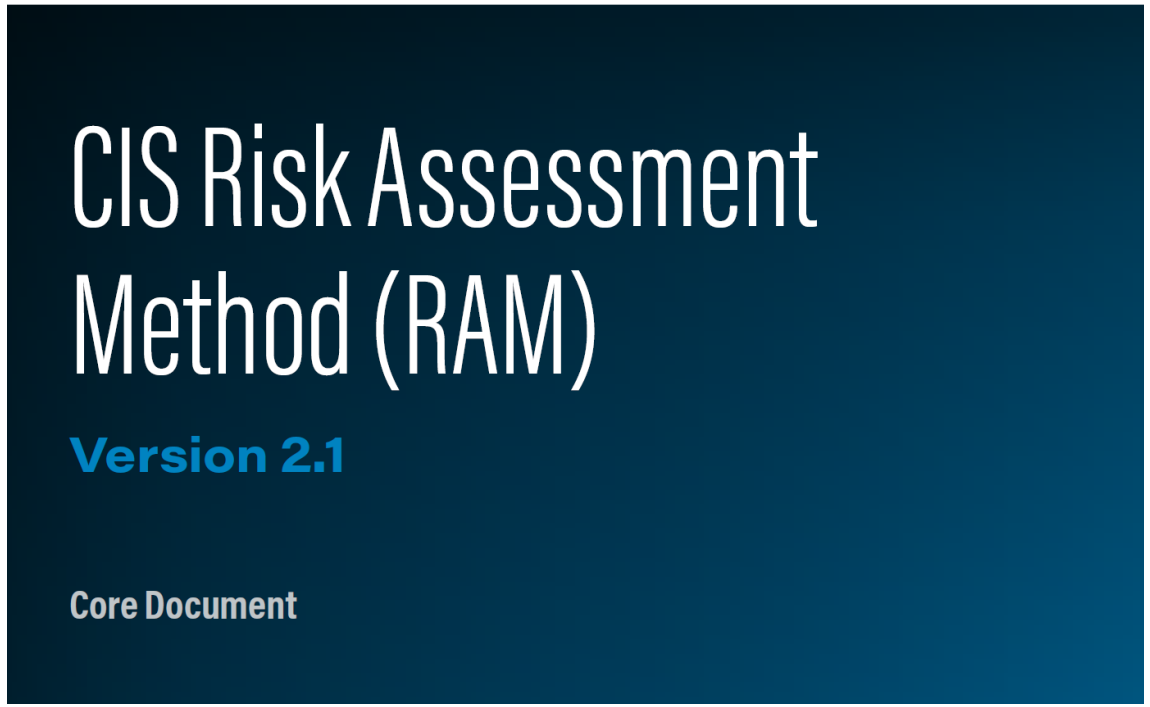
Recommendation 1: Inventory and Control of Enterprise Assets *(CIS Control 1.2)*	
Recommendation	Implement a centralized system to maintain an up-to-date inventory of all enterprise assets, including hardware, software, cloud resources, and IoT devices. Establish a documented process for tracking, updating, and verifying the inventory on a regular basis. Integrate asset management practices into the organization's procurement, deployment, and decommissioning workflows.
Context	• Ensures a comprehensive understanding of the organization's asset landscape. • Facilitates faster identification and mitigation of security vulnerabilities associated with unmanaged or unauthorized assets. • Supports compliance with regulatory and audit requirements.
Examples	• Asset management tools like ServiceNow (https://www.servicenow.com/) or Lansweeper (https://www.lansweeper.com/) automate asset discovery and tracking. • Develop a checklist for onboarding and decommissioning assets, including asset tagging, system configuration, and secure disposal. • Conduct periodic audits to validate the accuracy of the inventory and identify any discrepancies or unauthorized assets.

CIS RAM

(Risk Assessment Method)

CIS RAM – Introduction

- CIS RAM was authored by HALOCK Security Labs in partnership with the CIS to establish reasonable implementation of the CIS Controls.
- By leveraging CIS RAM, enterprises can methodically build what is reasonable and appropriate security safeguards ("reasonable" controls) for their specific environment.
- Provides standardized methods to achieve compliance.
- Ensures enterprises devote the right amount of resources to maintain security.
- Incorporates DoCRA (Duty of Care Risk Analysis)



Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

DoCRA (Duty of Care Risk Analysis)

- DoCRA is a method for analyzing risk as regulators and judges expect it to be done.
- DoCRA was developed by Halock Security Labs, an information security firm founded in 1996.
- Halock worked together with CIS to incorporate DoCRA into CIS RAM.
- Regulations and judicial "balancing tests" expect that organizations consider the likelihood and degree of harm they may cause themselves and others, and to use safeguards that reduce those risks – as long as those safeguards are not overly burdensome.
- Duty of Care Risk Analysis (DoCRA) can be used to analyze cyber security risks using any variety of control standards or regulatory requirements.
- The CIS Controls Risk Assessment Method (CIS RAM) is based upon DoCRA, and DoCRA has been successfully used in litigation to help explain the use of risk assessments for determining whether a control was "reasonable."
- DoCRA methods are used to analyze risks with:
  - ISO 27001/27002
  - NIST Special Publications 800-53
  - the HIPAA Security Rule
  - GDPR
  - 23 NYCRR Part 500
  - 201 CMR 17.00
  - The NIST Cybersecurity Framework
  - Maturity model-based controls models, such as FFIEC CAT.

SOURCE: https://www.halock.com/the-duty-of-care-risk-analysis-standard-docra/

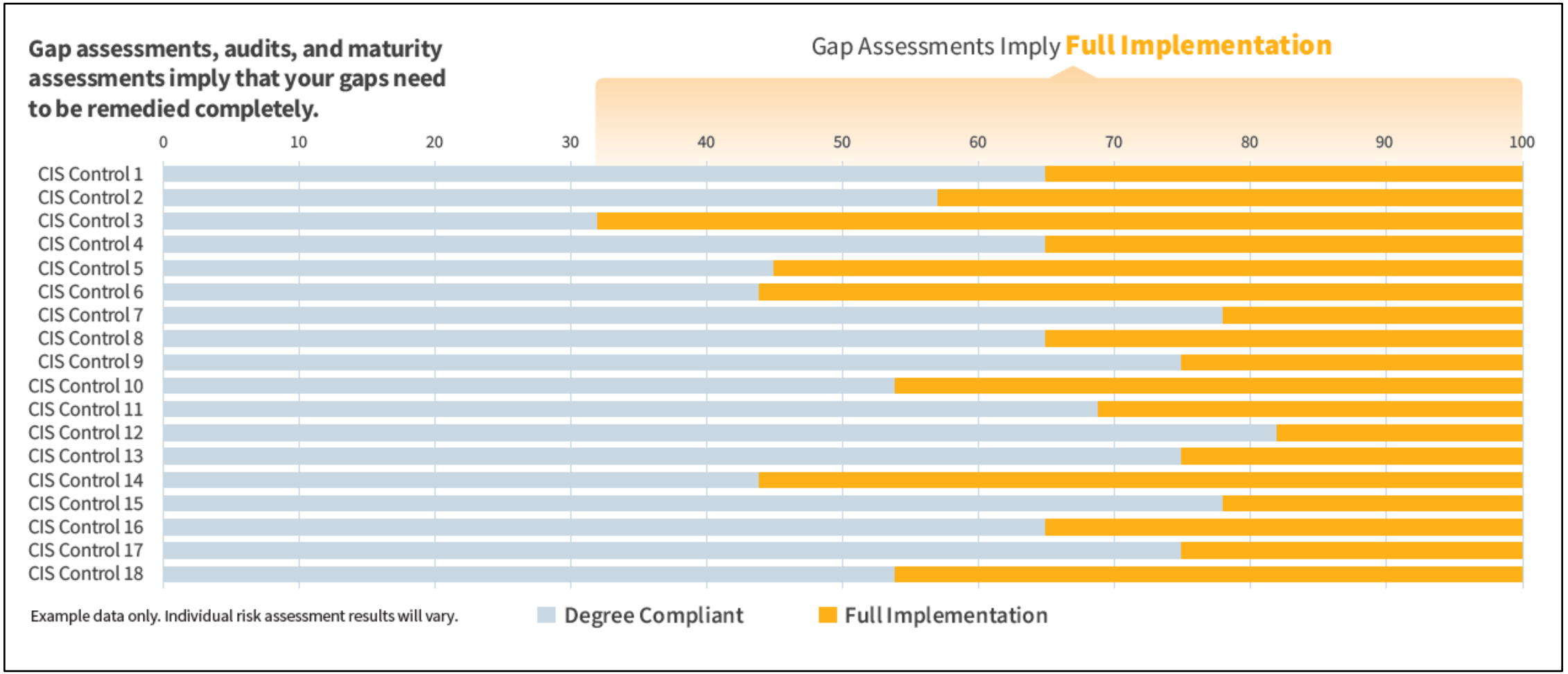
CIS RAM – DoCRA

THE PROBLEM

Interested Party	Their Concerns	Your Challenges
CIOs / Executives / Board ➡	How does our **investment** in the CIS Controls tie to what is important to the business?	Justifying security **investments** requires a defendable risk calculation, translating risks into initiatives and executive-level dashboards.
Attorneys / Judges ➡	Did you implement **reasonable** controls that could have prevented a breach?	Demonstrating to a judge that the CIS Controls you implemented are **reasonable**.
Regulators ➡	Is your use of the CIS Controls **reasonable and appropriate** to achieve their version of **compliance?**	Showing regulators that your implemented CIS Controls achieves their version of **compliance**.
Customers ➡	Are you **appropriately protecting our information** from harm?	Assuring customers that their information is **appropriately protected**.
IT and Security Professionals ➡	How can we **get this done**?	**Prioritizing CIS Controls implementation**, and accepting risks at a reasonable level.

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

CIS RAM – Full Implementation?



CIS RAM – The Solution

CIS RAM is the Solution

CIS RAM addresses these challenges in the following ways:

- CIS RAM provides a method for evaluating risk by calculating the expectancy of an impact to customers, business objectives, and external entities (regulators, vendors, etc.).
- CIS RAM provides a method to "draw a line" at an enterprise's Acceptable Risk Definition, with risks below the line adhering to **due care** and risks above the line requiring risk treatment.
- Together these principles provide enterprises with a concise and defendable process to accept or address risk.

New in CIS RAM 2.1

- Workbooks automate much of your risk analysis for faster results.
- CIS RAM 2.1 estimates expectancy by comparing the commonality of reported threats to the strength of CIS Safeguards that prevent them.
- Using the Veris Community Database (VCDB), CIS RAM introduces an evidence-based heuristic for estimating expectancy.

CIS RAM Helps You Apply the Right Amount of Security

Risk analysis helps shape and customize controls to address the internal and external challenges that enterprises face. Too often enterprises rely on gap assessments to determine the severity of their vulnerabilities. **CIS RAM enables you to apply just the right amount of security — not too much, not too little** — striking a balance between keeping your enterprise safe and ensuring you can conduct business as usual. Remediating all gap assessment deficiencies can lead to over-securing and over-investing, while remediating risks identified in a CIS RAM assessment can lead to applying just the right amount of security and investment.

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

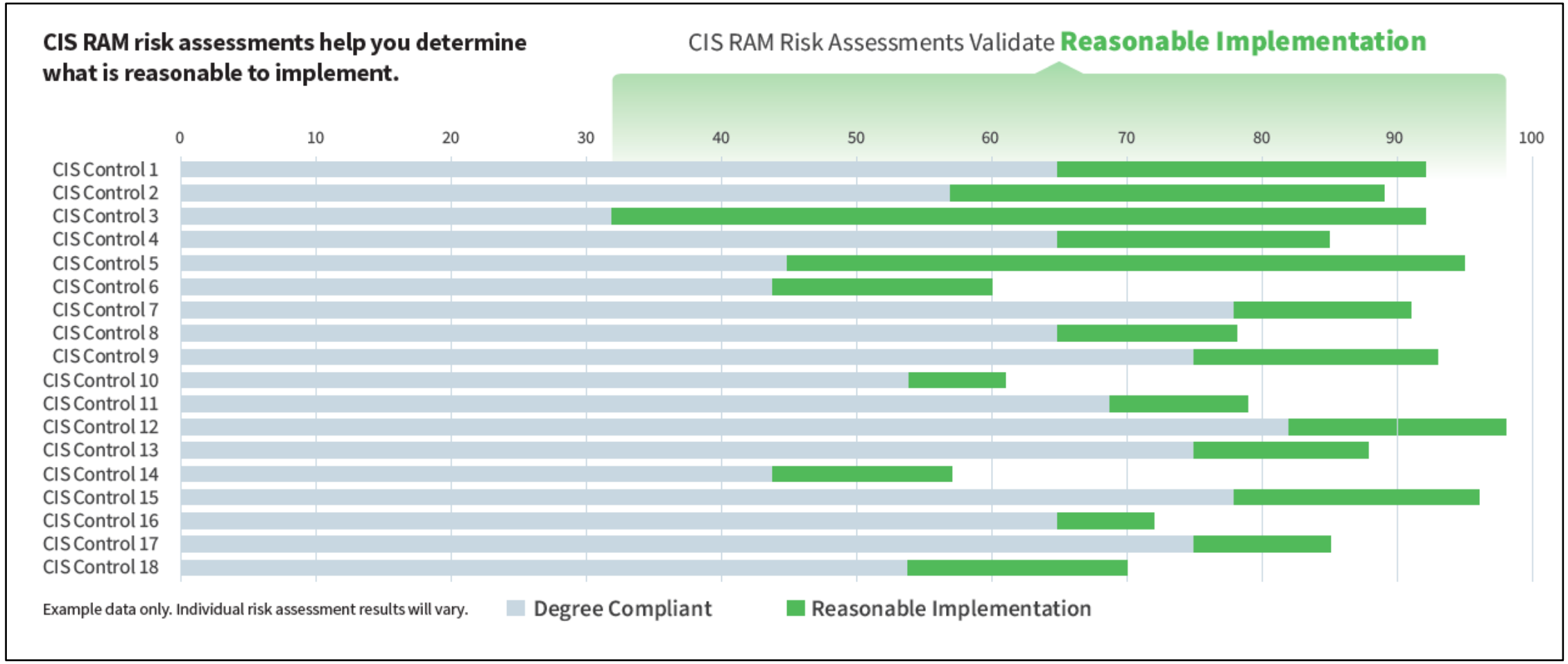
CIS RAM – DoCRA

THE SOLUTION

Interested Party	CIS RAM Solution
CIOs / Executives / Board ➡	Risks are concisely calculated and prioritized against the needs of customers, business objectives, and external entities. This helps justify investments, create defendable risk calculations, and translate risks into prioritized initiatives.
Attorneys / Judges ➡	CIS RAM allows you to achieve a **reasonable** implementation of the CIS Controls by evaluating your risks in a manner that aligns with judicial reasoning.
Regulators ➡	CIS RAM balances risks with burdens to match regulators' expectations for reasonable and appropriate **compliance**.
Customers ➡	The **Acceptable Risk Definition** is stated in plain language allowing you to explain to Customers how their information is **appropriately protected**.
IT and Security Professionals ➡	CIS RAM allows you to prioritize what matters to interested parties, and to accept risks at a level the enterprise agreed to.

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

CIS RAM – Reasonable Implementation



Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

CIS RAM – Acceptable Risk Formula

Impact Threshold	×	Expectancy Threshold	=	Risk Threshold
3	×	3	=	9
		...therefore...		
	Acceptable Risk		<	**9**

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

CIS RAM – Acceptable Formula

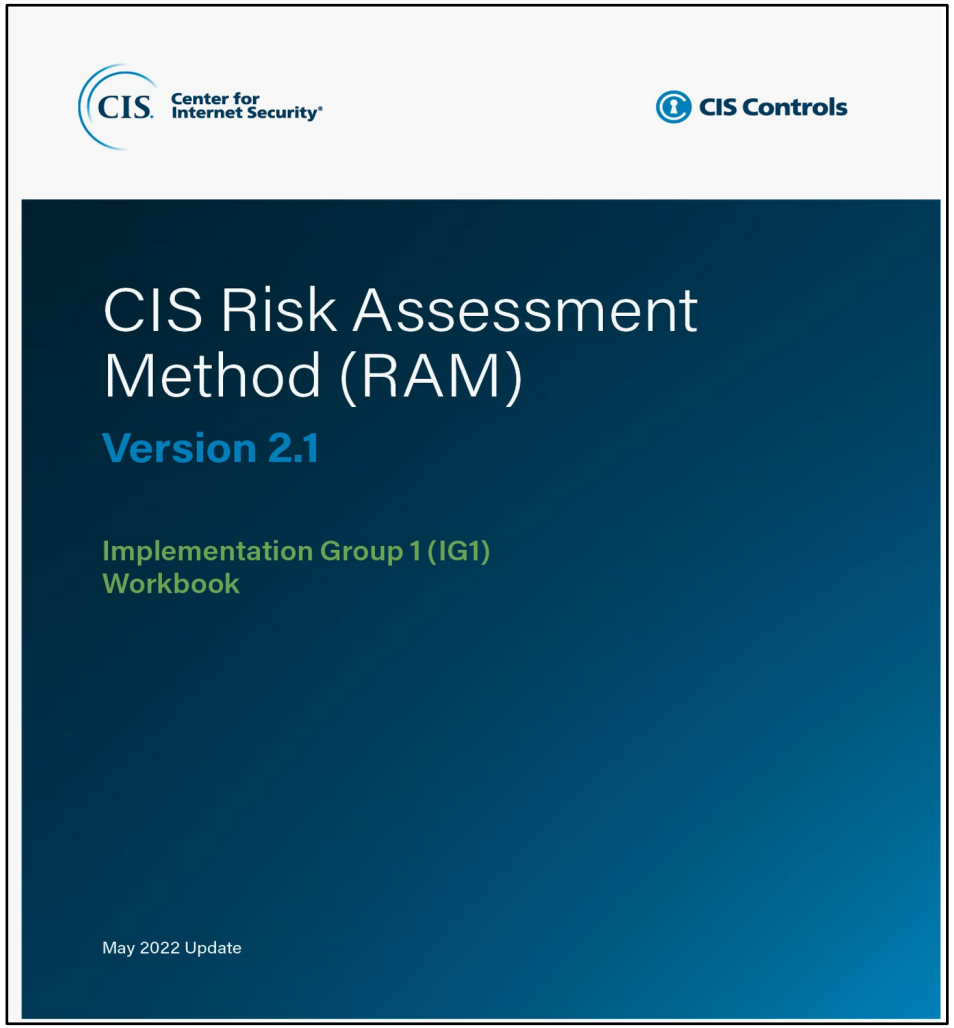
Impact Scores	Impact to Mission	Impact to Operational Objectives	Impact to Obligations
Definition:	**Define the enterprise's Mission (why the risk is worth engaging):**	**Define the enterprise's Operational Objectives (the enterprise's goals):**	**Define the enterprise's Obligations (duty of care owed to others):**
1 **Negligible**	Describe a negligible impact to the Mission.	Describe a negligible impact to the Operational Objectives.	Describe a negligible impact to the Obligations.
2 **Acceptable**	Describe an acceptable impact to the Mission.	Describe an acceptable impact to the Operational Objectives.	Describe an acceptable impact to the Obligations.
3 **Unacceptable**	Describe an unacceptable impact to the Mission.	Describe an unacceptable impact to the Operational Objectives.	Describe an unacceptable impact to the Obligations.
4 **High**	Describe a high, recoverable impact to the Mission.	Describe a high, recoverable impact to the Operational Objectives.	Describe a high, recoverable impact to the Obligations.
5 **Catastrophic**	Describe an unrecoverable impact to the Mission.	Describe an unrecoverable impact to the Operational Objectives.	Describe an unrecoverable impact to the Obligations.

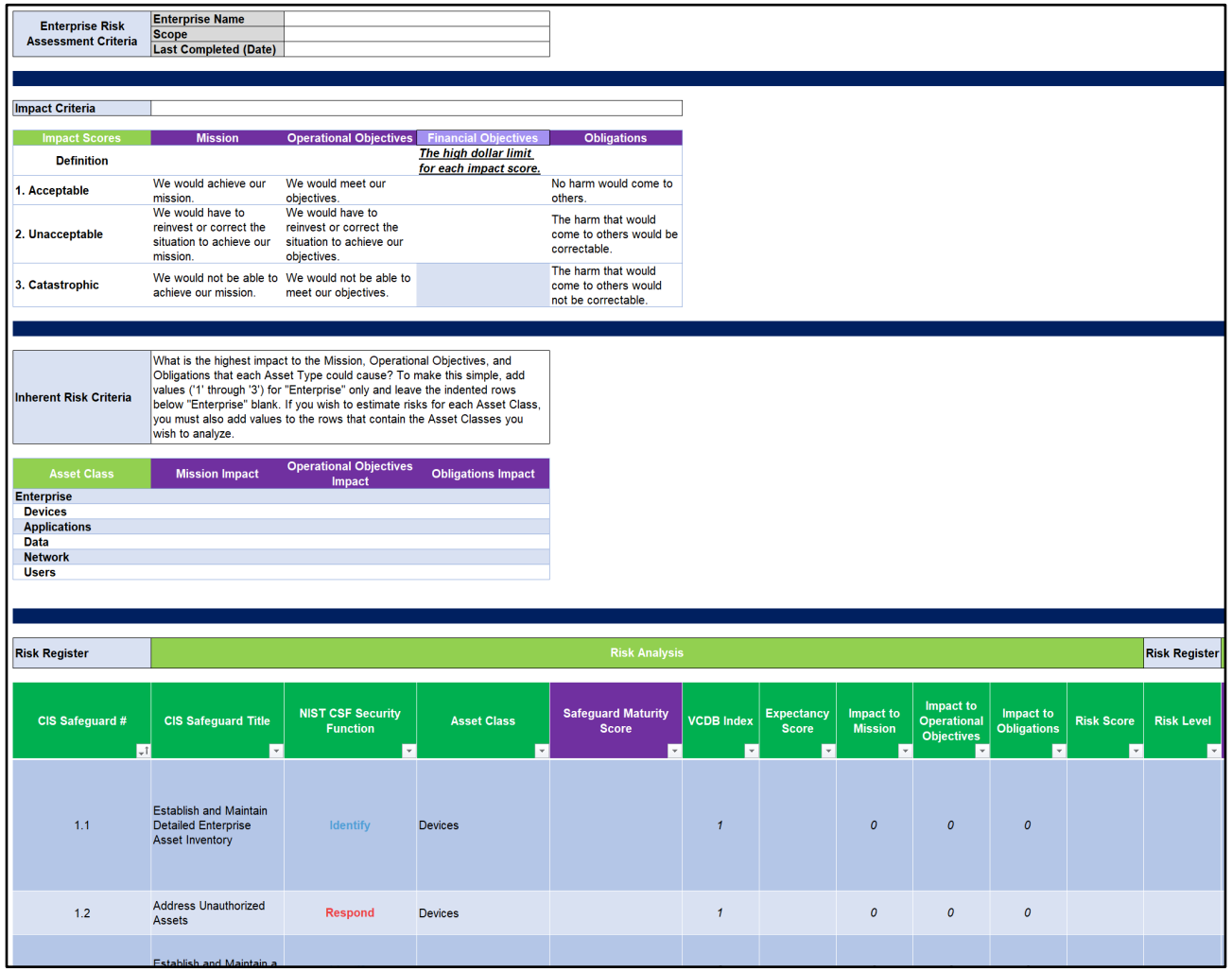
Expectancy Scores	Expectancy Scores Defined
1	Not foreseeable
2	Foreseeable, but unexpected
3	Expected, but not common
4	Common
5	Could be happening now

Impact Threshold	×	Expectancy Threshold	=	Risk Threshold
3	×	3	=	9
		...therefore...		
Acceptable Risk			**<**	**9**

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

CIS RAM – IG1 Workbook





Enterprise Risk Assessment Criteria	Enterprise Name	
	Scope	
	Last Completed (Date)	

Impact Criteria	

Impact Scores	Mission	Operational Objectives	Financial Objectives	Obligations
Definition			*The high dollar limit for each impact score.*	
1. Acceptable	We would achieve our mission.	We would meet our objectives.		No harm would come to others.
2. Unacceptable	We would have to reinvest or correct the situation to achieve our mission.	We would have to reinvest or correct the situation to achieve our objectives.		The harm that would come to others would be correctable.
3. Catastrophic	We would not be able to achieve our mission.	We would not be able to meet our objectives.		The harm that would come to others would not be correctable.

Inherent Risk Criteria	What is the highest impact to the Mission, Operational Objectives, and Obligations that each Asset Type could cause? To make this simple, add values ('1' through '3') for "Enterprise" only and leave the indented rows below "Enterprise" blank. If you wish to estimate risks for each Asset Class, you must also add values to the rows that contain the Asset Classes you wish to analyze.

Asset Class	Mission Impact	Operational Objectives Impact	Obligations Impact
Enterprise			
Devices			
Applications			
Data			
Network			
Users			

Risk Register	Risk Analysis	Risk Register

CIS Safeguard #	CIS Safeguard Title	NIST CSF Security Function	Asset Class	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Obligations	Risk Score	Risk Level
1.1	Establish and Maintain Detailed Enterprise Asset Inventory	Identify	Devices		1		0	0	0		
1.2	Address Unauthorized Assets	Respond	Devices		1		0	0	0		
	Establish and Maintain a										

Source: https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method

Wrap Up

Questions?

If interested, please contact us at CyberArch@uga.edu