

CIS Risk Assessment Method (RAM)

Version 2.1

Core Document

January 2022

CIS RAM v2.1

Center for Internet Security® Risk Assessment Method Version 2.1

January 2022

Background and Acknowledgments

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

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

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

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

Editor

Chris Cronin, Partner, HALOCK Security Labs

Contributors

Aaron Piper, CIS

David Andrew, Partner, HALOCK Security Labs

Jim Mirochnik, Partner, HALOCK Security Labs

Paul Otto, Attorney, Hogan Lovells US LLP

Robin Regnier, CIS

Terry Kurzynski, Partner, HALOCK Security Labs

Valecia Stocchetti, CIS

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (<https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

CIS RAM also incorporates the CIS Critical Security Controls® (CIS Controls®) Version 7.1 and Version 8, which are licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls and CIS RAM Core, you are authorized to copy and redistribute the content as a framework for use by you, within your organization and outside of your organization for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform or build upon the CIS Controls or CIS RAM Core, you may not distribute the modified materials. Commercial use of the CIS Controls or CIS RAM Core is subject to the prior approval of the Center for Internet Security, Inc. (CIS).

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

© 2022 Center for Internet Security, Inc.

Contents

Forward	iii
Who is This Risk Assessment Method For?	iv
What This Document Provides	v
Glossary	vi
Style Conventions in This Document	viii
Acronyms and Abbreviations	ix
<hr/>	
CIS RAM Principles and Practices	1
Risk Assessment Process	2
Developing the Risk Assessment Criteria	3
Developing the Risk Acceptance Criteria	6
Modeling the Risks	7
Evaluating the Risks	8
Recommending CIS Safeguards	9
Evaluating Recommended Safeguards	10
Summary	12
Recommended Next Steps	13
Helpful Resources	14
Contact Information	16

Forward

The objective of the Center for Internet Security® Risk Assessment Method (CIS RAM) is to help enterprises plan and justify their implementation of CIS Critical Security Controls® (CIS Controls®) Versions 7.1 and 8, whether those Controls are fully or partially operating. Few enterprises can apply all of the CIS Controls in all environments and protect all information assets. Some Controls offer effective security, but at the cost of necessary efficiency, collaboration, utility, productivity, or available funds and resources.

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 ISO 27005¹, NIST Special Publications 800-30², and Risk Information Technology (IT)³. 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 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 regulators⁴, litigators⁵, and the legal community in general.⁶

CIS designed and prioritized the CIS Controls so that they would prevent or detect the most common causes of cybersecurity events, as determined by a community of information security professionals. As a result, the CIS Controls have risk considerations at their core.

Since risks vary from one enterprise to the next, the risk analysis methods described in this document will assist enterprises in applying sensible and practical CIS Controls so that they reasonably and defensibly address each enterprise's unique risks and resources.

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

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

3 RISK IT Framework provided by ISACA

4 Executive Order 12866, 1993

5 The Learned Hand Rule, *United States v. Carroll Towing Co.* – 159 F.2d 169

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

Who is This Risk Assessment Method For?

CIS RAM Core (this document) serves as a foundation for other documents in the CIS RAM family of documents. CIS RAM Core is useful to individuals and enterprises that wish to understand the principles and practices supporting the CIS RAM family of documents. CIS RAM Core is also useful for enterprises and cybersecurity practitioners who are experienced at assessing risk, and who are able to quickly adopt its principles and practices for their environment.

Supplemental documents in the CIS RAM family will demonstrate methods for conducting risk assessments. One document for each Implementation Group (IG1, IG2, and IG3) will be the anchors in the CIS RAM family. Other topics that may be useful to the community include:

- Estimating expectancy and impact using both qualitative and quantitative models
- Estimating impacts using qualitative and quantitative models
- Combining the principles and practices of CIS RAM with other risk assessment methods, such as Factor Analysis of Information Risk (FAIR) and Applied Information Economics (AIE)⁷
- Measuring and reporting risk to nontechnical executives

Members of the CIS RAM Community who have developed methods for extending CIS RAM into these and other areas are welcome to participate in developing these and similar modules.

Each of the documents in the CIS RAM family of documents have material to help users accomplish their risk assessments, and include:

- Examples
- Templates
- Exercises
- Background material
- Further guidance on risk analysis techniques

⁷ <https://hubbardresearch.com/about/applied-information-economics/>

What This Document Provides

The CIS RAM Core is a “bare essentials” version of CIS RAM that provides the principles and practices of CIS RAM risk assessments to help users rapidly understand and implement the risk assessment method.

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

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

Glossary

Appropriate	A condition in which risks to information assets will not foreseeably create harm that is greater than what the enterprise or interested parties can tolerate.
Asset Class	A group of information assets that are evaluated as one set based on their similarity. Devices, applications, data, users, and network devices are examples, all of which fall under the category of enterprise assets.
Burden	The negative impact that a Safeguard may pose to the enterprise, or to others.
Business Owners	Personnel who own business processes, goods, or services that information technologies support (customer service managers, product managers, sales management, etc.).
CIS Critical Security Controls (CIS Controls)	A prioritized set of actions to protect information assets from threats, using technical or procedural CIS Safeguards.
CIS Safeguard	Technical or procedural protections that prevent or detect threats against information assets. CIS Safeguards are implementations of the CIS Controls.
Constituents	Individuals or enterprises that may benefit from effective security over information assets, or may be harmed if security fails.
Due Care	The amount of care that a reasonable person would take to prevent foreseeable harm to others.
Duty of Care	The responsibility to ensure that no harm comes to others while conducting activities, offering goods or services, or performing any acts that could foreseeably harm others.
Expectancy	The estimation that if an incident were to occur that it would be due to the threat described in the analysis.
Expectancy Score	The score — usually ranked from '1' to '3' or '1' to '5' — 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, usually from '1' to '3' or '1' to '5'. For example, CIS RAM for IG1 uses Impact Scores ranging from '1' to '3', whereas CIS RAM for IG2 and IG3 use Impact Scores ranging from '1' to '5'.
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 or 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'.
Observed Risk	The current risk as it appears to the risk assessor.
Probability	The product of quantitative analysis that estimates the expectancy of an event as a percentage within a given time period.

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.
Residual Risk	The risk that remains after a Safeguard is applied. This concept is not directly used by CIS RAM, but implies that risk is lowered when a Safeguard is applied. Residual risk does not take into account the potential negative impacts to the enterprise when Safeguards are applied.
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 Evaluation	The mathematical component of risk analysis that estimates the expectancy and impact of a risk, and compares it to acceptable risk.
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, reduce, transfer, or avoid 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. <i>Confidentiality, Integrity, and Availability</i> 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.
Stewards	Personnel who are responsible for the security and proper operations of information assets (database administrator, records manager, network engineer, etc.).
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’

Acronyms and Abbreviations

CIS	Center for Internet Security
CIS RAM	Center for Internet Security Risk Assessment Method
DoCRA	Duty of Care Risk Analysis
FAIR	Factor Analysis of Information Risk
IG1	Implementation Group 1
ISO	International Organization for Standardization
IT	Information Technology
NIST	National Institute of Standards and Technology

CIS RAM Principles and Practices

CIS RAM Core uses the Duty of Care Risk Analysis Standard⁸ (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 enterprise. 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 follows⁹:

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.

⁸ Also known as “DoCRA” or “the DoCRA Standard” – <https://www.docra.org>

⁹ Quoted from “the DoCRA Standard” – <https://www.docra.org>

Risk Assessment Process

CIS RAM risk assessments involve the following activities:

- **Developing the Risk Assessment Criteria and Risk Acceptance Criteria:** Establish and define the criteria for evaluating and accepting risk.
- **Modeling the Risks:** Evaluate current implementations of the CIS Safeguards that would prevent or detect foreseeable threats.
- **Evaluating the Risks:** Estimate the expectancy and impact of security breaches to arrive at the risk score, then determine whether identified risks are acceptable.
- **Recommending CIS Safeguards:** Propose CIS Safeguards that would reduce unacceptable risks.
- **Evaluating Recommended CIS Safeguards:** Risk-analyze the recommended CIS Safeguards to ensure that they pose acceptably low risks without creating an undue burden.

CIS RAM for IG1, IG2, and IG3 will all include these activities, but will vary from one another in how risks are modeled:

- **CIS RAM for IG1 will model risks using the CIS Controls as the basis for each risk analysis.** IG1 enterprises will not have expert resources to help them model risks, so the Control-based risk analysis will help enterprises model risks by first asking, "We should use all of these recommended Safeguards, but how much and why?"
- **CIS RAM for IG2 will model risks using assets or asset classes as the basis for each analysis.** IG2 enterprises will have capable technical experts on-hand who will be guided to consider how to protect each asset or asset class against foreseeable threats. The asset-based risk analysis will help enterprises model risks by first asking, "We should protect all of these assets, but with which Safeguards and why?"
- **CIS RAM for IG3 will model risks using foreseeable threats as the basis for each analysis.** IG3 enterprises will have cybersecurity experts available to them who will be guided to consider how foreseeable threats would operate in their enterprise. The threat-based analysis will help enterprises model risks by first asking, "We should prepare for these threats, but using which Safeguards on which assets and why?"

Developing the Risk Assessment Criteria

CIS RAM Core evaluates risk using “Risk = Impact x Expectancy.” This calculation will evaluate both currently observed risks and recommended CIS Safeguards so that risk assessors can compare them and determine whether recommended Safeguards are “reasonable.”

Risk assessors will define their Risk Assessment Criteria by creating definitions for “Impact” and “Expectancy.” Users should refer to the workbooks that are provided with each CIS RAM module (for IG1, IG2, and IG3) for criteria examples.

Impacts will consider the enterprise’s Mission (the benefit that interested parties gain from the enterprise), their Operational Objectives (the enterprise’s goals), and their Obligations (to protect others from harm). Impact Scores will state levels of magnitude (‘1’ through ‘5’) to help risk assessors consistently estimate the impact that may occur from a threat. Impacts are defined in the model provided below. Magnitudes ‘1’ and ‘2’ are shaded to reference acceptably low magnitudes.

TABLE 1. Impact Criteria definition guidelines

IMPACT SCORES	IMPACT TO MISSION	IMPACT TO OPERATIONAL OBJECTIVES	IMPACT TO OBLIGATIONS
<i>Definition</i>	<i>Define the enterprise’s Mission (why the risk is worth engaging).</i>	<i>Define the enterprise’s Operational Objectives (the enterprise’s goals).</i>	<i>Define the enterprise’s Obligations (duty of care owed to others).</i>
1 Negligible	Describe a negligible impact to the Mission.	Describe a negligible impact to the Operational Objectives.	Describe a negligible impact to the Obligations.
2 Acceptable	Describe an acceptable impact to the Mission.	Describe an acceptable impact to the Operational Objectives.	Describe an acceptable impact to the Obligations.
3 Unacceptable	Describe an unacceptable impact to the Mission.	Describe an unacceptable impact to the Operational Objectives.	Describe an unacceptable impact to the Obligations.
4 High	Describe a high, recoverable impact to the Mission.	Describe a high, recoverable impact to the Operational Objectives.	Describe a high, recoverable impact to the Obligations.
5 Catastrophic	Describe an unrecoverable impact to the Mission.	Describe an unrecoverable impact to the Operational Objectives.	Describe an unrecoverable impact to the Obligations.

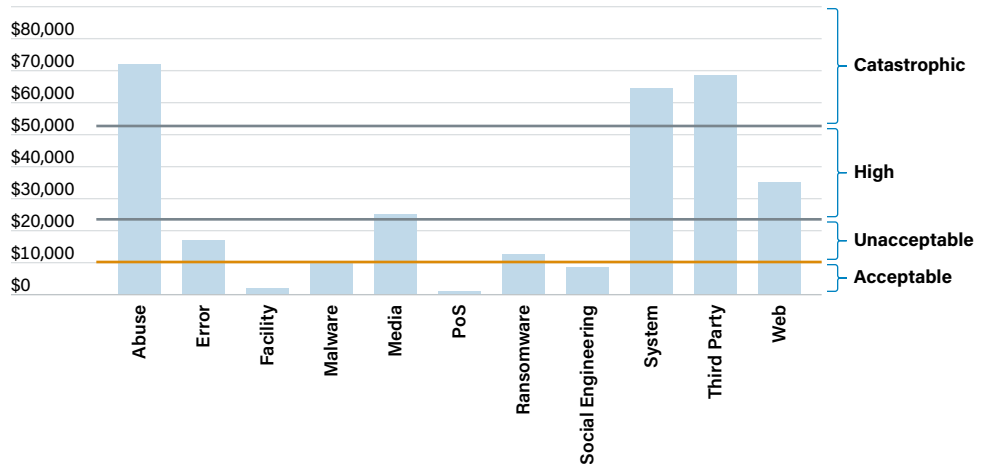
Impact Threshold definitions should describe harm that is equally acceptable or unacceptable for all potentially affected parties. In other words, an Impact Threshold of '3' should describe an impact that is as undesirable to the enterprise's Mission as it would be to their Operational Objectives and their Obligations. Enterprises should establish with their Impact Definition, the understanding that what is negligible, unacceptable, or catastrophic to them must be equal to what is negligible, unacceptable, or catastrophic to others.

Readers will notice variations in how CIS RAM for IG1, IG2, and IG3 use impact criteria. For example, each IG version will provide the option for defining and using "Financial Objectives." This will help enterprises compare budget requests to threshold limits for each magnitude and to ensure that they are comfortable spending some amount of money against the impact they are trying to avoid. Additionally, CIS RAM for IG1 uses only three levels of magnitude to simplify the analysis for IG1 enterprises, whereas CIS RAM for IG2 and IG3 use all five levels of magnitude.

When enterprises use *qualitative* impact estimates, they may use Impact Threshold values as Impact Scores (e.g., if an Impact Threshold of '3' describes the estimated impact of a risk, then the score '3' may be used in the risk analysis).

If enterprises use *quantitative* impact estimates, they may apply Impact Thresholds as bands across ranges of impacts that would be acceptable, unacceptable, high, and catastrophic. This allows enterprises to compare impacts to each other, even if they use dissimilar metrics (whether qualitative estimates using Impact Scores for each Impact Threshold, or a variety of quantitative units, such as dollars, time, percentages of harm, or population counts). Shown below in Figure 1 is an example of how this could be applied.

FIGURE 1. Expressing quantitative risk in Impact Thresholds



Enterprises may also define Expectancy using a five-scale table (or three-scale for IG1 enterprises), or percentages of probability. Expectancy is expressed qualitatively and uses the familiar concept of “foreseeability” to ease estimation and communication, and to adopt the language used by legal authorities and regulators.

TABLE 2. Example qualitative Expectancy definition

The table displays examples only, and is not meant to imply a single, correct model.

EXPECTANCY SCORES	EXPECTANCY SCORES DEFINED
1	Not foreseeable
2	Foreseeable, but unexpected
3	Expected, but not common
4	Common
5	Could be happening now

Enterprises that use percentages of probability may use a similar model, but will want to express foreseeability in terms of probabilistic ranges, as shown below in Table 3.

TABLE 3. Example quantitative Expectancy definition guidelines

The table displays examples only, and is not meant to imply a single, correct model.

EXPECTANCY THRESHOLD	EXPECTANCY THRESHOLD DEFINED
0% / yr	Not foreseeable
< 1% / yr	Foreseeable, but unexpected
>=1% to < 20% / yr	Expected, but not common
>=20% to < 50% / yr	Common
>= 50% / yr	Could be happening now

As of CIS RAM Core v2.1, CIS RAM is migrating to the term “Expectancy” rather than “Likelihood.” “Expectancy” does not imply probability that an incident may happen within a given time period, as “likelihood” and “probability” do. Rather, it implies that we know a security incident will occur, but we expect it to occur via a foreseeable threat. CIS RAM 2.1 automates the estimation of security incidents by comparing the commonality of reported threats to the reliability of Safeguards that would prevent them. Therefore, “expectancy” is a more appropriate term.

Developing the Risk Acceptance Criteria

After using common language terms to describe a variety of Impact Types and Expectancies, enterprises will have the basis for Risk Acceptance. By selecting the minimal Expectancy and Impact that they would want to prevent, they would conversely define risk levels that they would accept. For example, an enterprise that would invest against risks that are "Expected, but not common" (Expectancy is '3') and that would cause an unacceptably high Impact (Impact is '3' or above), their Acceptable Risk Criteria could be stated like this:

TABLE 4. Risk Acceptance Criteria example for qualitative estimates

IMPACT THRESHOLD	×	EXPECTANCY THRESHOLD	=	RISK THRESHOLD
3	×	3	=	9
...therefore...				
Acceptable Risk			<	9

The same enterprise could also express that same Risk Acceptance quantitatively like this (where their acceptable Impact Thresholds are: "12.2% of value loss" for their Mission, "\$10,000" for their Operational Objectives, and "99 people" for their Obligations):

TABLE 5. Risk Acceptance Criteria example for quantitative estimates

	IMPACTS	EXPECTANCY
Mission Impact Threshold	12.2% value loss	< 20% / yr
Operational Objectives Impact Threshold	\$10,000	< 20% / yr
Obligations Impact Threshold	99 people	< 20% / yr

With clearly defined criteria for analyzing and accepting risk, risk assessors may estimate risks using consistent scoring and plain-language statements that are easy to communicate, and simple to calculate and compare.

While enterprises may choose their Risk Acceptance Criteria in versions IG2 and IG3, IG1 provides default Risk Acceptance Criteria of 'below 6' out of '9'.

Modeling the Risks

Risks are modeled by associating information assets with the CIS Safeguards that protect them, the vulnerabilities that may be present, and the threats that may compromise the information assets. While other CIS RAM documents describe different ways to model risks, CIS RAM Core describes the component steps in analyzing risks, regardless of the sequence of those steps.

- 1 Identify an information asset or asset class, such as a specific firewall or a set of similarly managed firewalls, an application, or a set of identically configured servers, etc.
- 2 Identify threats that may compromise the Confidentiality, Integrity, or Availability of those information assets or Asset Classes.
- 3 List CIS Safeguards that would protect the information asset or Asset Class against foreseeable threats.
- 4 Indicate if the CIS Safeguards are implemented in the environment and how they are implemented.
- 5 Consider any vulnerabilities that may exist related to each Safeguard and Asset Class. The risk assessor should take care to consider what may go wrong, even if Safeguards are implemented completely. Errors in administration, new threats, intentional harm, failed systems, and insufficient skills or resources are common vulnerabilities for Safeguards that are completely implemented.

TABLE 6. Risk Assessment threat model guidelines

RISK ANALYSIS	VALUE
CIS Safeguard	Identify a CIS Safeguard from CIS Controls v7.1 or v8.
Description	Describe the CIS Safeguard as written in the CIS Controls.
Information Asset	State the information asset or Asset Class that is being assessed.
Threat	Describe an action that may compromise the asset’s security.
Safeguard	Describe whether and how the CIS Safeguard is applied to the asset.
Vulnerability	State any vulnerabilities that may be exploited by a threat.

At this point, the risk assessor has formed a story about the security of its information assets that should be protected by CIS Controls. Some Controls indicate vulnerabilities that may allow foreseeable threats to compromise the assets. However, the enterprise still needs to know the acceptability and relative importance of the risks. The risk assessor is now ready to estimate the Expectancy and Impact of those risks.

Evaluating the Risks

Since the risk assessor has Impact and Expectancy Criteria already defined, they can select Expectancy and Impact Values based on the descriptions in the definitions.

Estimating Expectancy and Impact can be challenging for many risk assessors. While laws and regulations do not require “accurate” risk forecasting, enterprises are best served by sound estimations. Guidance for estimating Expectancy and Impact is provided in additional documentation in the CIS RAM family of documents.

TABLE 7. Risk Analysis guidelines

RISK ANALYSIS	MEANING
CIS Safeguard #	The unique CIS Safeguard identifier, as published in the CIS Controls.
CIS Safeguard Title	The title of the CIS Safeguard, as published in the CIS Controls.
Implementation Group (IG)	The Implementation Group (IG1, IG2, IG3), as published in the CIS Controls.
Asset Class	The asset class, as published in the CIS Controls.
Asset Name	An optional field used to input the name of an individual asset to distinguish its risks from other Asset Class risks.
Our Implementation	A brief description of how the Safeguard is already implemented and operated in the enterprise.
Evidence of Implementation	Proof to show how the Safeguard is already implemented and operated in the enterprise.
Vulnerabilities	An optional field used to record vulnerabilities with a specific asset.
Safeguard Maturity Score	A score of ‘1’ through ‘5’ designating the reliability of a Safeguard’s effectiveness against threats.
VCDB Index	An automatically calculated value to represent how common the related threat is as a cause for reported cybersecurity incidents.
Expectancy Score	An automatically calculated value to represent how commonly the related threat would be the cause of a cybersecurity incident, given your current Safeguard.
Impact to Mission	The magnitude of harm that a successful threat would cause to your Mission.
Impact to Operational Objectives	The magnitude of harm that a successful threat would cause to your Operational Objectives.
Impact to Financial Objectives	The magnitude of harm that a successful threat would cause to your Financial Objectives.
Impact to Obligations	The magnitude of harm that a successful threat would cause to your Obligations.
Risk Score	The product of the Expectancy and the highest of the three (or four, if using Impact to Financial Objectives) Impacts.
Risk Level	An evaluation of the risk as negligible, acceptable, unacceptable, high, or catastrophic.

Risk Acceptability is automatically determined because the Risk Assessment Criteria had been defined prior to the assessment. Scores below the Risk Acceptance Criteria may automatically be recorded as accepted by management. No ad hoc decisions need to be made.

Recommending CIS Safeguards

Risks that evaluate to unacceptably high scores must be reduced by improving a CIS Safeguard, or by applying a new CIS Safeguard. For example, if a software development team is not well trained and produces vulnerable web applications, they may improve upon CIS Safeguard¹⁰ 16.9 by training their team. Alternatively, they may introduce another CIS Safeguard, such as CIS Safeguard 13.10, by implementing a web application firewall.

Each enterprise and environment will need to make choices about which CIS Safeguard they will use to address a risk, but will also need to evaluate their recommended CIS Safeguards to determine whether they would effectively reduce risks while not creating new, unacceptable risks. That step is taken care of by evaluating the recommendations using the same Risk Assessment Criteria that were used to evaluate the risk.

Evaluating Recommended Safeguards

Risk assessors must be careful to not assume that new Safeguards will necessarily reduce all risks. While improved Controls or new Safeguards may reduce risks in one area (traditionally thought of as “residual risk”), they also potentially create risks in other areas. This is why CIS RAM uses the phrase “Safeguard Risk” instead of “Residual Risk.”

Common examples of Safeguards that increase risks are: new security controls that slow productivity, encouraging personnel to find unsafe workarounds, stringent access controls for information that is needed in critical situations (such as clinical care, emergency response, or monitoring volatile systems and processes), data protections that impede collaboration and research, encryption that prevents monitoring, or controls that are excessively expensive.

These can all be considered “Safeguard Risks” that may harm an enterprise’s Mission, Objectives, and Obligations. All of the CIS Controls that the enterprise would use to address the risks are good controls. However, security practitioners should implement the Controls so that they meet the objective for reducing risks while not posing new risks.

Recommended Safeguards are evaluated similarly to risks, as shown in Table 8 below. Example Risk Registers that evaluate risks and recommendations can be found in workbooks that are provided with each CIS RAM module (for IG1, IG2, and IG3), but there will be variances with how each module evaluates Safeguard Risks.

TABLE 8. Risk Treatment guidelines

RISK TREATMENT	MEANING
Risk Treatment Option	A statement about whether the enterprise will accept or reduce the risk.
Risk Treatment Safeguard	The unique CIS Safeguard identifier, as published in the CIS Controls.
Risk Treatment Safeguard Title	The title of the CIS Safeguard, as published in the CIS Controls.
Risk Treatment Safeguard Description	The description of the CIS Safeguard, as published in the CIS Controls.
Our Planned Implementation	A brief description of how the Safeguard will be implemented and operated in the enterprise.
Risk Treatment Safeguard Maturity Score	A score of ‘1’ through ‘5’ designating the planned reliability of a Safeguard’s effectiveness against threats.
Risk Treatment Safeguard Expectancy Score	An automatically calculated value to represent how commonly the related threat would be the cause of a cybersecurity incident, given the planned Safeguard.
Risk Treatment Safeguard Impact to Mission	The magnitude of harm that a successful threat would cause to your Mission.
Risk Treatment Safeguard Impact to Operational Objectives	The magnitude of harm that a successful threat would cause to your Operational Objectives.
Risk Treatment Safeguard Impact to Financial Objectives	The magnitude of harm that a successful threat would cause to your Financial Objectives.
Risk Treatment Safeguard Impact to Obligations	The magnitude of harm that a successful threat would cause to your Obligations.
Risk Treatment Safeguard Risk Score	The product of the Expectancy and the highest of the three Impacts, given the planned Safeguard.

RISK TREATMENT	MEANING
Reasonable and Acceptable	A determination of whether the planned Safeguard is reasonable and acceptable.
Risk Treatment Safeguard Cost	An estimate of how much the Safeguard is expected to cost.
Implementation Quarter	When the Safeguard is planned for completion of implementation (which quarter).
Implementation Year	When the Safeguard is planned for completion of implementation (which year).

In terms of the acceptability of Safeguard Risks, risk assessors must consider the following:

- 1 As stated in Principle 2, *"Risks must be reduced to a level that would not require a remedy to any party."* Risk assessors automatically adhere to this principle by acknowledging "Safeguard Risk Acceptability."
- 2 Also recall Principle 3, *"Safeguards must not be more burdensome than the risks they protect against."* Risk assessors can determine whether a recommended safeguard is overly burdensome by seeing if the Safeguard Risk is higher than the original risk.

It is generally true that if a Safeguard Risk Score is acceptably low, then it is by default a reasonable treatment for an unacceptably high risk. However, the evaluation of "reasonable" risk treatments remains useful in two important ways:

- 1 Enterprises that choose to reduce an acceptable risk should know whether the Safeguard Risk is higher than the original risk, even if they are both acceptably low. Why try to remedy an acceptable condition by making another condition that is worse?
- 2 If a customer, a client, a legal authority, or a regulator requires a specific safeguard, enterprises can model those safeguards to determine whether they create an unreasonably high burden. Such analysis may provide a convincing case that the requirement would increase risk.

Summary

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

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

Recommended Next Steps

CIS RAM users may develop enough understanding of a DoCRA-based risk assessment by reading this document, reading other documents in the CIS RAM family, and using templates and examples in workbooks that are provided with each CIS RAM module (for IG1, IG2, and IG3). The concepts and processes described in CIS RAM Core may be new and challenging to many users. CIS RAM Core users should, as a next step, read other documents in the CIS RAM family to understand how to model threats, estimate expectancies and impacts, use qualitative and quantitative methods, and align CIS RAM with other risk assessment methods they may already use.

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

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](https://www.cisecurity.org) or follow us on Twitter: [@CISecurity](https://twitter.com/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 organizations 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 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>)

Binary Risk Analysis (BRA)

Binary Risk Analysis is published as version 1.0. The analysis method is presented as a worksheet and an application at the hosting website. The BRA provides risk analysts with a concise and consistent process for evaluating information security risks by breaking down the components of a threat scenario, including the capabilities to defend against variably robust and common threats. (<http://binary.protect.io>)

FAIR Institute

The FAIR Institute maintains and educates risk analysts on the use of Factor Analysis of Information Risk. The FAIR method is similar to BRA in that it provides a consistent method for evaluating information risk based on characteristics of the components of information risks. (<https://www.fairinstitute.org/>)

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

©2022 Center for Internet Security, Inc.

Contact Information

CIS


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

HALOCK Security Labs


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

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](https://cisecurity.org) or follow us on Twitter: @CISecurity.

 cisecurity.org

 info@cisecurity.org

 518-266-3460

 Center for Internet Security

 @CISecurity

 TheCISecurity

 cisecurity