CIS Center for Internet Security®

CIS Controls

CIS Risk Assessment Method (RAM)

Version 2.1

Implementation Group 1 (IG1)

January 2022

CIS RAM v2.1

Implementation Group 1 (IG1): Workbook Edition

January 2022

Background and Acknowledgments

The original content of CIS RAM was developed by HALOCK Security Labs. It is based on their extensive experience helping clients and legal authorities resolve cybersecurity and due care issues. Recognizing the universal need for a vendor-neutral, open, industry-wide approach to these issues, HALOCK Security Labs and CIS collaborated so that this process would be openly available to the entire cybersecurity community. This generous contribution of intellectual property (and the extensive work to generalize and tailor it to the CIS Controls) has been donated to CIS and is now available and maintained as a CIS community-supported best practice.

As with all CIS work, we welcome your feedback, and we welcome volunteers who wish to participate in the evolution of this and other CIS products.

CIS gratefully acknowledges the contributions provided by HALOCK Security Labs and the DoCRA Council in developing CIS RAM and the CIS RAM Workbook.

Significant contributions to Version 2.1 of CIS RAM were made by:

Editor

Chris Cronin, Partner, HALOCK Security Labs

Contributors

Aaron Piper, CIS
Himani Solanki, ISO/IEC 27001:2013 Internal Auditor
Jim Bertel, CISSP, CISM, CRISC, CEH, Director, Security Risk Management, Reinsurance Group of America
Rick Doten, VP, Information Security, Centene Corporation
Robin Regnier, CIS
Roger D. Brotz, Senior Director of Security, Acadia Software
Valecia Stocchetti, CIS

Contents

Forward

The objective of the Center for Internet Security® Risk Assessment Method (CIS RAM) is to help enterprises plan and justify their implementation of CIS Critical Security Controls® (CIS Controls®) Versions 7.1 and 8, whether those Controls are fully or partially operating. Few enterprises can apply all of the CIS Controls in all environments and protect all information assets. While the CIS Controls offer foundational elements for Information Technology (IT) risk reduction, some Controls may pose more of a burden to enterprises than the benefit they provide. A CIS RAM risk assessment will help enterprises implement Safeguards that reduce risks both to the public and to themselves.

Who is This Risk Assessment Method for?

CIS RAM is a highly extensible and flexible method for assessing cybersecurity risk. CIS RAM for Implementation Group 1 (CIS RAM for IG1) is intended for enterprises using the IG1 set of CIS Safeguards. CIS RAM for IG1 uses CIS RAM Core's three principles and 10 practices, and supports the legal, regulatory, and information security standards that CIS RAM Core addresses.

CIS RAM for IG1 is written as a user manual for the Workbook, a set of Microsoft® Excel® worksheets provided by CIS as a template for conducting a risk assessment.

Risk assessments may be conducted in a variety of ways. They may focus initially on recommended CIS Controls to identify vulnerabilities within a given scope; they may focus primarily on information assets to determine how well protected those assets are by the CIS Controls; or they may focus first on known threats to see how they would play out in an environment. Risk assessments may also vary by whether they use quantitative analysis (purely numerical representations of risk) or qualitative analysis (ranked value statements). CIS RAM for IG1 focuses on a set of CIS Safeguards within the CIS Controls, and a combination of qualitative and quantitative analyses.

This approach will make cybersecurity risk assessments accessible to enterprises that have limited cybersecurity expertise, yet will still provide them with meaningful, data-driven analysis of the reasonableness of their cybersecurity controls and programs.

CIS RAM for IG1 as Part of the CIS RAM Family of Documents

CIS RAM for IG1 is one module in the CIS RAM family of documents. CIS RAM Core, the foundation for other documents in the CIS RAM family, provides the authoritative and methodological basis for all CIS RAM modules. Each module presents a variation of CIS RAM, and is suitable for enterprises with different needs.

The user will need to use professional judgment (either theirs, or the judgment of specialized practitioners) to conduct the risk assessment. Professional judgment will help:

- Determine the scope of the assessment
- Define the enterprise's Mission, Objectives (Operational and Financial), and Obligations
- Decide which risks will be evaluated
- Identify vulnerabilities and foreseeable threats
- Estimate expectancy and impact
- Recommend Risk Treatment Safeguards

Glossary

Appropriate	A condition in which risks to information assets will not foreseeably create harm that is greater than what the enterprise or interested parties can tolerate.
Asset Class	A group of information assets that are evaluated as one set based on their similarity. Devices, applications, data, users, and network devices are examples, all of which fall under the category of enterprise assets.
Burden	The negative impact that a Safeguard may pose to the enterprise, or to others.
Business Owners	Personnel who own business processes, goods, or services that information technologies support (customer service managers, product managers, sales management, etc.).
CIS Critical Security Controls (CIS Controls)	A prioritized set of actions to protect information assets from threats, using technical or procedural CIS Safeguards.
CIS Safeguard	Technical or procedural protections that prevent or detect threats against information assets. CIS Safeguards are implementations of the CIS Controls.
Constituents	Individuals or enterprises that may benefit from effective security over information assets, or may be harmed if security fails.
Due Care	The amount of care that a reasonable person would take to prevent foreseeable harm to others.
Duty of Care	The responsibility to ensure that no harm comes to others while conducting activities, offering goods or services, or performing any acts that could foreseeably harm others.
Expectancy	The estimation that if an incident were to occur that it would be due to the threat described in the analysis.
Expectancy Score	The score, ranked from ‘1’ to ‘3’ in CIS RAM 2.1 for IG1, associated with the expectancy.
Impact	The harm that may be suffered when a threat compromises an information asset.
Impact Criteria	The rules used to define impacts.
Impact Score	The magnitude of impact that can be suffered. This is stated in plain language and is associated with numeric scales, ranked from ‘1’ to ‘3’ in CIS RAM for IG1.
Impact Type	A category of impact that estimates the amount of harm that may come to a party or a purpose. CIS RAM describes three impact types: Mission, Objectives (Operational and Financial), and Obligations.
Information Asset	Information or the systems, processes, people, and facilities that facilitate information handling.
Inherent Risk	The impact that would occur when a threat compromises an unprotected asset.
Maturity Score	A score to designate the reliability of a Safeguard’s effectiveness against threats, ranked from ‘1’ to ‘5.’
Reasonable	A condition in which a Safeguard will not create a burden to the enterprise that is greater than the risk it is meant to protect against.
Risk	The expectancy that a threat will compromise the security of an information asset and the magnitude of harm that would result.

Risk Analysis	The process of estimating the expectancy that an event will create a degree of impact. The foreseeability of a threat, the expected effectiveness of Safeguards, and an evaluated result are necessary components of risk analysis. Risk analysis may occur during a comprehensive risk assessment, or as part of other activities such as change management, vulnerability assessments, system development and acquisition, and policy exceptions.
Risk Assessment	A comprehensive project that evaluates the potential for harm to occur within a scope of information assets, controls, and threats.
Risk Management	A process for analyzing, mitigating, overseeing, and reducing risk.
Risk Treatment	To reduce the expectancy and/or impact of a risk using a Safeguard.
Risk Treatment Option	The selection of a method for addressing risks. Enterprises may choose to accept or reduce risks.
Risk Treatment Safeguards	Safeguards from the CIS Controls that may be implemented and operated to reduce the expectancy and/or impact of a risk.
Safeguard Risk	The risk posed by a recommended Safeguard. An enterprise's Mission or Objectives may be negatively impacted by a new security control. These impacts must be evaluated to understand their burden on the enterprise, and to determine whether the burden is reasonable.
Security	An assurance that characteristics of information assets are protected. *Confidentiality*, *Integrity*, and *Availability* are common security characteristics. Other characteristics of information assets such as velocity, authenticity, and reliability may also be considered if these are valuable to the enterprise and its constituents.
Threat	A potential or foreseeable event that could compromise the security of information assets.
Threat Model	A description of how a threat could compromise an information asset, given the current Safeguards and vulnerabilities around the asset.
Vulnerability	A weakness that could permit a threat to compromise the security of information assets.

Style Conventions in This Document

This document uses textual formatting to indicate the context of certain words and phrases. The following table documents these intentional uses.

USAGE	PURPOSE	EXAMPLES
Capitalized common words	To indicate a specific component of a CIS RAM risk analysis.	We estimate Mission Impact to ensure that our risks consistently address our purpose.
Common words in double quotes	To indicate an element within the CIS RAM risk assessment worksheet or document.	State your mission in the "Mission Impact" field.
Numbers within single quotes	To indicate a value that is in the Risk Register.	The resulting Risk Score is '8.'

Style Conventions in the Workbook

Some conventions that are used in the CIS RAM Workbook serve as guidelines to provide you with the simplest possible risk assessment experience. Beginners are encouraged to limit their input to the unlocked cells. However, the Workbook can be unlocked by selecting "Unprotect Sheet" under the "Review" menu.

FORMAT	PURPOSE	EXAMPLES
Locked text cells	Fixed text that anchors the risk assessment to good practices.	CIS Controls and Safeguards. Definitions (such as Impact Score definitions and the "Inherent Risk Criteria" cell).
Locked calculated fields	These cells automatically calculate Impact and Expectancy values based on previous information you provided (Impact Scores) or by comparing your Safeguard Maturity Score to the commonality of attacks against the Asset Class (Expectancy Scores).	Impact and Expectancy Scores.
Purple headers	To indicate required cells that you will use to enter information.	Impact definitions, Safeguard Maturity Score, Risk Treatment Option, Risk Treatment Maturity Score.
Light-purple headers	To indicate optional cells where you may choose to enter information.	Our Planned Implementation, Risk Treatment Safeguard Cost, Implementation Quarter, Implementation Year.

Acronyms and Abbreviations

CIS	Center for Internet Security
CIS RAM	Center for Internet Security Risk Assessment Method
DoCRA	Duty of Care Risk Analysis
FAIR	Factor Analysis of Information Risk
IG1	Implementation Group 1
ISO	International Organization for Standardization
IT	Information Technology
MAC	Media Access Control
NIST	National Institute of Standards and Technology
STEM	Science, technology, engineering, and mathematics
VERIS	Vocabulary for Event Recording and Incident Sharing

CIS RAM Principles and Practices

CIS RAM Core uses the Duty of Care Risk Analysis Standard[1] (DoCRA) as its foundation. DoCRA presents risk evaluation methods that are familiar to legal authorities, regulators, and information security professionals to create a "universal translator" for these disciplines. The standard includes three principles and 10 practices that guide risk assessors in developing this universal translator for their organization. The three principles state the characteristics of risk assessments that align to regulatory and legal expectations. The 10 practices describe features of risk assessments that make the three principles achievable. DoCRA describes the principles and practices as follows[2]:

Principles

1. Risk analysis must consider the interests of all parties that may be harmed by the risk.
2. Risks must be reduced to a level that would not require a remedy to any party.
3. Safeguards must not be more burdensome than the risks they protect against.

Practices

1. Risk analysis considers the likelihood that threats could create magnitudes of impact.
2. Tolerance thresholds are stated in plain language and are applied to each factor in a risk analysis.
3. Impact and likelihood scores have a qualitative component that concisely states the concerns of interested parties, authorities, and the assessing organization.
4. Impact and likelihood scores are derived by a quantitative calculation that permits comparability among all evaluated risks, safeguards, and against risk acceptance criteria.
5. Impact definitions ensure that the magnitude of harm to one party is equated with the magnitude of harm to others.
6. Impact definitions should have an explicit boundary between those magnitudes that would be acceptable to all parties and those that would not be.
7. Impact definitions address; the organization's mission or utility to explain why the organization and others engage risk, the organization's self-interested objectives, and the organization's obligations to protect others from harm.
8. Risk analysis relies on a standard of care to analyze current controls and recommended safeguards.
9. Risk is analyzed by subject matter experts who use evidence to evaluate risks and safeguards.
10. Risk assessments cannot evaluate all foreseeable risks. Therefore, risk assessments re-occur to identify and address more risks over time.

[1] Also known as "DoCRA" or "the DoCRA Standard" – https://www.docra.org

[2] Quotes from "the DoCRA Standard" – https://www.docra.org

Using CIS RAM for IG1

CIS RAM for IG1 Goals

CIS RAM for IG1 was designed to help you conduct a straightforward and simple risk assessment if your enterprise has limited cybersecurity expertise and few resources. IG1 enterprises should benefit from risk analysis, even if threat modeling, expectancy estimation, and risk criteria definitions normally require seasoned experts who may not be available to you. This document can best be used as a manual for its accompanying risk assessment Workbook. The intent of CIS RAM for IG1 is to help enterprises conduct a competent, data-driven risk assessment with the least amount of expertise possible.

You will be able to follow this document's illustrated instructions for completing a CIS RAM risk assessment and will receive explanations for each step as it occurs. This will help you quickly evaluate your cybersecurity risks with as much or as little background explanation of the analysis you will need.

After conducting a CIS RAM for IG1 risk assessment, your enterprise will understand how well prepared they are for the most and least commonly reported threats that cause security incidents. They will have a description for reasonable implementations of CIS Safeguards for risks that are unacceptably high. They will also have a baseline of risk analysis that they can use to further investigate and estimate risks in more detail, if needed.

Finally, while CIS RAM for IG1 is simpler than an assessment that models risks primarily by asset configurations or threats, it will demonstrate that your enterprise has implemented reasonable controls (or has a plan to implement reasonable controls) that should acceptably reduce risks for potentially harmed parties.

CIS RAM for IG1 Risk Assessment Process

CIS RAM for IG1 risk assessments involve the following activities:

- **Developing the Impact Criteria:** Define Impact Criteria, including the enterprise's Mission, Objectives, and Obligations.
- **Estimating the Inherent Risk Criteria:** Estimate the maximum impact that information assets could cause.
- **Evaluating the Risks:** Estimate the Expectancy and Impact of security incidents by stating the Maturity of a CIS Safeguard.
- **Recommending Safeguards:** Propose reasonable implementations of CIS Safeguards that would reduce unacceptable risks.

How CIS RAM for IG1 Works

CIS RAM for IG1 assists IG1 enterprises by significantly automating risk estimations and threat models. CIS RAM for IG1 reduces the complexity of risk analysis by providing the following:

1. A simple format for stating an enterprise's Impact Criteria and range of magnitudes of Impact that you or others may suffer.
2. A fixed definition for Expectancy Criteria and Risk Acceptance Criteria.
3. A simple Risk Register.

4. Automated Expectancy calculation based on the commonality of reported threats and the Maturity of the enterprise’s Safeguards.

All enterprises face a unique set of risks, and comprehensive risk assessments can identify and evaluate those unique risks. However, the automation within CIS RAM for IG1 narrows your enterprise’s risk assessment focus on how well your implementation of CIS Safeguards reduce the most and least common causes of reported cybersecurity incidents in the general population. This is a trade-off, as is all risk management. This trade-off helps smaller enterprises make data-driven risk decisions, but may not result in a comprehensive risk assessment that models all foreseeable threats in your environment.

Shown below are the key activities for conducting a risk assessment using CIS RAM for IG1:

ACTIVITY	
Developing the Impact Criteria	The risk assessor briefly defines their enterprise’s Mission, Objectives, and Obligations. The Workbook provides default language for Impact Scores, Expectancy Scores, and Risk Acceptance Criteria.
Estimating Inherent Risk Criteria	The risk assessor estimates the highest Impact that their information assets could create if they experienced a cybersecurity attack.
Evaluating Risks	The risk assessor states the Maturity (“Maturity Score”) of their implementation of each CIS Safeguard. This automatically creates a Risk Score by associating inherent risks with the commonality of attacks that the Safeguard prevents, and the Safeguard’s capability.
Recommending Safeguards	The risk assessor describes Safeguards that they believe will reasonably reduce risks to all parties.

Instructions and Parts

CIS RAM for IG1 will present each risk assessment activity and provide four parts:

1. **Instructions** for using a Workbook element
2. An **explanation** for the activity so the reader understands the intent and usage of the activity
3. **Examples** for information the risk assessor can add to the Workbook
4. **Alternatives** that the risk assessor may choose if the default values in the Workbook are not sufficient for their needs

CIS RAM for IG1 Instructions

The CIS RAM for IG1 Workbook contains all of the materials described in these instructions. The Workbook may be downloaded from our website here, or may be downloaded from CIS WorkBench here. The default materials, elements, and text will assist you in your analysis. This document does not imply that risk assessors must follow these instructions exactly. Risk assessors may find some of the default material to be insufficient for their needs. Instructions will provide examples and potential alternatives to the Workbook's default text and elements. Risk assessors should either adhere to these instructions or innovate from them based on their comfort level.

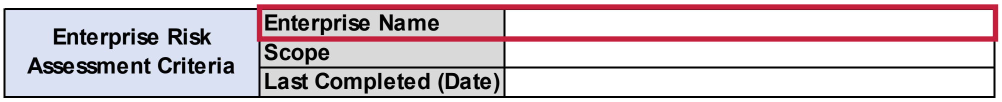
It is also encouraged to read other documents in the CIS RAM family to understand how to model threats, estimate expectancies and impacts, use qualitative and quantitative methods, or align CIS RAM with other risk assessment methods.

Risk Register Record Header

ENTERPRISE NAME

Since the Risk Register is useful as a record for cybersecurity risk management, dedicate time to state the name of your enterprise that the risk assessment applies to, describe the scope of the enterprise that the Risk Register contains, and enter the date that the Risk Register was last updated.

FIGURE 1. Enterprise Name



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

Instructions: In the "Enterprise Name" field, state the name of your enterprise.

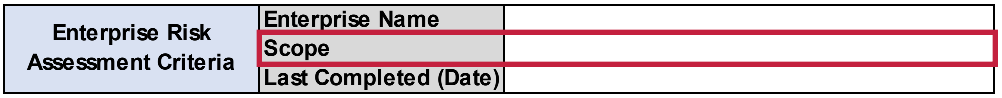
Explanation: The enterprise will be able to use the risk assessment as a record of their risk management program. State your enterprise's name here.

Examples: Center for Internet Security, Inc., State Department of Commerce, Secretary of State's Office, etc.

Alternatives: None apply.

SCOPE

FIGURE 2. Scope



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

Instructions: In the "Scope" field, state or describe the portion of the enterprise that the risk assessment is evaluating.

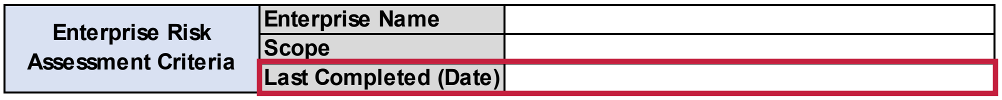
Explanation: Risk assessments may apply to the whole enterprise, or just portions of it. Enterprises may operate in an environment that has different controls from other parts of their environment, or they may prioritize their risk management in one portion of the enterprise. Communicate to the Workbook's readers what portion of the enterprise these controls and risks apply to. Each enterprise should work with auditors, authorities, or stakeholders to verify that the scope of the assessment does not exclude information assets that could pose harm to themselves or others.

Examples: All assets, Production DMZ, <Domain Name> network, Headquarters, Corporate network, Store locations, etc.

Alternatives: None apply.

LAST COMPLETED (DATE)

FIGURE 3. Last Completed



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

Instructions: In the "Last Completed (Date)" field, enter the date that the Risk Register was last updated.

Explanation: Risk assessments are often used over time to update current controls or other information. Let the Workbook reader know when the Risk Register was last updated by entering in the date here.

Examples: August 1, 2021

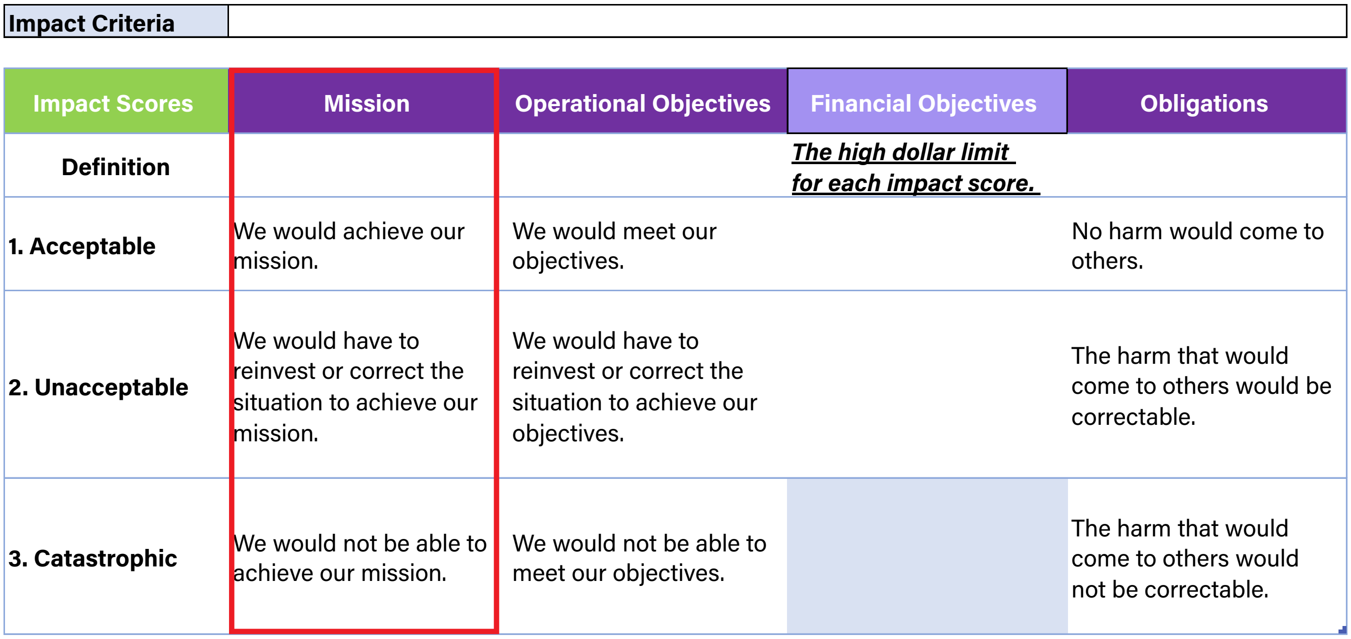
Alternatives: None apply.

Impact Criteria

Since CIS RAM requires that risks consider all interested parties, Impact Criteria should clearly state those interests. Enterprises have their Mission (the value or benefit they create), their Objectives (their self-interests), and their Obligations (to prevent harm to others). The Workbook helps define these terms for use in assessing magnitudes of harm in the Risk Register.

FIGURE 4. Mission

MISSION



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.

Instructions: In the "Mission" field, state the value your enterprise provides to the public, your customers, or others. If your enterprise has already stated their Mission, you may include it here.

Explanation: An enterprise's Mission is both the benefit they provide others, as well as the reason that we engage in risk to begin with. We include Mission in risk analysis to indicate whether the risk of a threat intolerably harms the benefit we provide, and to ensure that Safeguards do not reduce those benefits while reducing risks to Obligations.

Examples:

TABLE 1. Example Mission Definitions

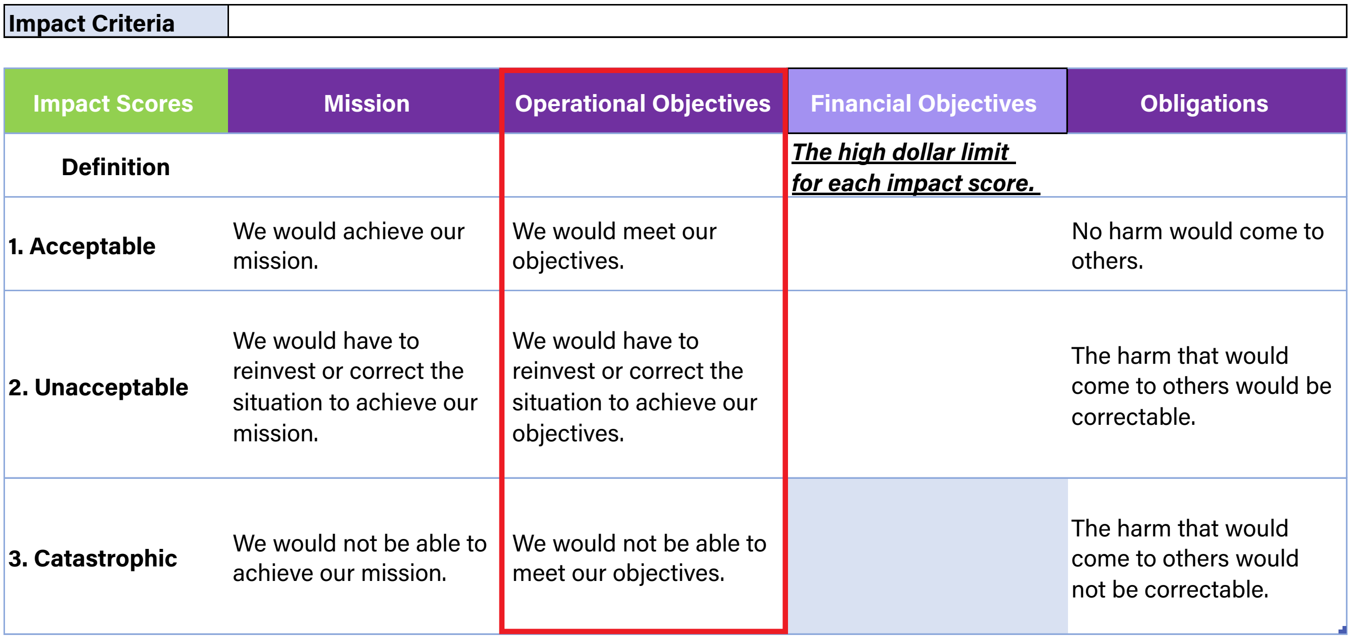
ENTERPRISE TYPE	EXAMPLE MISSIONS
Healthcare Provider	• To improve patient health. • To sustain and improve the health of our community. • To improve patient health outcomes. • To provide essential healthcare to each member of our underserved community. • To provide healthcare options to the people in our community. • To advance the effectiveness of healthcare through research. • To educate the next generation of family practitioners through patient care.
Bank, Credit Union	• To provide financial services and investment products to our customers. • To provide financial security to our members through planning services, and financial products that meet or exceed market performance. • To enable our community to thrive through investments in their homes, education, and local businesses. • To provide our household customers with every financial service option they may need.

ENTERPRISE TYPE	EXAMPLE MISSIONS
Retail	• To provide unique and quality products that our customers cannot find anywhere else. • To provide quality products at low prices. • To service and support our customers who buy from us. • To be the most trusted name in the business. • To offer bulk goods at near-wholesale prices. • To provide expert support for the latest in consumer technology. • To help clients achieve their health goals through healthy food and nutrition products.
Nonprofit, NGO	• To inspire girls to succeed in science, technology, engineering, and mathematics (STEM) specialties. • To enable impoverished communities to develop and grow economic self-sufficiency. • To reduce drug and alcohol dependency in our community. • To support our community through faith-based action. • To situate newly arriving immigrants in homes, schools, and employment. • To improve the cybersecurity health of the country's critical infrastructure.
Professional Services	• To provide our clients with expert advice at competitive rates. • To represent our clients' interests to the best of our ability. • To make life's most important financial decisions easier.
Education	• To prepare each generation to succeed to the best of their ability. • To inspire young artists to find their voice. • To meet or exceed performance standards issued by the state. • To help each student achieve their potential.
Hospitality	• To provide comfortable, safe lodging for travelers. • To create a luxurious experience. • To help our guests forget all of their troubles. • To provide a romantic getaway for our guests. • To create a full experience for vacationing families and couples.
Manufacturing	• To create custom products quickly and inexpensively. • To provide assemblers with components that match their specifications without variance. • To provide wholesalers with high-volume, plastic consumer products that meet stringent engineering requirements.
Critical Infrastructure	• To provide reliable power to our region. • To provide municipalities with choices in affordable and sustainable energy options. • To move America's products on time, on budget, as required. • To ensure the safety of all in-flight aircraft and their passengers, from take-off to landing. • To ensure consumer confidence in the safety of food products.

Alternatives: Enterprises may use one phrase or multiple phrases if they apply to the enterprise's Mission. You should try to keep this definition as simple as possible, and should only reference something the enterprise already measures its success by.

FIGURE 5. Operational Objectives

OPERATIONAL OBJECTIVES



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.

Instructions: In the "Operational Objectives" field, state a key measure for self-focused success. Preferably, this would be a goal that your enterprise currently tries to achieve, and measures.

Explanation: Operational Objectives (e.g., profitability, growth in market presence or share price, maintaining an operational budget), can be diminished as a result of cybersecurity attacks. They can also be diminished by expensive or restrictive cybersecurity controls. Risk assessors consider the expectancy that threats and Safeguards will diminish Operational Objectives.

Examples:

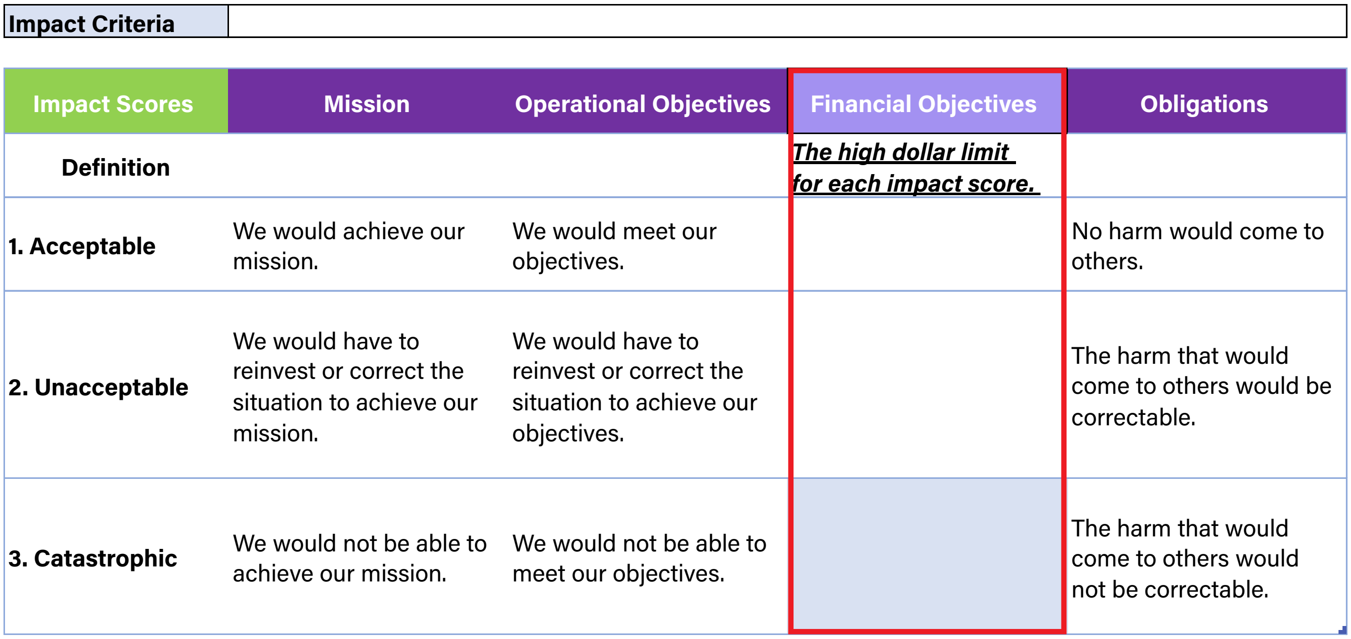
TABLE 2. Example Operational Objectives

ENTERPRISE TYPE	EXAMPLE OBJECTIVES
Healthcare Provider	• Maintain a balanced budget (nonprofit) • Grow the Foundation (nonprofit) • Profitability (for-profit) • Meet our plan for growth of clinical locations
Bank, Credit Union	• Return-on-assets must meet or exceed (x%) annually • Share growth (credit unions) • Loan-to-Share Ratio (credit unions)
Retail	• Profitable growth • Growth in share value (public retailers)
Nonprofit, NGO	• Maintain a balanced budget • Grow the Foundation
Professional Services	• Maintain position in the marketplace • Profitable growth
Education	• Maintain an operational budget • Grow the Foundation
Hospitality	• Profitable growth • Meet our plan for growth in locations
Manufacturing	• Profit • Profitable growth
Critical Infrastructure	• Profit • Profitable growth

Alternatives: Enterprises may use one phrase or multiple phrases, if appropriate. You should try to keep this definition as simple as possible, and should only reference something the enterprise already uses to measures its success.

FIGURE 6. Financial Objectives

FINANCIAL OBJECTIVES (OPTIONAL)



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.

Instructions: In the “Financial Objectives” field, you may wish to state the highest financial value (e.g., dollars) that would be appropriate for the Impact Magnitude. This is not a required field.

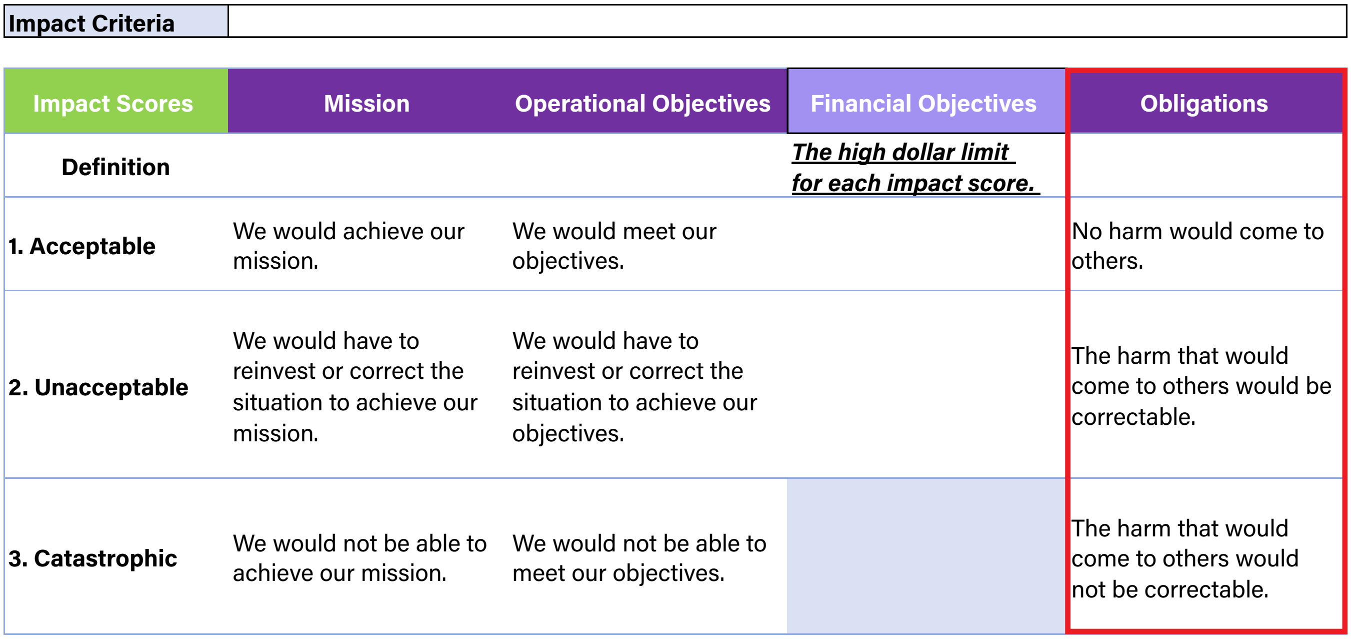
Explanation: Some enterprises find that financial analysis is an important part of how decisions are made about cybersecurity investments. Since CIS RAM’s risk analysis compares unlike things, the Impact Criteria model presents financial values in terms of upper limits, rather than ranges of continuous data. This can be read as: “If this risk occurs, we would have to reinvest or correct the situation to achieve our objectives, which would mean costs go up to $x, if $x was in the row labeled “2. Unacceptable.”

Examples: If an enterprise would accept unexpected costs up to $10,000 but no more, they would place “$10,000” in the “Financial Objectives” field in the row labeled “1. Acceptable.” If the enterprise could still meet their Operational Objectives after incurring costs of up to $1MM, but could not meet them if costs exceeded $1MM, then they would place “$1MM” in the “Financial Objectives” field in the row labeled “2. Unacceptable.” You will notice that you cannot add cost amounts in the “3. Catastrophic” field. There is no reason to put a dollar value in that field, because once an incident crosses the line into catastrophic territory, then $1MM + $1 is as bad as $1B; either way they would not survive.

Alternatives: You may decide to not use this field.

FIGURE 7. Obligations

OBLIGATIONS



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.

Instructions: In the “Obligations” field, state a kind of harm you may cause someone else as a result of a cybersecurity incident.

Explanation: An important aspect of risk management is reducing the expectancy of harm we may cause others. Risks caused by threats and burdensome Safeguards should therefore consider the risk of harm to others.

Examples: Note that these examples all reference preventing harm to others. To prevent theft of a customer’s identity; To ensure customer privacy; To protect customer finances; To ensure ongoing protection of client interests; To secure intellectual property in our care; To prevent our systems from being used to attack other systems and networks.

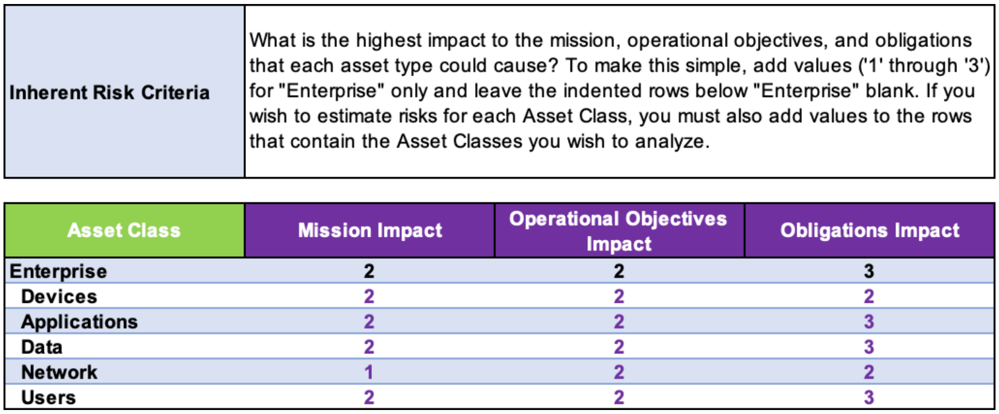
Alternatives: Enterprises may use one phrase or multiple phrases, if appropriate. You should try to keep this definition as simple as possible.

Inherent Risk Criteria

CIS RAM for IG1 automates impact estimates in the Risk Register. To do that, the Workbook first needs to understand inherent risks of your information assets. Inherent Risk is the potential maximum impact that may occur if there are no controls in place. The Inherent Risk of a database that stores login credentials of 1,000 bank customers is the sum of dollars stored in those users' accounts. Similarly, the Inherent Risk of an application that a company depends on for its operations is loss of those operations.

You may use the Inherent Risk Criteria table minimally, or fully. Minimal use of the table only provides Inherent Risk values in the "Enterprise" row. Note that while this may make preparing your risk assessment simpler, your risks may become indistinguishable and clustered with similar Risk Scores, as the Expectancy Scores for all Safeguards will be based on the Asset Class with the highest incident count (in the Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (VCDB)). Full use of the Asset Class table is preferred, as it will add some variation in the scores and will require some careful consideration while preparing the risk assessment.

FIGURE 8. Inherent Risk Criteria



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	2	2	3
Devices	2	2	2
Applications	2	2	3
Data	2	2	3
Network	1	2	2
Users	2	2	3

Instructions: Review the definitions for each magnitude in the Impact Scores table. Consider the magnitude of harm that each Asset Class could potentially cause if it were attacked in a cybersecurity incident. Record in the Asset Class table the potential magnitude of Impact (the Inherent Risk) that the Asset Class in each row could create to the Mission, Operational Objectives, and Obligations. Scoring is done on a scale of '1' to '3.' Note that while CIS RAM for IG1 uses Impact Scores ranging from '1' to '3' (for simplicity), CIS RAM for IG2 and IG3 use Impact Scores ranging from '1' to '5.'

Explanation: The Inherent Risk Criteria table stores the maximum Impact Value that information assets may pose to the Mission, Operational Objectives, and Obligations. Devices may pose an Inherent Mission Impact of '2' while applications may pose an inherent Obligations Impact of '3.' Each time the Risk Register references devices, it will use a Mission Impact Score of '2.' Each time the Risk Register references applications, it will use a Obligations Impact Score of '3.'

Examples:

FIGURE 9. Example Inherent Risk Criteria

Asset Class	Mission Impact	Operational Objectives Impact	Obligations Impact
Enterprise	2	2	3
Devices	2	2	2
Applications	2	2	3
Data	2	2	2

Alternatives: You may either limit your use of the table to the "Enterprise" row for easy setup and high-level risk assessments, or you may complete the table to provide more granularity in your risk assessment. You may also wish to add other asset classes to the table. If you do this within the table structure, the new information assets will populate in the "Asset Class" field in the Risk Register shown in Figure 9 on page 13.

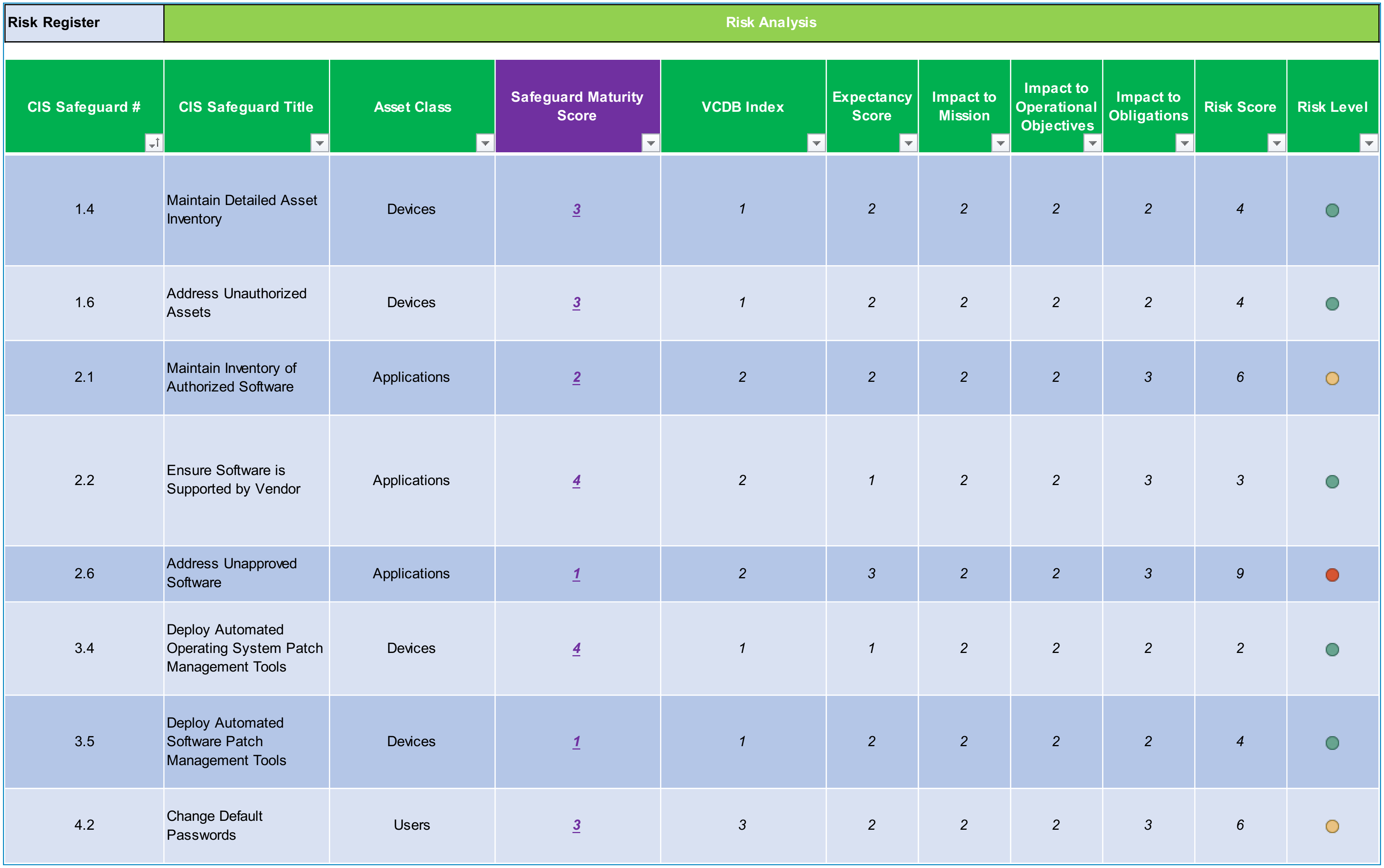
Note: The Risk Register below will populate its three Impact Scores by referring to the values you put in the Asset Class table. If you notice that your three Impact Scores (and consequently your Risk Scores) evaluate to '0' in the Risk Register, it is likely because the Impact Values for the corresponding Asset Class are blank in this table.

Risk Register: Risk Analysis

Now that you have established your risk assessment parameters, you can start estimating your cybersecurity risks using the Risk Register in the Workbook. The Risk Register includes all of the fields you will need to evaluate your cybersecurity risks that are associated with CIS Controls for IG1. Due to the automation in the Workbook and your preparation in previous activities, you will only need to enter information in one field of the Risk Register to analyze your risks, although some fields are available for you to adjust to suit your needs.

The CIS RAM for IG1 Risk Register will help you identify and evaluate risks that are associated with IG1 CIS Safeguards. Your enterprise may have risks that go beyond what these Safeguards will indicate. If resources permit, or if your enterprise believes their risks may extend beyond the CIS Safeguards in IG1, you may seek assistance from risk experts to help identify and evaluate those risks, or to help design reasonable controls to address those risks.

FIGURE 10. Risk Register: Risk Analysis (CIS Controls v7.1)



Risk Register	Risk Analysis									
CIS Safeguard #	CIS Safeguard Title	Asset Class	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Obligations	Risk Score	Risk Level
1.4	Maintain Detailed Asset Inventory	Devices	3	1	2	2	2	2	4	🟢
1.6	Address Unauthorized Assets	Devices	3	1	2	2	2	2	4	🟢
2.1	Maintain Inventory of Authorized Software	Applications	2	2	2	2	2	3	6	🟡
2.2	Ensure Software is Supported by Vendor	Applications	4	2	1	2	2	3	3	🟢
2.6	Address Unapproved Software	Applications	1	2	3	2	2	3	9	🔴
3.4	Deploy Automated Operating System Patch Management Tools	Devices	4	1	1	2	2	2	2	🟢
3.5	Deploy Automated Software Patch Management Tools	Devices	1	1	2	2	2	2	4	🟢
4.2	Change Default Passwords	Users	3	3	2	2	2	3	6	🟡

Instructions: Read each Safeguard as it is stated in the Risk Register. If you need more guidance about what that Safeguard entails, read its description in the official CIS Controls document. Determine the maturity of the Safeguard as you use it, and enter that maturity in the "Safeguard Maturity Score" cell for that Safeguard. The remainder of your risk analysis will be automatically filled in. Read the Maturity Scores guidance in Appendix A to help you select the correct score. For users of CIS-Hosted CSAT (Controls Self Assessment Tool) and CIS CSAT Pro, you may choose to utilize CSAT scoring to populate the "Safeguard Maturity Score" column in CIS RAM 2.1 for IG1. Additional guidance on how to import CSAT scoring can be found in Appendix C. Ensure that your enterprise's method for scoring Safeguards in CSAT aligns closely enough with Safeguard Maturity Scores in CIS RAM. Adjustments may be needed based on your enterprise's current scoring methodology.

Explanation: Your Safeguard Maturity Score is paired with the Asset Class to create a Expectancy Score. Asset Classes are aggregations of threat activities that are listed in the VCDB. Asset Classes that appear more often in the VCDB push Expectancy Scores higher. Maturity Scores for Safeguards push Expectancy Scores lower. An index is provided in the Workbook to associate Maturity Scores and Asset Classes to create Expectancy Scores. The Risk Register simply selects the right Expectancy Score based on your input.

The Risk Register then multiplies the Expectancy Score to the highest Impact Score to create the Risk Score. All Risk Scores below '6' are acceptable and appear as green "Risk Levels." Risks that score '6' are unacceptable and appear as yellow "Risk Levels." Risks that score as '9' are high and appear as red "Risk Levels."

See Appendix D for guidance on unprotecting the spreadsheet to add rows, or to change default values, formulas, and lookups.

Examples: Examples are provided in Figure 9.

Alternatives: You may elect to change your use of the Risk Register in many ways:

1. You may decide that a specific Safeguard should be evaluated with a different Asset Class than the one that is provided by default. The value in the Asset Class column can be changed by using the drop-down list. Note that the Impact columns to the right will be populated by the scores for that Asset Class in the Inherent Risk Criteria table.
    a. Note: The Asset Class you select in each Risk Register row should have a value ('1' through '3') in the Asset Class table. If you only populated the "Enterprise" row in the Asset Class table, then the Risk Register will only calculate Impact Scores (and consequently Risk Scores) when the Asset Class is "Enterprise" for that row. If only the Enterprise Asset Class is filled out in the Asset Class table, then ensure that all Safeguards are assigned the "Enterprise" Asset Class to correctly calculate the risk. If you wish to calculate Risk Scores for other Asset Classes, add Impact Values for those asset classes in the Asset Class table.
2. You may wish to evaluate a Safeguard's risk using a different Impact Score than the values that are automatically provided in the "Impact to Mission," "Impact to Operational Objectives," and "Impact to Obligations" columns. If that is the case, then manually enter those values. Note that this will replace an Excel "vLookup" function in that cell with the number you enter. If you wish to revert to the automated Impact Value, then copy the "vLookup" function from that same column in a different row and paste the function into the cell you wish to re-automate.
3. You may wish to evaluate the risk associated with a Safeguard more than once. For example, if you apply a Safeguard differently for file servers than for end-user devices, you may wish to add a row to the Risk Register table (either at the bottom of the table or by inserting a row next to the same Safeguard). You may manually enter the relevant Safeguard information into that row. The table's lookup tables and automated calculations will be automatically created in your new row.

Risk Register: Risk Treatment

When risks are identified as unacceptably high (the Risk Score is ‘6’ or ‘9’), you should consider a Risk Treatment Safeguard that will reduce your risks to an acceptable level.

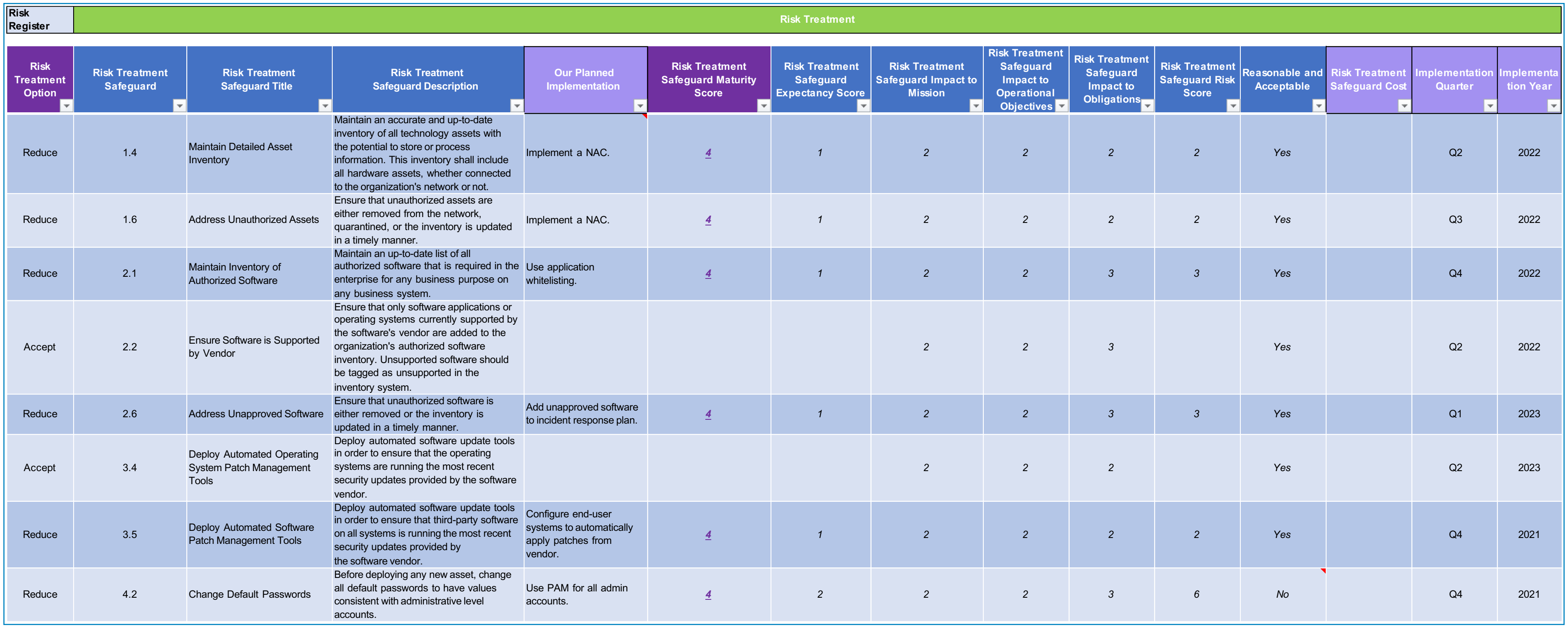
The “Risk Treatment” column includes two values. Select “Accept” for risks that you will not reduce (typically, acceptably low risks with Risk Scores less than ‘6’), and select “Reduce” for risks with Risk Scores that are unacceptably high (where risk scores are ‘6’ or ‘9’).

The Risk Register provides default values in several columns to assist you, but you may wish to describe other safeguards in these columns. You will notice that the default values for Risk Treatment Safeguard and Risk Treatment Safeguard Title are identical to the “CIS Safeguard #” and the “CIS Safeguard Title” columns to the left. This is because we assume that you will be able to apply the CIS Safeguard as the CIS Controls describes it.

You may change the values in these columns if you need to use an alternative safeguard to address the risk in that row. For example, Safeguard 13.6, “Utilize approved whole disk encryption software to encrypt the hard drive of all mobile devices,” may not be practical for all enterprise mobile devices. The Safeguard reduces the risk of breaching sensitive data or credentials when the device is stolen, lost, or otherwise misused. However, some devices are not completely in the control of the enterprises that use them and their storage volumes may not be encrypted or may have weak encryption. In such cases, the enterprise may plan to use encrypted folders within the storage volume, or may prevent mobile devices from connecting to sensitive networks. An enterprise that decides to prevent mobile devices from connecting to their network may leave “Risk Treatment Safeguard” blank. They could describe “Risk Treatment Title” as “Do not connect mobile devices to the network” and could optionally describe the “Our Planned Implementation” cell as, “We will use policies and Media Access Control (MAC) filters to prevent mobile devices from joining our network.”

Alternate safeguards should still reduce risks to the Mission, Operational Objectives, and Obligations to acceptable levels, but CIS RAM and the Risk Register provide you the flexibility to evaluate alternative means for reducing risks if the CIS Safeguard is not a practical option for your enterprise.

FIGURE 11. Risk Register: Risk Treatment (CIS Controls v7.1)



Risk Register	Risk Treatment													
Risk Treatment Option	Risk Treatment Safeguard	Risk Treatment Safeguard Title	Risk Treatment Safeguard Description	Our Planned Implementation	Risk Treatment Safeguard Maturity Score	Risk Treatment Safeguard Expectancy Score	Risk Treatment Safeguard Impact to Mission	Risk Treatment Safeguard Impact to Operational Objectives	Risk Treatment Safeguard Impact to Obligations	Risk Treatment Safeguard Risk Score	Reasonable and Acceptable	Risk Treatment Safeguard Cost	Implementation Quarter	Implementa tion Year
Reduce	1.4	Maintain Detailed Asset Inventory	Maintain an accurate and up-to-date inventory of all technology assets with the potential to store or process information. This inventory shall include all hardware assets, whether connected to the organization's network or not.	Implement a NAC.	4	1	2	2	2	2	Yes		Q2	2022
Reduce	1.6	Address Unauthorized Assets	Ensure that unauthorized assets are either removed from the network, quarantined, or the inventory is updated in a timely manner.	Implement a NAC.	4	1	2	2	2	2	Yes		Q3	2022
Reduce	2.1	Maintain Inventory of Authorized Software	Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	Use application whitelisting.	4	1	2	2	3	3	Yes		Q4	2022
Accept	2.2	Ensure Software is Supported by Vendor	Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.				2	2	3		Yes		Q2	2022
Reduce	2.6	Address Unapproved Software	Ensure that unauthorized software is either removed or the inventory is updated in a timely manner.	Add unapproved software to incident response plan.	4	1	2	2	3	3	Yes		Q1	2023
Accept	3.4	Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.				2	2	2		Yes		Q2	2023
Reduce	3.5	Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.	Configure end-user systems to automatically apply patches from vendor.	4	1	2	2	2	2	Yes		Q4	2021
Reduce	4.2	Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.	Use PAM for all admin accounts.	4	2	2	2	3	6	No		Q4	2021

Instructions: For all risks that are evaluated as unacceptable (typically Risk Scores that are '6' or '9'), describe how you will implement the CIS Safeguard to reduce the risk. In the "Risk Treatment Option" cell, select the value "Reduce" to indicate that you will be planning a risk-reducing safeguard. The CIS Safeguards are provided to you by default, but you may substitute that default text to describe alternative safeguards if you use controls other than what CIS recommends. If you do select an alternative to a CIS Safeguard, do so with advice from a mentor or expert to be sure your alternative meets the objectives of the safeguard.

For the columns "Risk Treatment Safeguard," "Risk Treatment Safeguard Title," and "Risk Treatment Safeguard Description," either accept the CIS Safeguard default values or describe your alternative. Additionally, some enterprises specify how they will implement or operate the Safeguard by using the column "Our Planned Implementation." This might be phrased as a policy statement, such as "The annual application review process will check for upcoming version deprecations. Applications will be updated within the following year." Such phrasing may help convert your risk analysis into a practical instruction, or a risk-based clause for your policies. Finally, state the degree of maturity you expect to achieve with the Safeguard in the "Risk Treatment Safeguard Maturity Score" cell. The automated cells will populate based on your input.

If your Impact Criteria includes Cost Impact entries, you should also add an amount for the expected Safeguard cost in the "Risk Treatment Safeguard Cost" cell. *Enter only one financial cost per solution*. Even if you repeat your Safeguard in multiple rows (as is demonstrated in the example above), the cost should only appear once to prevent recounting in the "Impact to Financial Objectives" cell to the right of the Risk Register.

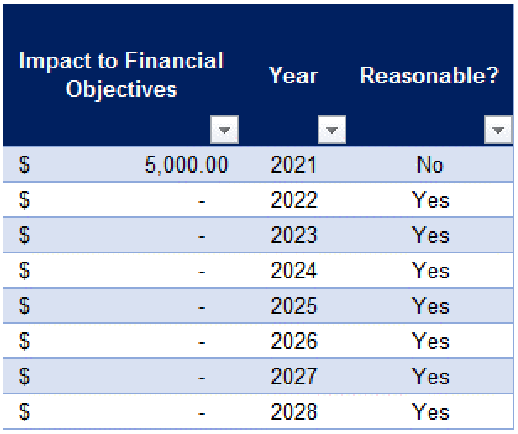
Add the quarter and year you expect to implement the Risk Treatment Safeguard in the "Implementation Quarter" and "Implementation Year" columns. The "Implementation Year" column will run a sum of Risk Treatment Safeguard costs in the "Impact to Financial Objectives" table to the right of the Risk Register (shown below in Figure 11). This table will run a test to determine whether Risk Treatment Safeguards are Reasonable, given the Cost Objectives you defined.

Explanation: Your Risk Treatment Safeguard Risk Score is calculated the same way your Risk Score was calculated in the "Risk Register: Risk Analysis" section, but by pairing the Asset Class with the Risk Treatment Safeguard Expectancy Score and the highest Risk Treatment Safeguard Impact Scores. The final column conducts a test to determine whether your Safeguard is "Reasonable and Acceptable."

Examples: Examples are shown above in Figure 10.

Alternatives: None.

FIGURE 12. Impact to Financial Objectives Table



Impact to Financial Objectives	Year	Reasonable?
$ 5,000.00	2021	No
$ -	2022	Yes
$ -	2023	Yes
$ -	2024	Yes
$ -	2025	Yes
$ -	2026	Yes
$ -	2027	Yes
$ -	2028	Yes

Summary

CIS RAM provides a model of cybersecurity risk analysis that helps enterprises combine the interests of business, legal and regulatory authorities, and information security practitioners. This model provides a basis for consensus by providing equal attention and care to the interests of all parties that may be impacted by risk.

Enterprises that use CIS RAM can then develop a plan and expectations for securing an environment reasonably, even if the CIS Controls are not comprehensively implemented to all information assets.

Recommended Next Steps

CIS RAM users should, as a next step, read other documents in the CIS RAM family to understand how to model threats, estimate expectancies and impacts, use qualitative and quantitative methods, and align CIS RAM with other risk assessment methods they may already use.

The full CIS RAM family of documents provides many examples, exercises, and background material to help become familiar with the reasoning and processes behind the method. As CIS RAM users become practitioners, they will be asked to explain why CIS RAM is an appropriate risk assessment method. CIS RAM practitioners should be able to address the business, legal, and regulatory principles that support the method, so they assure interested parties that their interests are being fairly addressed.

APPENDIX A

Maturity Scores

The CIS RAM for IG1 Maturity Scores are defined differently from other maturity models in that they focus on how reliably a control will protect against security incidents. Other maturity models blend the concepts of formal implementation, documentation, and automation.
This maturity model helps the enterprise estimate the Expectancy of security incidents by comparing the reliability of controls against the commonality of threats that the controls would prevent.

MATURITY SCORE	
1	Safeguard is not implemented or is inconsistently implemented.
2	Safeguard is implemented fully on some assets or partially on all assets.
3	Safeguard is implemented on all assets.
4	Safeguard is tested and inconsistencies are corrected.
5	Safeguard has mechanisms that ensure consistent implementation over time.

While estimating maturity of a control, ask how an independent assessor would answer the question. Do they see the control consistently applied on all assets, but tests are not conducted? Then, the Maturity Score is '3.' Are tests conducted, but not all flaws are corrected? Then, a '4' has not been achieved.

APPENDIX B

Expectancy Scores

The CIS RAM for IG1 Risk Register automatically arrives at a Expectancy Score by comparing the commonality of reported Asset Classes to the maturity of your Safeguards that prevent those Asset Classes.

In this way, CIS RAM for IG1 does not think of Expectancy in terms of the probability that an attack will occur. Expectancy in this risk framework helps you consider the most likely (and least likely) causes for attacks that may occur. Much like wearing a seat belt or exercising, we take precautions against the most likely causes of harm without having to predict when accidents or illness will occur.

Expectancy in CIS RAM ranks the expected commonality of Asset Classes in your environment and uses the following model:

EXPECTANCY SCORE	DEFINITION
1	The risk is not plausible in this environment.
2	This risk should be expected to cause a security incident at some time.
3	We should expect this to happen soon, if it has not already occurred.

The IG1 Workbook contains a table (VCDB Index Weight Table) in the Lookup Tables tab that associates your selected Maturity Score with a VCDB Index to establish the Expectancy Score. The VCDB Index Weight Table enforces a rule that the Expectancy of a risk is driven by the relationship between a Safeguard's capabilities and the commonality of the threat that the Safeguard is designed to prevent. Threats that appear more frequently in the VCDB must be paired with Safeguards with higher Maturity Scores to drive the Expectancy Score down. Conversely, the lower the Maturity Score, the higher the Expectancy Score.

CIS RAM's use of VCDB data is not meant to be predictive, nor is it meant to hold up to the rigors of probability modeling. CIS RAM simply guides the user to expect to see common threats more frequently, and less-common threats less frequently.

APPENDIX C

Importing CSAT Scores into CIS RAM

For users of the CIS-Hosted Controls Self Assessment Tool (CSAT) or CIS CSAT Pro, instructions on how to import CSAT Scores into CIS RAM appear below. Specific examples and additional guidance can be found in the CIS RAM for IG1 Workbook.

CIS CSAT Pro: Steps to Export Data to Import into CIS RAM IG1 Workbook

Note: Please ensure that your enterprise's method for scoring Safeguards in CSAT Pro aligns closely enough with the CIS RAM Maturity Scores, as defined here.

1 In CIS CSAT Pro, filter on IG1 and Export Filtered CSV.

   a Go to the Assessment Summary page for the assessment of interest (this is reachable from the Assessment Summary tab at the top of the Assessment Dashboard for that assessment).

   b Click the Filter button.

   c Select "IG-1" for the Implementation Group filter and click Search.

   d Click the "Export Filtered CSV" button to export the report.

2 Copy your scores from the exported CSAT Pro CSV file to the CIS RAM for IG1 Workbook.

   a In the CSAT Pro CSV file, copy the contents of column E (labeled "Sub-Control[3] Score") excluding the heading row.

   b Go to the "CIS CSAT Pro" tab in the CIS RAM for IG1 Workbook.

   c Find the appropriate section in the "CIS CSAT Pro" tab based on which CIS Controls version you are using (either CSAT Pro for CIS Controls v7.1 or CSAT Pro for CIS Controls v8.0).

   d Paste the copied data into the appropriate section of the "CIS CSAT Pro" tab.

   e For instance, if you are using Controls v7.1, you might copy cells E2 to E44 from the CSAT Pro CSV to C5 to C47 in the "CIS CSAT Pro" tab of the CIS RAM for IG1 Workbook.

3 Note: Adjustments may need to be made based on your scoring from CSAT to CIS RAM.

4 Once scores are final, copy the scores in the "CIS RAM Maturity Score Final" column into the "Safeguard Maturity Score" column of the appropriate CIS RAM tab – "Risk Register 7.1 for IG1" for v7.1 of the CIS Controls or "Risk Register 8 for IG1" for v8 of the CIS Controls.

   a Right-click to copy and "Paste Special" as "Values" (e.g., 1,2,3).

   b Note: Values of 'N' and 'DIV/0!' may copy over from the "CIS CSAT Pro" and "CIS-Hosted CSAT" tabs, if present. If copied, these values can be deleted from the "Safeguard Maturity Score" cell and will not affect the functionality of the CIS RAM Risk Register.

CIS-Hosted CSAT: Steps to Export Data to Import into CIS RAM IG1 Workbook

Note: This method will average the four scoring categories in CIS-Hosted CSAT for each Safeguard and aligns those averages with the CIS RAM Maturity Scores. Please review the CIS RAM Maturity Scores, as defined here, to ensure this method aligns closely enough for your enterprise's scoring practices.

5 In CIS-Hosted CSAT, filter on IG1 and export the filtered Safeguards.

[3] "Safeguards" were known as "Sub-Controls" prior to Version 8 of the CIS Controls.

a Go to the All Controls page for the assessment of interest (this is reachable from the All Controls link on the menu on the left under "Current Assessment").

b Click the Filter button.

c Select "Group 1" for the Implementation Group filter and click Filter.

d Check to see if any of these Safeguards are in the blue (Not Assessed) state. You can see this in the "#" column – there will be a colored circle in each row by the Safeguard number. Any Safeguards that have a blue circle there will not export; if you have any blue Safeguards and you want to continue these steps, one way to get them out of the blue state is to:

i Select the checkbox next to each blue Safeguard.

ii Select "Un-Assign the control" from the Bulk Action option dropdown and click the "Save" button next to the dropdown. Please note: If any of the selected Safeguards were assigned, this will remove the assignee and the due date.

e Click the Download Report button to export the report.

6 Copy your scores from the exported CIS-Hosted CSAT XLSX file to the CIS RAM IG1 Workbook.

a In the CIS-Hosted CSAT XLSX file, copy the contents of columns E through H (labeled Policy Defined, Control Implemented, Control Automated, and Control Reported) excluding the heading row.

b Go to the "CIS-Hosted CSAT" tab in the CIS RAM for IG1 Workbook.

c Find the appropriate section in the "CIS-Hosted CSAT" tab based on which CIS Controls version you are using (either CIS-Hosted CSAT for CIS Controls v7.1 or CIS-Hosted CSAT for CIS Controls v8.0).

d Paste the copied data into the appropriate section of the "CIS-Hosted CSAT" tab.

e For instance, if you are using Controls v7.1, you might copy the cells from E2:E44 over to H2:H44 from the CIS-Hosted CSAT XLSX file, select cell C14 in the "CIS-Hosted CSAT" tab in the CIS RAM for IG1 Workbook and paste them there.

7 Note: Adjustments may need to be made based on your scoring from CSAT to CIS RAM.

8 Once scores are final, copy the scores in the "CIS RAM Maturity Score Final" column into the "Safeguard Maturity Score" column of the appropriate CIS RAM tab – "Risk Register 7.1 for IG1" for v7.1 of the CIS Controls or "Risk Register 8 for IG1" for v8 of the CIS Controls.

a Right-click to copy and "Paste Special" as "Values" (e.g., 1,2,3).

b Note: Values of 'N' and 'DIV/0!' may copy over from the "CIS CSAT Pro" and "CIS-Hosted CSAT" tabs, if present. If copied, these values can be deleted from the "Safeguard Maturity Score" cell and will not affect the functionality of the CIS RAM Risk Register.

APPENDIX D

Customizing the Workbook

The CIS RAM for IG1 Workbook protects most cells in the Risk Register and lookup tables to prevent users from accidentally changing the formulas and lookups that automate the risk analysis and make it simple.

If users are confident in their use of Microsoft® Excel® and wish to modify values, such as Risk Acceptance Criteria, they may “unprotect” the document by going to the “Review” tab in the Excel menu and selecting the “Unprotect sheet” button. However, guidance for maintenance of the workbook, formulas, lookups, and protected cells is beyond the scope of this document.

APPENDIX E:

How CIS RAM for IG1 Supports Standards and the Law

Laws, regulations, and information security standards all consider the need to balance security against an enterprise's purpose and its objectives and require risk assessments to find and document that balance. The risk assessment method described here provides a basis for communicating cybersecurity risk among security professionals, business management, legal authorities, and regulators using a common language that is meaningful to all parties.

CIS RAM conforms to and supplements established information security risk assessment standards and methods, such as NIST Special Publications 800-30[4], ISO 27005[5], and RISK Information Technology (IT)[6]. By conforming to these standards and methods, CIS RAM ensures that the user will conduct risk assessments in conformance to established (or authoritative) practices. By supplementing these methods, CIS RAM helps its users evaluate risks and Safeguards using the concept of "due care" and "reasonable safeguards" that the legal community and regulators use to determine whether an enterprise acts as a "reasonable person."

In addition, CIS RAM supports the cost-benefit analysis definitions for reasonableness used by U.S.-based regulators[7], litigators[8], and the legal community in general[9].

[4] NIST Special Publication 800-30 Rev. 1 provided by the National Institute of Standards and Technology

[5] ISO/IEC 27005:2011 provided by the International Organization for Standardization

[6] RISK IT Framework provided by ISACA

[7] Executive Order 12866, 1993

[8] The Learned Hand Rule. United States v. Carroll Towing Co. – 159 F.2d 169

[9] The Sedona Conference, Commentary on a Reasonable Security Test, 22 SEDONA CONF. J. 345

Helpful Resources

CIS (Center for Internet Security)

The Center for Internet Security, Inc. (CIS) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously refine these standards to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial (SLTT) government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

HALOCK Security Labs

Established in 1996, HALOCK Security Labs is an information security professional services firm based in Schaumburg, Illinois. For more than 20 years, HALOCK® has provided Purpose Driven Security® services to help enterprises achieve their Mission and Objectives through sound security practices. HALOCK uses their deep background in the legal and regulatory landscape, security technologies and standards, business governance, and data analytics to provide evidence-based security analysis and guidance to their clients. (www.halock.com) For guidance in implementing the CIS RAM: (www.halock.com/cisram)

DoCRA Council

The DoCRA Council maintains and educates risk practitioners on the use of the Duty of Care Risk Analysis (DoCRA) Standard that CIS RAM is based on. While DoCRA is applicable to evaluation of information security risk, it is designed to be generally applicable to other areas of business that must manage risk and regulatory compliance. (www.docra.org)

International Organization for Standardization (ISO®)

ISO provides to information security professionals a set of standards and certifications for managing information security through an information security management system ("ISMS"). ISO 27001 is a risk-based method for organizations to secure information assets so that they support the business context, and requirements of interested parties. ISO 27005 is an information security risk assessment process that aligns with CIS RAM. (https://www.iso.org/isoiec-27001-information-security.html)

National Institute of Standards and Technology (NIST®)

NIST provides a series of standards and recommendations for securing systems and information, known as "Special Publications" in the SP 800 series. NIST SP 800-30 provides guidance for assessing information security risk. NIST SP 800-37 and NIST SP 800-39 each present an approach for managing information security risk within an organization. While these approaches are designed to address federal information systems and reference roles within federal agencies, their principles and practices are generally applicable to many organizations. (https://csrc.nist.gov/publications/sp)

NIST also provides the Framework for Improving Critical Infrastructure ("Cybersecurity Framework"). The framework organizes information security controls within a structure that prepares for and responds to cybersecurity incidents. The Cybersecurity Framework aligns its categories and subcategories of controls with those of other control documents, including the CIS Critical Security Controls. (https://www.nist.gov/framework)

Information Systems Audit and Control Association (ISACA®)

Well known for their IT assurance standards and certifications, ISACA provides an information security risk management framework known as Risk IT. Risk IT bases its risk analysis method on ISO 31000, and adds risk governance and response to the analysis to provide a lifecycle of IT risk management. (https://www.isaca.org/resources/it-risk)

All references to tools or other products in this document are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Contact Information

CIS

31 Tech Valley Drive
East Greenbush, NY 12061
518.266.3460
controlsinfo@cisecurity.org

HALOCK Security Labs

1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847.221.0200
cisram@halock.com

Center for Internet Security®

CIS Controls

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Critical Security Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. election offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity