CIS Center for Internet Security®

CIS Controls

CIS Risk Assessment Method (RAM)

Version 2.1

Implementation Group 2 (IG2)
Workbook Edition

Revised August 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

Valecia Stocchetti, Sr. Cybersecurity Engineer, CIS
Robin Regnier, Controls Coordinator, CIS
Alan B. Watkins, Independent Consultant
Brent Ruby, Sr. Security Program Manager, Walker & Dunlop
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Michael Petrov, CEO, Digital Edge

Contents

Foreword

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 IT risk reduction, some Safeguards 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 2 (CIS RAM for IG2) is intended for enterprises using the IG1 and IG2 sets of CIS Safeguards. CIS RAM for IG2 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 IG2 is written as a user manual for the Workbook, a set of Microsoft® Excel worksheets provided by CIS as templates for 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 on determining how well protected the enterprise's 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 in methodology, using either quantitative analysis (purely numerical representations of risk) or qualitative analysis (ranked value statements). CIS RAM for IG2 focuses on a set of CIS Safeguards within the CIS Controls, and combines both 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 IG2 as Part of the CIS RAM Family of Documents

CIS RAM for IG2 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.
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 Criteria	The rules used to estimate Expectancy Scores.
Expectancy Score	The score, ranked from '1' to '5' in CIS RAM 2.1 for IG2, 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 '5' in CIS RAM for IG2.
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
IG2	Implementation Group 2
ISO	International Organization for Standardization
IT	Information Technology
MFA	Multi-factor Authentication
NIST	National Institute of Standards and Technology
VCDB	VERIS Community Database
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 IG2

Goals

CIS RAM for IG2 was designed to help you conduct a risk assessment if your enterprise has expertise in developing, managing, and configuring systems, applications, and networks. IG2 enterprises are able to understand how asset classes are configured and managed, and are able to evaluate risks associated with separate asset classes, rather than the enterprise as a whole. This document can best be used as a manual for its accompanying risk assessment Workbook ("CIS RAM 2.1 for IG2 Workbook"). The intent of CIS RAM for IG2 is to help enterprises conduct a competent, data-driven risk assessment while minimizing any guesswork in their risk estimations.

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 IG2 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 IG2 is simpler than an assessment that models risks primarily by threat models, it will demonstrate that your enterprise has implemented reasonable Safeguards (or has a plan to implement reasonable Safeguards) that are based on configurations of assets, and that should acceptably reduce risks for potentially harmed parties.

Risk Assessment Process

CIS RAM for IG2 assists IG2 enterprises by significantly automating risk estimations and threat models. It reduces the complexity of risk analysis by providing the following:

- A simple format for stating an enterprise's Impact Criteria and range of magnitudes of Impact that you or others may suffer
- Guidance for stating your enterprise's Risk Acceptance Criteria
- A fixed definition for Expectancy Criteria
- A simple Risk Register
- 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 IG2 narrows your enterprise's risk assessment focus on how well your implementation of CIS Safeguards reduces 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 enterprises make data-driven risk decisions, but may not result in a comprehensive risk assessment that models all foreseeable threats in your environment.

CIS RAM for IG2 risk assessments involve the following activities:

Activity	Description
Developing the Impact Criteria	The risk assessor briefly defines their enterprise's Mission, Operational Objectives, Financial Objectives, and Obligations. The risk assessor then defines their Impact Scores and defines their level of Acceptable Risk. Expectancy Score definitions are provided by default.
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 IG2 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 IG2 Instructions

The CIS RAM for IG2 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 that you 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.

Impact Criteria Survey

Purpose and Use

The **Impact Criteria Survey** helps you state in plain language how you will estimate the magnitudes of harm that may result from a security incident. This is the first important step you will take to implement the DoCRA Standard's three principles. In order to evaluate risk to yourself and others you must define the kinds of harm that you and others might suffer when a cybersecurity incident occurs.

However, defining Impact Criteria is not necessarily intuitive, so CIS RAM for IG2 provides the Impact Criteria Survey to help you accomplish this.

You will start this process by providing responses to the prompts for the Impact Areas — "Mission," "Operational Objectives," "Financial Objectives," and "Obligations." Your responses should be simple, and they should be recognizable within your enterprise.

You will then either accept default responses for **Impact Magnitude** definitions, or you will provide responses that your enterprise would recognize as "Negligible," "Acceptable," "Unacceptable," "High," and "Catastrophic" results.

Some enterprises may believe that Impact Criteria based on business and operational concerns is beyond what cybersecurity is interested in. CIS RAM asserts that cybersecurity matters because of what security incidents can harm, so Mission, Objectives, and Obligations are very useful categories for considering harms.

CIS RAM includes Mission as an Impact Area so you keep in mind that neither security incidents nor overly burdensome Safeguards should compromise the reason why you engage in the risk to begin with. Your enterprise creates value, benefit, and (what lawyers call) "utility" which should be conscientiously protected.

The **Operational Objectives Impact Area** ensures that your enterprise can protect itself against the harms that may come from cybersecurity incidents or overly burdensome Safeguards. This is generally a non-quantitative value.

The **Financial Objectives Impact Area** will help your enterprise set monetary limits to risks and Safeguard costs that you can tolerate to operate a single Safeguard or apply to an annual budget.

And finally, the **Obligations Impact Area** reminds your enterprise that you must also protect people other than yourselves who may be harmed by a security incident, or from the unintended consequences of a Safeguard.

We consider these Impacts because of why we do cybersecurity—to protect ourselves and others.

Defining Impact Areas

As your first step in implementing the three principles, you will first define what your enterprise is trying to protect from cybersecurity incidents. Executives who take responsibility for cybersecurity risk and who provide resources and prioritization for reducing cybersecurity risk should participate in defining the Impact Areas, or at least review and accept them when they have been defined.

The Mission prompt (in Figure 1) is asking you to concisely describe the benefit your enterprise provides to others. This is important for two reasons. One is that you want to protect that benefit from cybersecurity incidents, but the other is that a Safeguard that you implement to reduce the risk should also not compromise the benefit. By stating your enterprise's Mission, you are ensuring that this concern will be evaluated in each risk analysis.

In the example below, a manufacturer of custom "widgets" states that their mission is to produce just-in-time, custom widgets that meet demanding requirements, and quickly. If they produce those widgets slowly or poorly, then the risk they pose to their customers by handling their intellectual property (widget design specifications) would be less worthwhile.

Figure 1. Mission prompt and example response

	Prompt	Response
Mission	*How would you concisely describe the benefit that your enterprise provides your customers, clients, constituents, or the public? This is why they engage in this risk with you.*	Reliably produce just-in-time, custom widgets that meet demanding resiliency and design specifications, and within market-leading turnaround times.

The Operational Objectives prompt (in Figure 2) is asking you a qualitative (not quantitative) question about what your enterprise must achieve for their own benefit. Growth, profitability, reputation, and maintaining a certain market position are common Operational Objectives for for-profit enterprises. Nonprofit enterprises may have goals for membership growth, investments into the mission, maintaining key leadership, or obtaining and maintaining key partnerships.

In the example below, the manufacturer says that it wants to maintain its market position as the best manufacturer in their field. They will want to protect their reputation both in terms of a cybersecurity incident and cybersecurity Safeguards that could conceivably interfere with their efficiency, speed, and responsiveness to their customers' just-in-time requests.

Your enterprise may consider the Operational Objectives and Financial Objectives to be redundant. In other words, if your Operational Objective is to be profitable, then there may be no need to state Operational Objectives and Financial Objectives separately. Therefore, you should consider the Operational Objectives Impact Area to be optional if you are defining the Financial Objectives Impact Area.

Figure 2. Operational Objectives prompt and example response

	Prompt	Response
Operational Objectives	*What business or organizational goals does the enterprise attempt to achieve?*	To maintain our market position as the best custom widgets manufacturer.

The Financial Objectives prompt (in Figure 3) asks you to state a financial goal that your enterprise operates to. Profitability and profitable growth are common Financial Objectives. Banks and investment enterprises may strive for a planned return-on-assets or growth in assets. Nonprofits may target growth in their foundation, maintaining a balanced budget, or increasing membership revenue.

In the example below, the manufacturer states its Financial Objectives as achieving their profitability goals according to their plan. They will want to protect their profitable performance from both a cybersecurity incident, and from over-investing in too many Safeguards in too short a period of time.

Your enterprise may or may not decide to include quantified Financial Objectives in your risk analysis. The values provided in this Impact Area are useful for evaluating risks and Safeguards, but also for evaluating the reasonableness of annual budgets. However, you should consider this Impact Area optional in your risk analysis if you have stated your Operational Objectives.

Figure 3. Financial Objectives prompt and example response

	Prompt	Response
Financial Objectives	*What are the unexpected cost outlays that your enterprise could or could not tolerate?*	To achieve our profit goals each year.

The Obligations prompt (in Figure 4) asks you to define the harm that others may suffer if a cybersecurity incident were to occur. Surprisingly, this Impact Area is often overlooked in cybersecurity risk analysis. While some state that regulatory fines or lawsuits represent the impact to others, they do not. They represent harm to the enterprise's Objectives since the enterprise will pay those fines and settlements.

In the example below, the manufacturer understands that if their customers' intellectual property (their widget design criteria) is exposed in a cybersecurity incident, their customers may suffer competitively, they may lose market advantage and opportunity, and they may need to re-invest on their product designs. All of these would be losses that the customers would suffer, and that the manufacturer intends to prevent.

Figure 4. Obligations prompt and example response

	Prompt	Response
Obligations	*What harm may foreseeably come to others as a result of a cybersecurity incident?*	To protect our customers from harm due to loss of their intellectual property.

Again, developing definitions for Impact Areas is not intuitive, so Appendix A provides you with further guidance for defining your Impact Areas.

Defining Impact Magnitudes

Now that each Impact Area is defined, you should either review and accept the default definitions for Impact Magnitudes, or (optimally) define those Impact Magnitudes as they specifically apply to your enterprise.

Since enterprises can best estimate, plan for, and accept risk when it is meaningful to them, CIS RAM recommends that your enterprise define your own Impact Magnitudes rather than accept the default definitions provided here. As you will see, Impact Magnitudes describe observable outcomes that your enterprise may find Negligible, Acceptable, Unacceptable, High, or Catastrophic. When your Impact Magnitude scores reference outcomes that the enterprise knows to ignore or avoid, you will improve your consistency in impact estimations.

Executives who take responsibility for cybersecurity risk and who provide resources and prioritization for reducing cybersecurity risk should participate in defining the Impact Magnitudes, or at least review and accept them when they have been defined.

For enterprises that are not up to the challenge of defining your own Impact Magnitudes at the outset, CIS RAM for IG2 provides default definitions that may be sufficient, but they do not describe observable outcomes. If your enterprise uses these definitions, be aware that your impact estimates may be less consistent with each other. Each enterprise that starts with the default Impact Magnitude definitions should customize those definitions when executives require more clarity on the meaning of risk analysis, or when personnel involved in the risk management program disagree about impact estimates.

Impact Magnitudes range from "Negligible" to "Catastrophic." The meanings of these magnitudes are:

- **Negligible:** If any impact were to occur, it would not be in evidence, or it would be so low that it could safely be ignored.
- **Acceptable:** While this impact would be in evidence and may not be ignored, it would not require repair, correction, or compensation. The normal course of business may correct the issue.
- **Unacceptable:** The impact would require repair, correction, or compensation that could be accomplished with less than a major effort or investment.
- **High:** The impact would require significant repair, correction, or compensation and may actually lead to a catastrophic result if it is not addressed.
- **Catastrophic:** The impact would lead to an ultimate and irreparable loss.

Note that some risk analysts leave out negligible impacts (or '0' impacts when quantified risk analysis is used) in their risk assessments. These risk analysts argue that a negligible impact means that there is no risk worth considering. However, in cybersecurity, threats, threat vectors, and asset values change fairly rapidly. You will want to show how risk that was once thought to be negligible may become intolerably high. When you revisit your risk assessment (say, on an annual schedule) you can reconsider whether impacts you recently regarded as negligible have become more concerning to you or others.

Similarly, some risk analysts believe that risk assessments should only record unacceptable risks. They think of risk assessments as their list of things that need correcting, so there is little use in recording acceptable risks. However, keep in mind that regulations and frameworks either require or expect your enterprise to use certain safeguards. When you evaluate some safeguards as posing an acceptable risk, you will want to record that. This aids in your ability to review the risk posed by that safeguard in your subsequent risk assessment, and it records why you believed a safeguard was reasonable if your safeguards are scrutinized after an incident occurs.

Impact Magnitude definitions are most helpful when they are meaningful. Your definitions will be meaningful when they meet the following criteria:

- **The definitions describe observable outcomes:** If a definition describes a factual condition that can be objectively observed or measured, then the enterprise can agree when the Impact Magnitude has occurred. Examples of this include, "More than one customer would complain about the same issue," "Our customer surveys would rate us below 'Satisfied'," and "Our graduation rate would achieve our goal." They are all examples of observable outcomes. However, "Low," "We could do better," and color codes such as "Green/Yellow/Red" are not observable outcomes and would make it difficult for people to agree when those impacts have occurred.

- **The enterprise manages to those observable outcomes:** Enterprises generally work toward desired outcomes. Sometimes enterprises use specific metrics to manage to those outcomes. For some enterprises, however, defining CIS RAM Impact Magnitudes may be the first time they set explicit levels of tolerance for achieving goals or avoiding harms. If an enterprise knows its objectives succeed when they achieve a certain percentage of growth or profit, or their obligations fail if their customers suffer from a foreseeable harm, or a mission is no longer achievable when a certain condition is met, then they have the basis for agreement on what outcomes they should manage to. Impact Magnitudes should be collaboratively defined with executive risk owners, management, and personnel who are responsible for cybersecurity. This is the enterprise's best opportunity to establish definitions that they already manage to.

As you might guess by these criteria, the risk assessment will set out scenarios and will ask risk assessment participants to consider what the result of a scenario may be, and to determine whether that result merits a Negligible, Acceptable, Unacceptable, High, or Catastrophic rating.

If the default definitions would not be meaningful for your enterprise, you should define your own Impact Magnitudes. That exercise should be conducted with executives who make decisions about cybersecurity investments and priorities to ensure that the resulting definitions are meaningful.

Responding to Mission Impact Magnitude Prompts

The prompts and default responses to the Mission Impact Magnitudes are provided below (Figure 5). If you decide to accept the default responses, you should still review the default responses to become familiar with them. You will be using these default responses during risk analysis.

Note the default responses and how they align with the Impact Magnitude definitions. Executives in your enterprise may find that the default responses are sufficient to communicate the degrees of unacceptable impacts they would manage against. Review these responses and determine whether your enterprise would make meaningful risk estimates and decisions using the default responses.

Figure 5. Mission Impact Magnitude prompts and default responses

Impact Magnitude	Prompt	Response
Negligible	*What observable evidence would you have that your mission - as you defined it above - would be unaffected?*	The mission would remain intact.
Acceptable	*What observable evidence would you have that your mission would be compromised, but it would not require correction?*	This mission would not be perfectly achieved, but could be recovered within normal operations.
Unacceptable	*What observable evidence would you have that your mission would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?*	This mission would not be achieved, and would require short-term, unplanned efforts, resources, or investments to recover.
High	*What observable evidence would you have that your mission would be compromised so badly that extraordinary efforts would be required to restore it?*	This mission would not be achieved. If significant, unplanned efforts, resources, or investments are not made, the mission may not ever be achievable.
Catastrophic	*What observable evidence would you have that your mission would be compromised so badly that it could not be achieved?*	The mission would not be achievable.

If you have decided to define your own Impact Magnitudes, then observe the criteria provided below (Figure 6). In the provided example, the manufacturer we referred to earlier has followed the prompts in the Impact Criteria Survey. As a result, they have customized their Impact Magnitude definitions.

Figure 6. Mission Impact Magnitude prompts and custom responses

Impact Magnitude	Prompt	Response
Negligible	*What observable evidence would you have that your mission - as you defined it above - would be unaffected?*	All orders would be produced within specifications and on time and without unplanned effort.
Acceptable	*What observable evidence would you have that your mission would be compromised, but it would not require correction?*	All orders would be produced within specifications and on time, but some may require unplanned effort to stay within tolerance metrics.
Unacceptable	*What observable evidence would you have that your mission would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?*	Few orders each quarter (outside of our tolerance metrics) may miss targets, but could be corrected with adjustments or discounts.
High	*What observable evidence would you have that your mission would be compromised so badly that extraordinary efforts would be required to restore it?*	We would repeatedly miss targets outside of tolerance metrics, requiring regular adjustments or discounts per quarter, or would require significant re-investment to operate regularly within our tolerance metrics.
Catastrophic	*What observable evidence would you have that your mission would be compromised so badly that it could not be achieved?*	We could not meet our mission.

In this example, we see that the manufacturer uses "tolerance metrics" in their normal course of business to determine whether they are meeting their Mission. Tolerance metrics are often used in manufacturing to describe how far from perfect work product (or safety, or efficiency, etc.) may be and still be considered successful. Since this enterprise already has a way to measure their Mission, they simply use their Mission's criteria while responding to the Impact Criteria Survey.

- **Defining Negligible Mission Impact Magnitudes:** They know they will not pay attention to cybersecurity incidents (or any problems) if they result in all orders going out on time, within specifications, and without unplanned inefficiencies. This would indicate a Negligible result. For example, if a salesperson lost their laptop, the impact to their Obligations to protect customer intellectual property may be Unacceptable or High, but the impact to the Mission could still be Negligible.
- **Defining Acceptable Mission Impact Magnitudes:** The manufacturer also knows that some conditions will cause inefficiencies or issues that can be corrected while still allowing the company to meet production goals. Imagine a threat or a Safeguard at a manufacturer that creates inefficiencies, but would not delay orders. For example, a very zealous security team could require all manufacturing personnel to log into their control systems using multi-factor authentication (MFA). This would likely cause inefficiencies, especially if personnel occasionally lose their MFA device. However, the manufacturer could recover from the resulting slowdowns if the personnel have good technical support to help them log in quickly when needed.
- **Defining Unacceptable Mission Impact Magnitudes:** Some conditions could cause Unacceptable impacts to production goals, but that could be restored after unplanned cost or effort that could be recovered without significantly changing the business. Using the MFA example above, imagine that the technical support team is generally not responsive to manufacturing personnel who use MFA to log into their control systems. If MFA devices are occasionally lost, then the manufacturer may too-often miss their production goals and the manufacturer would find this Unacceptable, but likely not High as we are about to see.

- **Defining High Mission Impact Magnitudes:** Some impacts may be so severe that they require the enterprise to change — even temporarily — to recover from them. This manufacturer realizes that repeated failures to meet delivery targets means that they are not achieving their Mission, so something significant would have to change in order to make that happen. Imagine if their resource planning software provider was regularly hacked. They would need to find a new provider. Or imagine a Safeguard that was so disruptive — for example, re-imaging control device firmware before every job — that production timelines and commitments would have to change. Those could be High Impact Magnitudes.
- **Defining Catastrophic Mission Impact Magnitudes:** Some impacts could be so severe that they prevent the Impact Area from being possible. The manufacturer simply states that they could not meet their Mission as their definition for that Impact Magnitude. If they rely on non-secure technologies to meet their unique Mission, they may find that a total loss of those technologies — and a lack of alternatives — may make their Mission impossible to achieve.

As you can see, risk analysis is very dependent on the environment and what the enterprise cares to measure. By understanding their business objectives and by considering the degrees of tolerability they would accept, not accept, or could recover from, the example manufacturer has developed meaningful Impact Magnitude definitions for their Mission.

Responding to Operational Objectives Impact Magnitude Prompts

The prompts and default responses for the Operational Objectives Impact Magnitudes are shown below (Figure 7). If you decide to accept the default responses you should still review them so you are familiar with them.

Figure 7. Operational Objectives Impact Magnitude prompts and default responses

Impact Magnitude	Prompt	Response
Negligible	*What observable evidence would you have that your operational objectives - as you defined them above - would be unaffected?*	Growth plan would be intact.
Acceptable	*What observable evidence would you have that your operational objectives would be compromised, but it would not require correction?*	Growth plan would be off target, but within variance.
Unacceptable	*What observable evidence would you have that your operational objectives would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?*	Growth plan would be out of variance, but can be recovered within a fiscal year.
High	*What observable evidence would you have that your operational objectives would be compromised so badly that extraordinary efforts would be required to restore them?*	Growth plan would be out of variance, and may require multiple years to correct.
Catastrophic	*What observable evidence would you have that your operational objectives would be compromised so badly that they could not be achieved?*	We would not be able to grow.

If you define your own Operational Objectives Impact Magnitudes, you should consider metrics that your enterprise uses to determine whether they reach their operational goals. The example manufacturer defined this Impact Area as, "To maintain our market position as the best custom widgets manufacturer." To measure their achievement of that objective, they would need to observe evidence of whether they have achieved it.

Impact Magnitude	Prompt	Response
Negligible	*What observable evidence would you have that your operational objectives - as you defined them above - would be unaffected?*	Ranked as #1 in all categories in annual "Custom Widget World" Magazine poll.
Acceptable	*What observable evidence would you have that your operational objectives would be compromised, but it would not require correction?*	Ranked as #1 in only one category of "Custom Widget World" Magazine poll for only one year.
Unacceptable	*What observable evidence would you have that your operational objectives would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?*	Not ranked #1 in any category of "Custom Widget World" Magazine poll for one year.
High	*What observable evidence would you have that your operational objectives would be compromised so badly that extraordinary efforts would be required to restore them?*	Not ranked in top three in any category of "Custom Widget World" Magazine poll for two years or more.
Catastrophic	*What observable evidence would you have that your operational objectives would be compromised so badly that they could not be achieved?*	Unable to rank well in annual "Custom Widget World" Magazine poll.

Figure 8. Operational Objectives Impact Magnitude prompts and custom responses

In their case, they will rely on an annual industry poll in "Custom Widget World" magazine. In this fictional example, the magazine surveys the marketplace to determine who, among multiple categories, are the "best" manufacturers of custom widgets.

- **Defining Negligible Operational Objective Impact Magnitudes:** In this example, the manufacturer believes that they would normally appear as "Number 1" in all categories in the annual poll. So, if a cybersecurity incident or other condition created a Negligible impact to the Operational Objectives, they would remain at the top of the poll.
- **Defining Acceptable Operational Objective Impact Magnitudes:** The manufacturer knows that they will not always rank as "Number 1" in all categories for reasons beyond their control. If a cybersecurity incident or other condition caused them to rank as "Number 1" for only one category in a single year, that would be fine. A single notable work stoppage or a breach of non-sensitive information may sully their market reputation to a degree that would lead to that result.
- **Defining Unacceptable Operational Objective Impact Magnitudes:** The manufacturer believes that if they were not considered "Number 1" for any categories for a single year, they could recover in a year just by continuing to meet their normal performance goals. Perhaps they have had experience with this scenario, or they believe that a single miss may indicate a temporary problem. Or perhaps they understand that strategic investments sometimes cause the enterprise to perform imperfectly for a short period while they adjust to a new environment or process. These conditions may not seem to be related directly to cybersecurity attacks. However, keep in mind that the enterprise is defining levels of impact it can and cannot tolerate. If some cybersecurity incidents do not cause these Unacceptable impacts, then the incident itself (and the risk) are Acceptable.
- **Defining High Operational Objective Impact Magnitudes:** The manufacturer believes that if they could not be seen by the market as a top-three manufacturer over multiple years, that would indicate the need to make serious changes to the enterprise, but they could recover.
- **Defining Catastrophic Operational Objective Impact Magnitudes:** Finally, their Operational Objective to be the best custom widget manufacturer would obviously not be possible if they could not ever rank well in the annual poll.

There are many ways to measure Operational Objectives and they may include external or internal evidence. Our example demonstrates how easy it is to define these Impact Magnitudes once the enterprise articulates the observable results they will use to define each magnitude.

Responding to Financial Objectives Impact Magnitude Prompts

Since using the Financial Objectives Impact Area is optional and because Financial Objectives are so unique for each enterprise, the Workbook does not provide default values for Financial Objectives Impact Magnitudes.

As with other Impact Areas, each enterprise should consider goals they already manage to so they can define each Financial Objectives Impact Magnitude. By now, our example manufacturer is used to degrees of performance they will tolerate and those they will not. Recall that their definition for their Financial Objectives Impact Area was, "To achieve our profit goals each year." Their goals likely have an explicit line between profitability and loss, but may not distinguish between "Negligible" and "Acceptable," or between "High" and "Catastrophic." The Impact Criteria Survey provides prompts to help make this a simple task.

Figure 9. Financial Objectives Impact Magnitude prompts and custom responses

Impact Magnitude	Prompt	Response
Negligible	*What observable evidence would you have that your financial objectives - as you defined them above - would be unaffected?*	$1,000
Acceptable	*What observable evidence would you have that your financial objectives would be compromised, but it would not require correction?*	$10,000
Unacceptable	*What observable evidence would you have that your financial objectives would be compromised in a way that would require correction, but the correction could be achieved through the normal course of business?*	$500,000
High	*What observable evidence would you have that your financial objectives would be compromised so badly that extraordinary efforts would be required to restore them?*	$5,000,000
Catastrophic	*Leave this blank*	

- **Defining Negligible Financial Objectives Impact Magnitudes:** In this case, the manufacturer has said that they would not pay attention to a problem if it resulted in an unexpected $1,000 impact. Perhaps they know that they normally ignore budget variances that are smaller than that amount. The $1,000 figure is the maximum impact they would suffer and call it Negligible.
- **Defining Acceptable Financial Objectives Impact Magnitudes:** The manufacturer has determined that if they would not invest to prevent an unexpected impact of $10,000 (perhaps they regularly vary in their budgets by that amount each year), then they would accept an unexpected cost of up to that amount. Again, the $10,000 figure represents the maximum unexpected cost they could find Acceptable.
- **Defining Unacceptable Financial Objectives Impact Magnitudes:** If a security incident or a Safeguard creates a financial impact that exceeds $10,000 then it crosses into "Unacceptable" territory. The question for your enterprise is, "What is the ceiling for that Impact Magnitude?" By reading a description of the High Impact Magnitude definition, we get a sense of our upper limit for Unacceptable Impact Magnitudes for Financial Objectives. The manufacturer believes that while over $10,000 would be the floor of the unexpected financial impacts that they would accept, they believe that they could recover from an unexpected loss of $500,000 after a fiscal year. Beyond that, they would need to make significant changes to how they do business (layoffs, new efficiencies, or investments) to recover from that loss. As a result, they state $500,000 as their response to the prompt for Unacceptable.
- **Defining High Financial Objectives Impact Magnitudes:** You should again read the response to the previous prompt as the minimum threshold that puts your Impact Magnitude into High territory. The manufacturer set the minimum threshold for High Impact Magnitudes above $500,000 by making $500,000 the maximum amount for Unacceptable Impact Magnitudes. Once they cross the $500,000 impact amount they are in High territory. This prompt is asking us how high a Financial Objectives Impact Magnitude could be while still allowing us to continue existing or operating. In other words, when would the financial loss put us out of business? The manufacturer sets that limit at $5,000,000.

- **Defining Catastrophic Financial Objectives Impact Magnitudes:** There is no reason to provide a value for Catastrophic Financial Objectives Impact Magnitudes. Once an enterprise crosses the threshold into Catastrophic territory, the sky is the limit as to how much they could suffer.

Responding to Obligations Impact Magnitude Prompts

Obligations Impact Magnitudes remind us that we must protect others, and we must draw some lines between levels of harm we believe others are willing to tolerate. This step requires care and conscience. This step also reminds us of why we are engaged in cybersecurity — not only to protect ourselves from harm, but to protect others from harms that we may allow or cause.

The default Impact Magnitude prompts and responses are provided below (Figure 10). Note that the prompts and the responses both explicitly call out the harm that others may suffer.

Who "others" are, is dependent on the business context. It may be customers, the public, or it may be employees. The default responses are generic enough to include any or all of these populations.

Note also that the default response to "High" shows two possible High Impact Magnitudes—either many others could be harmed in a way that can be corrected, or a few others can be harmed in a way that can only be partially corrected. This default response is meant to help you consider ways in which a High impact may occur.

Figure 10. Obligations Impact Magnitude prompts and default responses

Impact Magnitude	Prompt	Response
Negligible	*Describe a condition where others would not be harmed.*	No harm could foreseeably result.
Acceptable	*Describe a condition where others would not be harmed to a degree that required correction or compensation.*	Any harm that could result would not require correction, repair, or compensation to make the harmed parties "whole."
Unacceptable	*Describe a condition where one or few others would be harmed to a degree that you could correct.*	Correctible harm may occur to one or few others.
High	*Describe a condition where many others would be harmed to a degree that you could correct, or where few others are harmed to a degree that others would always have a small degree of impairment.*	Correctible harm may occur to many others, or harm that can be partially corrected for a few others may occur.
Catastrophic	*Describe a condition where others would be irreparably harmed.*	We would not be able to protect others from any degree of harm.

If you choose to customize the Obligations Impact Magnitudes, first read your Impact Area definition. In the case of the example manufacturer, their Obligations Impact Area definition is, "To protect our customers from harm due to loss of their intellectual property." Your Obligations Impact Magnitude definitions should align with how you define your Obligations, of course, but they should also describe a degree of harm that you believe: 1) are plausible, given the Obligations, and 2) would realistically be understood by potentially harmed parties as Negligible, Acceptable, Unacceptable, High, and Catastrophic.

Defining Obligations Impact Magnitudes appears to be a difficult task, then. How would you (or our example manufacturer) know what levels of harm others would accept, or consider to be catastrophic?

The prompts that are provided in the Impact Criteria Survey should provide you with some helpful guidance. However, consider what regulators or other authorities would judge to be a violation, or a harm that should be corrected. By doing this, your definitions of Acceptable and Unacceptable harm can be based on the rules that society has laid for determining when harm is acceptable or not. You will not need to figure this out on your own.

Figure 11. Obligations Impact Magnitude prompts and custom responses

Impact Magnitude	Prompt	Response
Negligible	*Describe a condition where others would not be harmed.*	No customer would suffer a loss of competitive advantage.
Acceptable	*Describe a condition where others would not be harmed to a degree that required correction or compensation.*	One or few customers may be concerned about potential loss of competitive advantage, but no harm would result.
Unacceptable	*Describe a condition where one or few others would be harmed to a degree that you could correct.*	One or few customers would suffer minor loss of competitive advantage, but they could be made whole within a fiscal year.
High	*Describe a condition where many others would be harmed to a degree that you could correct, or where few others are harmed to a degree that others would always have a small degree of impairment.*	Many customers would suffer minor loss of competitive advantage, or one to few customers would suffer harm that would require significant business investment or planning to recover.
Catastrophic	*Describe a condition where others would be irreparably harmed.*	We would not be able to protect our customers from losses due to intellectual property theft.

- **Defining Negligible Obligations Impact Magnitudes:** The manufacturer is obligated to prevent harm to their customers through the loss of intellectual property. If product designs are stolen and made available to competitors, that could result in a loss of competitive advantage. A Negligible Impact Magnitude would mean that no customer would suffer a loss of competitive advantage.
- **Defining Acceptable Obligations Impact Magnitudes:** The manufacturer next considers what conditions may be more than Negligible, but still would not cause correctible harm to their customers. They know through experience that sometimes security incidents lead to concern even if no harm could foreseeably occur. Examples of this may be the loss of robustly encrypted information. Nobody wants to have information files leak, but the encryption may make the leak harmless. Similarly, a customer list may be exposed revealing the manufacturer's relationship with their customers, but if no foreseeable harm could result, then that may also be Acceptable.
- **Defining Unacceptable Obligations Impact Magnitudes:** For the Unacceptable Impact Magnitude, recall how the Mission and Operational Objectives were defined at this magnitude. In all cases, the manufacturer describes a level of harm that they would consider Unacceptable, and they apply that same level of harm to what they assume their customers would tolerate. Even if a customer disagrees after a breach and complains that their tolerance was different from the manufacturer's tolerance, the manufacturer can demonstrate to their customers, to authorities, and most importantly to their own personnel, that they care for their customers the same way they care for themselves.
- **Defining High Obligations Impact Magnitudes:** Again, see how you have defined High Impact Magnitudes for your Mission and Operational Objectives Impact Areas. They would require you to make significant reinvestment and business changes to recover. Apply that same thinking when considering what a High Impact Magnitude would mean for others you may harm. The manufacturer understands that High Obligations Impact Magnitudes would require their customers to make significant changes in the business to recover.
- **Defining Catastrophic Obligations Impact Magnitudes:** Here you must think of the worst kind of harm you may cause or allow through a cybersecurity incident, or even a Safeguard that is overzealous. Some enterprises may cause physical harm or death, and some even death to large populations. Others may just cause inconvenience, but to millions of people. In this example, the manufacturer considers that their worst scenario would be to cause loss of competitive advantage to all of their customers.

Enterprise Parameters

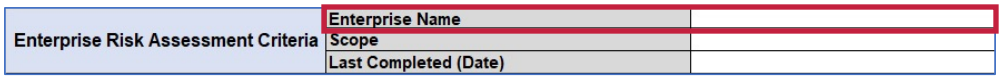
Your Enterprise Parameters tab collects your Risk Assessment Criteria. This tab stores the values that your risk assessment will use to estimate the impacts that the Impact Criteria Survey helped you define. It will contain criteria for evaluating Risk Expectancy, will help you establish your Risk Assessment Criteria, and will help you establish inherent Impact Values that can help automate your risk assessment.

Risk Register Record Header

Since the Risk Register is useful as a record for cybersecurity risk management, 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.

Enterprise Name

Figure 12. Enterprise Name



- **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 13. Scope

- **Instructions:** In the "Scope" field, state or describe the portion of the enterprise that the risk assessment is evaluating. Your enterprise may have more than one scope that it intends to evaluate and manage using different resources, management, or degrees of risk tolerance. For example, an application production environment may be the responsibility of a product team that operates to regulatory or contractual agreements, while corporate assets may be managed by IT and may need to meet other regulations or risk acceptability levels. If your enterprise intends to operate more than one distinct scope, you will want to make a copy of the workbook and use the name of each scope in each copy of the workbook.
- **Explanation:** Risk assessments may apply to the whole enterprise, or just portions of it. Enterprises may operate in an environment that has different Safeguards 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 Safeguards 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 14. Last Completed (Date)

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 Safeguards 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

Your Impact Criteria will be automatically populated based on how you responded to the prompts in the Impact Criteria Survey, or based on the default responses if you accepted those. The example below (Figure 15) is what your Impact Criteria table would look like if you accepted the default values. Note that the "Definition" line will be populated with the Mission, Objectives (Operational and/or Financial), and Obligations prompts entered in the Impact Criteria Survey tab of the Workbook. These are not default responses and are unique to each enterprise.

Figure 15. Impact Criteria based on default Impact Criteria Survey responses

Impact Scores	Mission	Operational Objectives	Financial Objectives	Obligations
Definition				
1. Negligible	*The mission would remain intact.*	*Growth plan would be intact.*		No harm could foreseeably result.
2. Acceptable	*This mission would not be perfectly achieved, but could be recovered within normal operations.*	*Growth plan would be off target, but within variance.*		Any harm that could result would not require correction, repair, or compensation to make the harmed parties "whole."
3. Unacceptable	*This mission would not be achieved, and would require short-term, unplanned efforts, resources, or investments to recover.*	*Growth plan would be out of variance, but can be recovered within a fiscal year.*		Correctible harm may occur to one or few others.
4. High	*This mission would not be achieved. If significant, unplanned efforts, resources, or investments are not made, the mission may not ever be achievable.*	*Growth plan would be out of variance, and may require multiple years to correct.*		Correctible harm may occur to many others, or harm that can be partially corrected for a few others may occur.
5. Catastrophic	*The mission would not be achievable.*	*We would not be able to grow.*		We would not be able to protect others from any degree of harm.

Expectancy Criteria

CIS RAM considers Expectancy not to mean the probability or frequency that something may happen, but the most likely way an eventual security incident will occur. This is a subtle but important distinction. CIS RAM risk assessments do not expect risk analysts to develop probability models to consider which attack is the most likely. Rather, starting in version 2, CIS RAM automates Expectancy Scores by comparing the commonality of reported threats to the maturity of the Safeguards that would prevent the threats. The more capable a Safeguard is, the less likely a common threat will be the cause of an eventual security incident.

This is a tightly controlled way of thinking about Expectancy, so CIS RAM provides a default model for distinguishing between degrees of Expectancy, as shown below (Figure 16).

Figure 16. Expectancy Criteria

Expectancy Criteria		
Expectancy Score	**Expectancy**	**Criteria**
1	Remote	Safeguard would reliably prevent the threat.
2	Unlikely	Safeguard would reliably prevent most occurrences of the threat.
3	As likely as not	Safeguard would prevent as many threat occurrences as it would miss.
4	Likely	Safeguard would prevent few threat occurrences.
5	Certain	Safeguard would not prevent threat occurrences.

Note that the Expectancy names are plain language and not probabilistic. Nor are they intended for risk assessment participants to guess. Risk assessors should not be expected to estimate risks by determining when a risk is "Likely" or "Unlikely" to occur. Rather, these Expectancies are derived by answering a different question about an observable condition—the maturity of a Safeguard (which will be discussed in the Risk Register section below). Using plain language for each Expectancy Score will simplify how risks are communicated to others after the risk assessment is completed.

Risk Acceptance Criteria

CIS RAM for IG2 helps your enterprise establish your own rule for when to accept cybersecurity risks or for when to address them. This rule is known as "Risk Acceptance Criteria." Using plain language, you can state the Expectancy of the impact that your enterprise would start to invest against cybersecurity risks.

In the example below (Figure 17), the Risk Acceptance Criteria could read numerically—"Invest against risks where the Expectancy is '3' and the Impact is '3', or the Risk is '9' and above. But accept all risks below that." Or it can be read with the associated plain language definitions established above—"Invest against risks where a threat is as likely as not to create an unacceptable impact to our Mission, our Objectives, or our Obligations. But accept all risks below that."

Figure 17. Risk Acceptance Criteria

Risk Acceptance Criteria		
We would start to invest against risks to prevent this expectancy and impact, or higher.	**Expectancy**	**Impact**
	Acceptable Risk is less than …	**0**

This Risk Acceptance Criteria helps your enterprise develop a consistent standard for accepting risks every time a risk analysis occurs. By accepting risk using these criteria, you will be saying that you considered risk to yourself and to others, and that your assessment evaluated and accepted risks equitably and consistently.

Inherent Risk Criteria

CIS RAM for IG2 automates impact estimates in the Risk Register. To take advantage of that, the Workbook first needs to understand the Inherent Risks of your information assets. Inherent Risk is the potential maximum impact that may occur if there are no Safeguards in place. For example, 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.

Since CIS RAM for IG2 evaluates risks based on Assets rather than Safeguards, you should estimate Inherent Risk Criteria for all of the Asset Classes listed in the Inherent Risk Criteria table. Note that CIS RAM for IG1 allows you to optionally leave Asset Class rows blank, except for the "Enterprise" row.

Keep in mind that while entering risks in the Risk Register, the Impact cells in the row you are working on will reflect the Impact Value in the "Inherent Risk Criteria" table by default. However, you will be able to manually adjust them for each row in case the risks you are describing will create impacts that are different than the default.

Figure 18. Example: Inherent Risk Criteria table

Inherent Risk Criteria	What is the highest impact to the Mission, Operational Objectives, Financial Objectives, and Obligations that each Asset Type could cause? The "Enterprise" Asset Class will automatically use the highest Impact Score you provide for the assets below.

Asset Class	Mission Impact	Operational Objectives Impact	Financial Objectives Impact	Obligations Impact
Enterprise	3	3	4	4
Devices	2	1	3	3
Applications	4	2	4	4
Data	3	4	5	2
Network	3	4	3	1
Users	3	3	4	4

- **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. In the Asset Class table, record the potential magnitude of impact (the Inherent Risk) that the Asset Class in each row could create to the Mission, Operational Objectives, Financial Objectives, and Obligations. Scoring is done on a scale of '1' to '5.'
- **Explanation:** The Inherent Risk Criteria table stores the maximum Impact Value that information assets may pose to the Mission, Operational Objectives, Financial Objectives, and Obligations. Devices may pose an Inherent Mission Impact of '2' while Applications may pose an inherent Mission Impact of '4.' 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 Mission Impact Score of '4.'

Note: The Risk Register (Figure 19) will populate its Impact Scores by referring to the values you put in the Asset Class table. If you notice that your 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

Figure 19. Risk Register: Risk Analysis (using Controls v8)

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 (Figure 19) includes all of the fields you will need to evaluate your cybersecurity risks that are associated with CIS Controls for IG2.

Asset Class	Asset Name	CIS Safeguard #	CIS Safeguard Title	IG1	IG2	Our Implementation	Evidence of Implementation	Vulnerabilities	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Financial Objectives	Impact to Obligations	Risk Score	Risk Level
Applications	Fabricore	2.1	Establish and Maintain a Software Inventory	x	x	We use AppXYZControl that monitors for applications installed on all servers and end-user systems.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\20211212\2\	Shell scripting tools and compilers are permitted, but we have no way of validating scripts, or side-loaded applications.	3	2	2	4	2	4	5	10	
Applications	Fabricore	2.2	Ensure Authorized Software is Currently Supported	x	x	AppXYZControl validates that installed applications are currently supported, and that current versions are implemented.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\20211212\2\	None observed	5	2	1	4	2	4	5	5	
Applications	Fabricore	2.3	Address Unauthorized Software	x	x	AppXYZControl identifies installed applications that were not permitted and alerts the Ops team. Ops team removes unapproved applications within five business days.	Monthly exceptions reports are located in \\fileserverALPHA\evidence\20211212\2\. Tickets for uninstall of unapproved applications are located in \\fileserverALPHA\evidence\20211212\2\.	Shell scripting tools are permitted, but we have no way of validating scripts, or uninstalled applications.	4	2	2	4	2	4	5	10	
Applications	Fabricore	2.4	Utilize Automated Software Inventory Tools		x	We use AppXYZControl that monitors for applications installed on all servers and end-user systems.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\20211212\2\	None observed	5	2	1	4	2	4	5	5	
Applications	Fabricore	2.5	Allowlist Authorized Software		x	AppXYZControl uses a list of approved software in its scans and identifies installed applications that are not on that list.	Monthly exceptions reports are located in \\fileserverALPHA\evidence\20211212\2\.	AppXYZControl identifies applications after they were installed. We are not preventing unauthorized applications from being installed.	4	2	2	4	2	4	5	10	
Applications	Fabricore	2.6	Allowlist Authorized Libraries		x	AppXYZControl uses a list of approved software libraries in its scans and identified installed applications that are not on that list.	Monthly exceptions reports are located in \\fileserverALPHA\evidence\20211212\2\.	AppXYZControl identifies applications after they were installed. We are not preventing unauthorized applications from being installed.	5	2	1	4	2	4	5	5	
Applications	Fabricore	4.1	Establish and Maintain a Secure Configuration Process	x	x	End-user systems and servers are built using images that we developed for business purposes and for minimum use (fewest processes, services, and applications).	SCAP policy files for each server and workstation type are located in \\fileserverBETA\SCAP\current\.	System images are not built from known-secure standards, such as vendor-provided or community-provided SCAP polices.	2	2	3	4	2	4	5	15	

Asset Class	Asset Name	CIS Safeguard #	CIS Safeguard Title	IG1	IG2	Our Implementation	Evidence of Implementation	Vulnerabilities	Safeguard Maturity Score	VCDB Index	Expectancy Score	Impact to Mission	Impact to Operational Objectives	Impact to Financial Objectives	Impact to Obligations	Risk Score	Risk Level
Applications	Fabricore	2.1	Establish and Maintain a Software Inventory	x	x	We use AppXYZControl that monitors for applications installed on all servers and end-user systems.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\202 11212\2\	Shell scripting tools and compilers are permitted, but we have no way of validating scripts, or side-loaded applications.	3	2	2	4	2	4	5	10	
Applications		2.1	Establish and Maintain a Software Inventory	x	x	We use AppXYZControl that monitors for applications installed on some servers and end-user systems.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\202 11212\2\	Shell scripting tools and compilers are permitted, but we have no way of validating scripts, or side-loaded applications.	2	2	3	4	2	4	5	15	
Applications	Fabricore	2.2	Ensure Authorized Software is Currently Supported	x	x	AppXYZControl validates that installed applications are currently supported, and that current versions are implemented.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\202 11212\2\	None observed	5	2	1	4	2	4	5	5	
Applications		2.2	Ensure Authorized Software is Currently Supported	x	x	AppXYZControl validates for some servers and workstations that installed applications are currently supported, and that current versions are implemented.	Monthly scan reports and "diff" reports are located in \\fileserverALPHA\evidence\202 11212\2\	None observed	2	2	3	4	2	4	5	15	

Figure 20. Risk Register: Risk Analysis with Distinct and Generic Assets

The Risk Register—Risk Analysis

The CIS RAM for IG2 Risk Register will help you identify and evaluate risks that are associated with IG2 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 IG2, you may seek assistance from risk experts to help identify and evaluate those risks, or to help design reasonable safeguards to address those risks.

Note in the Risk Register that most fields have green column headers. These headers indicate that the values in those columns are already completed for you or will be automatically completed when you provide information in the cells with dark-purple headers.

Columns with dark-purple headers require your input so that a risk analysis can occur. In the example above, three dark-purple cells require your response. One light-purple cell accepts your optional input, which we will describe next.

Note: If an individual asset has a different Inherent Risk than its Asset Class, you may enter the appropriate Impact Values to the Impact cells in those risk analysis rows. You may notice a green arrow at the top left of cells in the Impact columns after you have manually entered values in those columns. The green arrow informs you that you have manually edited a column that normally uses formulas to get its values. This will not affect the functionality of the Risk Register, but you may follow Microsoft® Excel's instructions for ignoring the error so that the green arrows do not distract you.

Your Input: ASSET NAME

You will notice a light-purple column header titled, "Asset Name." Column headers that are light-purple are optional for you to fill in. CIS RAM for IG2 is an asset-based risk assessment approach that organizes CIS Safeguards by the Asset Classes they protect. Therefore, your risk assessment conversations will likely center on Asset Classes (for example, applications, devices, and networks) rather than control topics (such as access controls, vulnerability management, and encryption) as they are in CIS RAM for IG1. This also means you can evaluate two or more specific assets within a class differently. This example Risk Register shows a fictional application called "Fabricore." The manufacturer evaluated all of their applications as a single Asset Class, but were especially interested in risks posed to their Fabricore application (perhaps because it is very sensitive, or it uses controls differently than other applications). The manufacturer evaluated risks that were specific to Fabricore by duplicating all of the rows associated with the Application Asset Class by copying and pasting them into the Risk Register. They then added the name of "Fabricore" in the "Asset Name" column to distinguish its risks from other Asset Class risks. Figure 20 shows duplicate rows for Safeguards 2.1 and 2.2 to show how one Safeguard may pose two different risks based on how they are protecting generic or distinct assets.

Your Input: OUR IMPLEMENTATION

The "Our Implementation" column requires you to describe how you have implemented the Safeguard, if at all. Your Risk Score will still be calculated if you leave this cell blank, but your risk analysis will not be comprehensive if you do not consider, record, and communicate how your Safeguards are implemented.

Our example manufacturer is evaluating risks associated with applications. While reviewing CIS Control 2, they review Safeguard 2.1, "Establish and Maintain a Software Inventory." They know a software inventory is generated by their software scanning tool, AppXYZControl. That fictional application scans network devices for applications, checks to see if they are currently supported by vendors, and alerts the enterprise when applications need to be updated, when they are no longer supported, or when unapproved applications are installed. AppXYZControl, however, does not recognize executable files or scripts unless they were implemented through package managers (Linux®) or are listed in a registry hive (Windows®).

The manufacturer describes their implementation of the Safeguard this way: "We use AppXYZControl that monitors for applications installed on all servers and end-user systems."

Your Input: EVIDENCE OF IMPLEMENTATION

Since independent auditors may rely on observations made during the risk assessment, the "Evidence of Implementation" column can be used to show what the "Our Implementation" column statement was based on. The example enterprise points independent auditors (or others who are interested) to a location where the evidence for the implemented safeguard can be found by stating, "Monthly scan reports and "diff" reports are located in \\ fileserverALPHA\evidence\20211212\2\."

Your Input: VULNERABILITIES

Since AppXYZControl does not recognize files or scripts that a user may have "side-loaded," or developed or saved without using the operating system's installation utility, this is a vulnerability. Infected applications or destructive scripts could be available on an end-user's system or a server and AppXYZControl would not alert the Operations team. Therefore, the manufacturer described their vulnerability this way, "Shell scripting tools and compilers are permitted, but we have no way of validating scripts, or side-loaded applications."

Your Input: SAFEGUARD MATURITY SCORE

Our example manufacturer entered a Maturity Score of '3' for Safeguard 2.1. Let's examine why.

Most of your automated risk analysis happens after you enter a value in the "Safeguard Maturity Score" column. You will enter a value from '1' to '5' to describe how reliable your implementation of the Safeguard is.

Maturity Scores for CIS RAM are slightly different from other maturity scores. While some maturity models describe the formalization of safeguards, or they combine formalization with automation, the maturity scoring in CIS RAM focuses on how reliable the Safeguard would be. Note that the definitions draw attention to how you would know that Safeguards are effective.

Table 1. CIS RAM Maturity Scores

Maturity Scores	Definition
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.

Consider which maturity definition best describes your use of the Safeguard for the Asset Class in that row of the Risk Register. Enter the corresponding Maturity Score ('1' through '5') in that column. The example manufacturer believed that their use of AppXYZControl was implemented on all assets, but that inconsistencies could not be corrected. They knew they were not catching scripts or "side-loaded" applications. A Maturity Score of '4' would be too high, they decided, and therefore selected a Maturity Score of '3.'

Additional information on Maturity Scores can be found in Appendix B. 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 IG2. Additional guidance on how to import CSAT scoring can be found in Appendix D. 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.

The Risk Register—Automated "Risk Score" and "Risk Level"

As stated above, your "Risk Score" and "Risk Level" columns should automatically populate after you enter a value in the "Safeguard Maturity Score" column. The Risk Score is calculated by multiplying the Expectancy Score with the highest Impact Score. The resulting "Risk Level" will be either green, yellow, or red. These colors indicate whether the risk evaluates as "acceptable" as you've described it in your Risk Acceptance Criteria. Green indicates that the risk evaluates as "acceptable." Yellow indicates that the risk is "unacceptably high, but not urgent." Red indicates that the risk is "urgent."

While planning your risk treatment activities, you will want to prioritize higher value risks over lower value risks. Of course, other criteria will come into play, such as the availability of resources to reduce risks. However, as a rule of thumb, it makes sense to focus on reducing the highest risks first.

Note: Enterprises should be aware that risk values such as '25,' '4,' and '12' do not meaningfully describe a risk. They are simply products of ordinal values that "order" your priorities. The more commonly a threat will create a high impact, the more you should prioritize it. And the less commonly a threat will create a low impact, the less of a priority it is.

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 Financial Objectives	Risk Treatment Safeguard Impact to Obligations	Risk Treatment Safeguard Risk Score	Reasonable and Acceptable
Reduce	2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Permit script scripting tools and compilers on only protected systems administrator computers.	1	1	4	2	2	4	4	Yes
Accept	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. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.				4	2	2	4		Yes
Reduce	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.	Permit script engines on only systems administrator computers.	1	1	4	2	2	4	4	Yes
Accept	2.4	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.				4	2	2	4		Yes
Reduce	2.5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.				4	2	2	4		No
Accept	2.6	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.				4	2	2	4		Yes
Reduce	4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Adopt SCAP policies for all devices. Create deployment images for each device and deploy systems using only those images. Add SCAP policies to the vulnerability scanning application and scan systems before putting them into production. Update the SCAP policies quarterly and include all approved changes to the updated policies.	4	2	4	2	2	4	8	Yes

Figure 21. Risk Register: Risk Treatment

The Risk Register: Risk Treatment

The columns with the blue headers (indicating that the value is either automatically calculated or fixed) are associated with Risk Treatment Safeguards. Risk Treatment Safeguards are what you plan to implement to reduce your risks to an acceptable level.

Your Input: RISK TREATMENT OPTION

The left-most column is "Risk Treatment Option." This column prompts you to state whether you intend to reduce or accept the risk. You should select to reduce all risks that are unacceptably high. Risks below your Risk Acceptance Criteria can be marked as "Accept." If you choose to, you can invest in reducing acceptable risks. Just make sure you have first resolved unacceptably high risks before pursuing perfection in others.

Your Input: OUR PLANNED IMPLEMENTATION

Use the "Our Planned Implementation" column to state how your enterprise expects to implement the Safeguard. By referring back to the Risk Analysis example in Figure 19, you will notice that risks associated with Safeguards 2.5 and 4.1 are unacceptably high. Consequently, those Safeguards are associated with the "Reduce" Risk Treatment Option, and their Risk Treatment Safeguard columns are the same as the Safeguards at the left of the row. CIS RAM encourages you to find a way to implement that Safeguard to reach an acceptably low risk score, but you may occasionally need to find an alternative approach for addressing the risk if the recommended Safeguard is not reasonable.

Note: If using a specific Safeguard is not practical or plausible in the short-term, but could happen in the future, then it is important to describe that eventual implementation in this column.

Note: If a Risk Treatment Safeguard poses too high an impact to your Mission, Objectives, or Obligations, that Safeguard cannot be reasonably implemented. In this case, consider other Safeguards that may mitigate the risk. It is appropriate within CIS RAM to state a Risk Treatment Safeguard that is different from the Safeguard at the head of the row. For example, if Safeguard 6.7, "Centralize Access Control," cannot be applied to a specific system, you may state as a Risk Treatment Safeguard 8.11, "Conduct Audit Log Reviews," if you see that alerts of anomalous activity on that system would make the associated risk acceptably low.

In the "Our Planned Implementation" column, describe briefly what you will do to implement and operate the Risk Treatment Safeguard. Since your risks were too high, your current use of a Safeguard is somehow not implemented well enough to provide you confidence that it will effectively protect assets, whether those assets belong to you or to others. Your planned implementation will likely be something to raise your maturity. Safeguards that are implemented only on key assets (Maturity = '2') could be implemented on all assets (Maturity = '3'), for example. Or Safeguards that are implemented everywhere (Maturity = '3') could be tested and corrected (Maturity = '4'), or automated (Maturity = '5').

As you describe your planned implementation, consider how you will implement the Safeguard, or improve the reliability (the Maturity) of your implementation. Describe that approach briefly in this column.

The example manufacturer decided to exclude compilers and scripting shells from all systems, except for a set of "protected" administrator systems that are used for maintenance.

Your Input: RISK TREATMENT SAFEGUARD MATURITY SCORE

You will use the "Risk Treatment Safeguard Maturity Score" column to state the degree of confidence you have that the Safeguard would be effective. You will use the same Maturity Score guidance you used in the risk analysis. After selecting a score of '1' to '5', your "Risk Treatment Safeguard Risk Score" will be automatically calculated by multiplying the highest "Risk Treatment Impact Score" (Impact to Mission, Objectives (Operational or Financial), and Obligations) with the "Risk Treatment Safeguard Expectancy Score."

Note: It may also be possible to reduce the Impact Score with some Risk Treatment Safeguards. One common way to reduce impacts to is isolate sensitive systems, or to remove sensitive data from some systems. If you manually add Impact Scores, you will remove the formulas that populate the impact columns, and a green triangle will appear at the top left of the cells you manually edited. This will not affect your Risk Treatment Risk Score calculation, but the row you edit will no longer reference the Inherent Risk Score of its Asset Class.

Additionally, your "Reasonable and Acceptable" score will be automatically calculated. The determination of "Acceptable" is achieved when the "Risk Treatment Safeguard Risk Score" is below your Acceptable Risk Score. "Reasonable" is determined when the "Risk Treatment Safeguard Risk Score" is equal to or below the "Risk Score."

In the example Risk Register, the manufacturer was able to plan for Reasonable and Acceptable Safeguard implementations for all but the last Risk Treatment Safeguard. They described a comprehensive, manual process for the 4.1 Risk Treatment Safeguard and selected a "Risk Treatment Safeguard Maturity Score" of '4' because they could not guarantee consistency of that Safeguard. When they notice that their resulting risk is not Reasonable and Acceptable, they will need to find a way to make the Risk Treatment Safeguard consistent (either through automation or through accountability, perhaps).

Risk Register: Cost Analysis

CIS RAM for IG2 includes a cost analysis for the Risk Treatment Safeguard. The cost analysis comes in two parts: 1) each row includes optional cells for estimating the "Risk Treatment Safeguard Cost" along with the quarter and year that a Safeguard is scheduled to be implemented, and 2) a "Reasonable Annual Cost" table that combines all Safeguard costs for each year and compares it to your "Acceptable" limit in the "Financial Objectives" column of your "Impact Criteria" table.

The first of these cost analyses helps you plan your budget for each Risk Treatment Safeguard. The second helps you determine whether the budget for an entire year is reasonable, given your enterprise's tolerance for unexpected impacts against business costs.

Figure 22. Example: Risk Treatment Safeguard Cost Analysis

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 Cost	Implementation Quarter	Implementation Year
Reduce	2.1	Establish and Maintain a Software Inventory	Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.	Permit script scripting tools and compilers on only protected systems administrator computers.	5	$ -	Q2	2022
Accept	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. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.					
Reduce	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.	Permit script engines on only systems administrator computers.	5	$ -	Q2	2022
Accept	2.4	Utilize Automated Software Inventory Tools	Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.					
Reduce	2.5	Allowlist Authorized Software	Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.					
Accept	2.6	Allowlist Authorized Libraries	Use technical controls to ensure that only authorized software libraries, such as specific .dll, .ocx, .so, etc., files, are allowed to load into a system process. Block unauthorized libraries from loading into a system process. Reassess bi-annually, or more frequently.					
Reduce	4.1	Establish and Maintain a Secure Configuration Process	Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	Adopt SCAP policies for all devices. Create deployment images for each device and deploy systems using only those images. Add SCAP policies to the vulnerability scanning application and scan systems before putting them into production. Update the SCAP policies quarterly and include all approved changes to the updated policies.	4	$ 501,000	Q2	2022

Our example manufacturer in Figure 22 expected their Risk Treatment Safeguards for 2.1 and 2.3 to cost no money, and that they could implement the Safeguards in Q2 of 2022. Their planned Risk Treatment Safeguard for 4.1 was going to be more expensive.

Recall that they stated a limit for acceptable impacts to their Financial Objectives as $10,000. However, their budgeted Risk Treatment Safeguard plan for 2022 is $501,000. As a result, the Reasonable Annual Cost table shows that this is an unreasonable budget increase. The manufacturer could find a less expensive implementation of their safeguard, or could request that executives approve a budget change to address this risk.[3] If this Safeguard is the only plausible option for reducing the risk, the latter approach may be their only option.

Figure 23. Reasonable Annual Cost table

Reasonable Annual Cost		
Impact to Financial Objectives	Year	Reasonable?
$ -	2021	Yes
$ 501,000.00	2022	No

Note: When estimating costs for Risk Treatment Safeguards, be sure to enter the cost once for Safeguards that you list multiple times. For example, if a network access control appliance would take care of five risks, enter the planned quarter and year for implementing the appliance for all five of those Risk Treatment Safeguard rows, but only enter the cost of the appliance in one of those Risk Treatment Safeguard rows. This ensures that the Reasonable Annual Cost table counts each cost once during the year it occurs.

3 If a larger budget is approved for the following year, then the $501,000 impact will no longer be unexpected. If an enterprise cannot afford to reduce risks to acceptable levels, this risk assessment should indicate to them the seriousness of the imbalance. The enterprise may need to operationally or financially adjust so they can satisfy their business goals while ensuring reasonable care for others who they may harm.

Conclusion

Cybersecurity risk analysis is an inexact but important process. If done correctly, we will have considered how well prepared we are for the most (and least) foreseeable events, and we will have considered how badly we or others could be harmed. We will also have thought about how CIS Controls and Safeguards can make us more prepared for those foreseeable threats while making sure that we, and those we protect, will be OK.

CIS RAM 2.1 for IG2 presents to enterprises some tools and instructions for conducting a duty of care risk analysis to meet these goals. While every risk method creates an imperfect model of the world, CIS RAM provides a data-informed construct to make the analysis consistent and reality-based. Further, CIS RAM helps enterprises evaluate and plan for risks using natural language so that difficult cybersecurity matters can be communicated simply, and so that nontechnical executives can make informed decisions.

CIS RAM is a family of documents built upon contributions from the CIS community. If you find opportunities to extend, expand, or improve this method, your contributions are welcome.

APPENDIX A

Defining Impact Criteria

Summary

Note: While this guidance will address concepts such as regulatory compliance and duty of care, this text should not be interpreted as legal advice. If you or your enterprise has questions about how and whether to apply these instructions to address compliance and liability, consult legal counsel.

Defining Impact Criteria is among the most important things you can do while conducting a CIS RAM risk assessment, especially for IG2 and IG3 enterprises. In IG1, CIS RAM presents default Impact Score definitions that are generic, prompting risk assessors to define just their Impact Areas. In CIS RAM IG2 and IG3, you define your Impact Areas and your Impact Scores.

Your Impact Criteria states what you intend to protect and the degrees of harm you or others could tolerate when a security incident occurs. CIS RAM is based on the Duty of Care Risk Analysis (DoCRA) Standard, which describes a set of principles and practices that should be used while we evaluate cybersecurity risk.

Why Mission, Objectives, and Obligations?

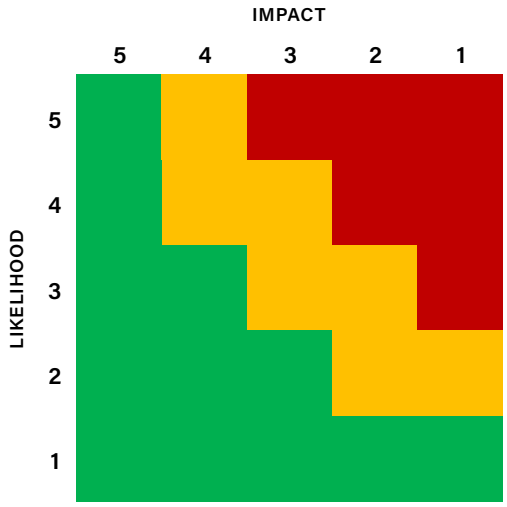


Figure 24. Generic heat map

We protect assets against cybersecurity incidents to prevent harm both to ourselves and to others. This important concept is often lost when we analyze risk. Consider how a "heat map" evaluates risk. The heat map provides a set of "ordinal" values ('1' through '5' in this example) that "order" degrees of high and low impacts and likelihoods. We infer from these heat maps that lower likelihoods of lower impacts are better than higher likelihoods of higher impacts. However, people participating in a risk assessment will likely not have a common understanding among themselves about what '1', '3', or '5' likelihoods or impacts mean. Any one person may not even maintain consistency in what they themselves mean by '1', '3', or '5' impacts, especially when they assess risks associated with a variety of cybersecurity topics.

Therefore, we need guidance for how to estimate whether a cybersecurity incident would cause a '1', '2', '3', '4', or '5' level impact[4].

4 This appendix demonstrates semi-quantitative risk analysis, which is an imperfect way to describe risk. Well-documented shortcomings in semi-quantitative analysis such as compression error are accepted in current CIS RAM modules. By defining risk impacts in well-defined ordinal ranges, risk assessors can compare unlike things such as missions, objectives, and obligations each on their own terms, and can compare how impact scores relate to acceptable, unacceptable, and catastrophic magnitudes of harm as multiple parties would experience them.

CIS RAM provides guidance for defining each of these levels of impact. However, more than that, CIS RAM describes three types of Impact so we are sure to consider potential harm to ourselves and to others. CIS RAM and DoCRA both include Mission, Objectives (Operational and Financial), and Obligations as Impact Areas that are to be evaluated separately. The highest value of these Impacts is multiplied against the Impact Score to calculate the Risk Score. This ensures that the risk evaluation and subsequent planning and mitigation are based on the worst-case scenario.

But why "Mission," "Operational Objectives," "Financial Objectives," and "Obligations" for CIS RAM?

- **Mission:** An enterprise's Mission is its purpose. The Mission is also the benefit that the public (its constituency, its customers, the general public, etc.) enjoys as a result of the risk. We do not want a cybersecurity incident to harm that value unacceptably. We also do not want a safeguard to harm that value unacceptably. This is a core tenet of DoCRA and CIS RAM. Neither an incident nor a safeguard should harm our mission.
- **Operational Objectives:** An enterprise's Operational Objectives are the goals it intends to achieve in its own self-interest. This Impact Area is defined as a statement (not a numerical value), such as "profitability," "growth," "maintain our lead in the industry," or "maintain a balanced budget." This Impact Area is what is most often addressed when enterprises evaluate risk. It is most often associated with "bottom-line, financial" concerns.
- **Financial Objectives:** Similar to "Operational Objectives," "Financial Objectives" is a self-interested Impact Area. However, it is defined in numerical terms (dollars) rather than as a statement so it can be compared to budget estimate in the Risk Register.
- **Obligations:** Since we must evaluate risks that we pose to others, the "Obligations" Impact Area includes parties who may be harmed, and the ways they may be harmed. Typically, these harms are associated with identity theft or financial fraud. However, the more we rely on technologies, the more we need to consider physical and psychological harms in this Impact Area.

By using these Impact Areas, we remind our colleagues why we manage cybersecurity with every risk analysis that we do. We remind them of why we plan to implement safeguards, and why we request investments in technologies, processes, and capabilities. We also prompt the right conversations when we prioritize and accept risks, because every conversation includes the levels of harm that we or others may suffer due to a cybersecurity incident, or an overly burdensome safeguard.

As well, CIS RAM is preparing the enterprise to describe their risk-based cybersecurity programs in ways that regulators and lawyers understand duty of care. Your risk assessment and your risk treatment plan will demonstrate that you looked out for yourselves and others equitably, and that your safeguards were not more burdensome than the risks they were meant to reduce.

Ways to Define Mission

While defining your Mission, consider the following:

- What benefit does your enterprise provide to others?
- What value do others receive by engaging in risk with you?
- What makes the risk worthwhile to others?

If your enterprise has already published a mission statement, you may find that it sufficiently defines these benefits. If that is not the case, CIS RAM advises that you work with officers of your enterprise to define this term.

Table 2. Example: Mission definitions

Be sure to state your Mission in terms that can be observed or measured, especially while determining whether your Mission is succeeding or failing. CIS RAM provides a few examples of Mission definitions below.

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.
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.

Enterprise Type	Example Missions
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.

Ways to Define Operational Objectives

Many enterprises have already defined their Operational Objectives, whether or not they have defined them as "objectives." These are performance goals that are normally associated with profitability, growth, maintaining budgets for nonprofits, or achievement of strategic goals.

While defining Operational Objectives, consider the following:

- Which goals are most essential for the enterprise to achieve?
- Which goals does management most often refer to when they determine whether the enterprise has failed or succeeded?
- When members of the enterprise request cybersecurity resources and management resists, what do they say they cannot sacrifice as a reason to not make security investments?

As with your Mission definition, be sure to state your Operational Objectives in terms that can be observed or measured, especially while determining whether your Operational Objectives are succeeding or failing. CIS RAM provides a few example Operational Objectives definitions below.

Table 3. 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

Enterprise Type	Example Objectives
Manufacturing	• Profit • Profitable growth
Critical Infrastructure	• Profit • Profitable growth

Ways to Define Financial Objectives

Your Financial Objectives are typically the simplest to define. They are often bound to profitability or budget maintenance for nonprofits and government agencies. Similar to Operational Objectives, while determining which numerical values to include in your Financial Objectives, consider the following:

- Which financial goals are most essential for the enterprise to achieve?
- Which financial goals do management most often refer to when they determine whether the enterprise has failed or succeeded?
- When members of the enterprise request cybersecurity resources and management resists, what financial interests do they say they cannot sacrifice as a reason to not make security investments?

Many of the example Operational Objectives definitions provided in Table 3 also serve as good examples for Financial Objectives.

Ways to Define Obligations

You should carefully consider your obligations to protect others. While protection against identity theft, privacy intrusion, or fraud are common obligations, you should think carefully about ways that a bad actor may cause harm. Here are some things to consider:

- Which individuals or enterprises could be harmed by abusing systems?
- Which individuals or enterprises could be harmed by abusing information?
- What kinds of harm could individuals or enterprises suffer?
- What dependencies do others have on the systems and information?
- How could those dependencies create vulnerabilities if the systems or information fail to remain secure?

Table 4. Example: Obligations

CIS RAM provides a few example Obligations definitions below.

Enterprise Type	Example Obligations
Healthcare Provider	• Protect patient privacy • Protect patients from medical device tampering • Protect payers from fraudulent claims
Banks, Credit Unions	• Protect customers/members from financial fraud • Protect customers/members from loss of privacy
Retail	• Protect customers from financial fraud • Protect customers from loss of privacy • Protect shareholders from avoidable losses (public companies)
Nonprofit, NGO	• Protect donor privacy • Protect constituency privacy

Enterprise Type	Example Obligations
Professional Services	• Protect client intellectual property • Protect clients from liabilities due to breached information
Education	• Protect privacy of minors
Hospitality	• Protect guests from financial fraud • Protect guests from loss of privacy • Protect guests from physical harm
Manufacturing	• Protect customers from failed products • Protect customers from exposure of intellectual property • Protect shareholders from avoidable losses (public companies)
Critical Infrastructure	• Protect the public from harm due to failed systems, services, or infrastructure. (Carefully consider the kinds of losses that the public can suffer from when systems, services, and infrastructure fail.)

Summary

Your Impact Areas should be carefully considered and discussed with executives who will make decisions about Risks and Risk Treatment Safeguards. The Impact Area definitions and Impact Score definitions are intended to help the enterprise communicate cybersecurity risk, so its terms should be commonly understood and valued.

Once you begin describing risks in terms of what matters to your enterprise's Mission, Objectives, and Obligations, your enterprise will have the tools they need to make informed cybersecurity decisions whether or not each member of the team understands the technical matters underlying each risk.

APPENDIX B

Maturity Scores

The CIS RAM for IG2 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 Safeguards against the commonality of threats that the Safeguards would prevent.

Table 5. Maturity Score table

Maturity Score	Definition
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 Safeguard, ask how an independent assessor would answer the question. Do they see the Safeguard 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 C

Expectancy Scores

The CIS RAM for IG2 Risk Register automatically arrives at an Expectancy Score by comparing the commonality of reported Asset Classes to the maturity of your Safeguards that prevent threats to those Asset Classes.

In this way, CIS RAM for IG2 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:

Table 6. Expectancy Score table

Expectancy Score	Expectancy	Definition
1	**Remote**	Safeguard would reliably prevent the threat.
2	**Unlikely**	Safeguard would reliably prevent most occurrences of the threat.
3	**As likely as not**	Safeguard would prevent as many threat occurrences as it would miss.
4	**Likely**	Safeguard would prevent few threat occurrences.
5	**Certain**	Safeguard would not prevent threat occurrences.

The IG2 Workbook contains a table (Vocabulary for Event Recording and Incident Sharing (VERIS) Community Database (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 D

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 IG2 Workbook.

CIS CSAT Pro: Steps to Export Data to Import into CIS RAM IG2 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 IG2 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 & IG-2" 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 IG2 Workbook.
   a. In the CSAT Pro CSV file, copy the contents of column E (labeled "Sub-Control[5] Score") excluding the heading row.
   b. Go to the "CIS CSAT Pro" tab in the CIS RAM for IG2 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.
      i. For instance, if you are using Controls v7.1, you might copy cells E2 to E141 from the CSAT Pro CSV to C5 to C146 in the "CIS CSAT Pro" tab of the CIS RAM for IG2 Workbook.

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

3. Once scores are final, go to the appropriate CIS RAM tab — "3a. Risk Register Controls v7.1" for v7.1 of the CIS Controls or "3b. Risk Register Controls v8" for v8 of the CIS Controls.
   a. Sort the Risk Register by 'CIS Safeguard #,' lowest to highest. (This is a critical step, as the Risk Register is sorted by 'Asset Class' by default, not 'CIS Safeguard #.')

   - Copy the scores in the "CIS RAM Maturity Score Final" column into the "Safeguard Maturity Score" column of the appropriate CIS RAM tab — "3a. Risk Register Controls v7.1" for v7.1 of the CIS Controls or "3b. Risk Register Controls v8" for v8 of the CIS Controls.
   - Right-click to copy and "Paste Special" as "Values" (e.g., 1,2,3).
   - Re-sort the Risk Register by 'Asset Class,' A > Z.

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.

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

CIS-Hosted CSAT: Steps to Export Data to Import into CIS RAM IG2 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.

1. In CIS-Hosted CSAT, filter on IG1 and IG2 and export the filtered Safeguards.
   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 both "Group 1" and "Group 2" for the Implementation Group filter and click Filter.
      i. 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:
   d. Select the checkbox next to each blue Safeguard.
   e. 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.
   f. Click the Download Report button to export the report.

2. Copy your scores from the exported CIS-Hosted CSAT XLSX file to the CIS RAM for IG2 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 IG2 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).
   d. Paste the copied data into the appropriate section of the "CIS-Hosted CSAT" tab.
      i. For instance, if you are using Controls v7.1, you might copy the cells from E2:E141 over to H2:H141 from the CIS-Hosted CSAT XLSX file, select cell C14 in the "CIS-Hosted CSAT" tab in the CIS RAM for IG2 Workbook and paste them there.

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

3. Once scores are final, go to the appropriate CIS RAM tab – "3a. Risk Register Controls v7.1" for v7.1 of the CIS Controls or "3b. Risk Register Controls v8" for v8 of the CIS Controls.
   a. Sort the Risk Register by 'CIS Safeguard #,' lowest to highest. (This is a critical step, as the Risk Register is sorted by 'Asset Class' by default, not 'CIS Safeguard #.')
   b. Copy the scores in the "CIS RAM Maturity Score Final" column into the "Safeguard Maturity Score" column of the appropriate CIS RAM tab – "3a. Risk Register Controls v7.1" for v7.1 of the CIS Controls or "3b. Risk Register Controls v8" for v8 of the CIS Controls.
   c. Right-click to copy and "Paste Special" as "Values" (e.g., 1,2,3).
   d. Re-sort the Risk Register by 'Asset Class,' A > Z.

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 E

Customizing the Workbook

The CIS RAM for IG2 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 F

How CIS RAM for IG2 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,[6] ISO 27005,[7] and RISK Information Technology (IT).[8] 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,[9] litigators,[10] and the legal community in general.[11]

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

7 ISO/IEC 27005:2011 provided by the International Organization for Standardization

8 RISK IT Framework provided by ISACA

9 Executive Order 12866, 1993

10 The Learned Hand Rule. United States v. Carroll Towing Co. - 159 F.2d 169

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

APPENDIX G

Helpful Resources

Center for Internet Security (CIS®)

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)

Contact Information

Center for Internet Security (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

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