Center for Internet Security®

CIS RAM *Express Edition* Version 1.0

For Rapid Implementation of CIS RAM v1.0

CIS RAM *Express Edition* - Center for Internet Security Risk Assessment Method (Version 1.0)

April 2018

Background and Acknowledgements

The original content of CIS RAM was developed by HALOCK Security Labs. It is based on their extensive experience helping clients and legal authorities deal with cybersecurity and due care issues. Recognizing the universal need for a vendor-neutral, open, industry-wide approach to these issues, HALOCK Security Labs approached CIS to make this work 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 also 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 1 of CIS RAM were made by:

Principal Author:
Chris Cronin. Partner, HALOCK Security Labs

Contributing Authors:
Jim Mirochnik, Terry Kurzynski, and David Andrew, Partners, HALOCK Security Labs. Erik Leach and Steve Lawn, HALOCK Security Labs. Paul Otto, Attorney, Hogan Lovells US LLP.

Review and vetting was provided by multiple members of the CIS staff.

Table of Contents

Forward

The objective of the Center for Internet Security® Risk Assessment Method Express Edition ("CIS RAM Express") and CIS RAM is to help organizations plan and justify their implementation of CIS Controls Version 7, whether those controls are fully or partially operating. Few organizations can apply all controls to all environments and 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 organization'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 Express conforms to and supplements established information security risk assessment standards, such as ISO 27005[1], NIST Special Publications 800-30[2], and RISK IT[3] . By conforming to these standards, CIS RAM Express ensures that the reader will conduct risk assessments according to established standards. By supplementing these standards, CIS RAM Express helps its readers evaluate risks and safeguards using the concept of "due care" and "reasonable safeguards" that the legal community and regulators use to determine whether organizations act as a "reasonable person."

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, CIS Controls V7 has risk considerations at its core.

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

Who is this risk assessment method for?

CIS RAM Express is useful to individuals and organizations who wish to understand the core processes and reasoning found in CIS RAM. CIS RAM Express is also useful for organizations and cybersecurity practitioners who are experienced at assessing risk, and who are able to quickly adopt its methods for their environment.

---

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

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

[3] RISK IT Framework provided by ISACA.

For users who need more direction than what they will find in CIS RAM Express, CIS RAM provides:

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

What this document provides:

The CIS RAM Express is a "bare essentials" version of the CIS RAM that provides fundamental components of the full CIS RAM document to help readers rapidly understand and implement the risk assessment method.

The CIS RAM Express provides a framework for assessing information security risk, including helpful guidance for establishing criteria for risk analysis and risk acceptance, and for evaluating risk using CIS Controls V7.

The reader will need to rely on 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, to define the organization's mission, objectives, and obligations, to decide which risks will be evaluated, to identify vulnerabilities and foreseeable threats, to estimate likelihood and impact, and to recommend risk treatment safeguards.

A supplemental document, CIS_RAM_Workbook provides examples and templates to demonstrate the instructions provided in this document. While the full CIS RAM provides three sets of instructions and examples for three levels of organizational maturity (Tier 1, Tier 2, and Tiers 3 & 4[4]), CIS RAM Express refers only to the instructions and examples for "Tier 2" organizations. Readers should therefore refer to templates and examples for Tier 2 organizations in the CIS_RAM_Workbook.

[4] As defined in, *Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0*, National Institute of Standards and Technology. February 12, 2014

Glossary

Appropriate: A condition in which risks to information assets will not foreseeably create harm that is greater than what the organization or interested parties can tolerate.

Asset Class: A group of information assets that are evaluated as one set based on their similarity. “Servers,” “end-user computers,” “network devices” are examples, as are “email servers,” “web servers” and “authentication servers.”

Attack Path: A series of activities and information assets within the lifecycle of a security incident.

Attack Path Model: A description of how a specific attack path may occur within an environment.

Burden: The negative impact that a safeguard may pose to the organization, or to others.

Business Owners: Personnel who own business processes, goods, or services that information technologies support. i.e. customer service managers, product managers, sales management.

Constituents: Individuals or organizations that may be benefit from effective security over information assets, or may be harmed if security fails.

Control: A documented method for protecting information assets using technical, physical, or procedural safeguards.

Control Objective: The intended outcome of a control.

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.

Impact: The harm that may be suffered when a threat compromises an information asset.

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’.

Impact Type: A category of impact that estimates the amount of harm that may come to a party or a purpose. The CIS RAM describes three impact types; Mission, Objectives, and Obligations.

Information Asset: Information or the systems, processes, people, and facilities that facilitate information handling.

Inherent Risk: The likelihood of an impact occurring when a threat compromises an unprotected asset.

Key Risk Indicator: Aggregations and trending analysis of measures that management may use to understand their risk status.

Likelihood: The degree to which a threat is expected to create an impact. May be stated in terms of frequency, foreseeability, or probability.

Measure: A repeatable, evidence-based indication that a safeguard achieves its control objective.

Observed Risk: The current risk as it appears to the risk assessor.

Probability: The product of statistical analysis that estimates the likelihood of an event.

Reasonable: A condition in which safeguards will not create a burden to the organization 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 potential negative impacts to the organization when safeguards are applied.

Risk: An estimation of the likelihood that a threat will create an undesirable impact. In terms of this method, risk may be expressed as the product of a likelihood and an impact.

Risk Analysis: The process of estimating the likelihood that an event will create an 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 policies 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 likelihood and impact of a risk, and compares it to acceptable risk.

Risk Management: A process for analyzing, mitigating, overseeing, and reducing risk.

Risk Treatment Option: The selection of a method for addressing risks. Organizations may choose to Accept, Reduce, Transfer, or Avoid risks.

Risk Treatment Plan: A comprehensive project plan for implementing risk treatment recommendations.

Risk Treatment Recommendations: A listing of safeguards or processes that may be implemented and operated to reduce the likelihood and/or impact of a risk.

Safeguard: Technologies, processes, and physical protections that prevent or detect threats against information assets. Safeguards are implementations of controls.

Safeguard Risk: The risk posed by recommended safeguards. An organization's mission or objectives may be negatively impacted by a new security control. These impacts must be evaluated to understand their burden on the organization, 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 organization and its constituents.

Steward: Personnel who are responsible for the security and proper operations of information assets, (e.g. database administrator, records manager, or network engineer).

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.

CIS RAM Express Edition

Principles and Practices

CIS RAM *Express Edition* uses the Duty of Care Risk Analysis Standard[5] ("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 ten 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 ten practices describe features of risk assessments that make the three principles achievable.

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 authorities and potentially affected parties would find appropriate.
3. Safeguards must not be more burdensome than the risks they protect against.

Practices

1. Risk analysis considers the likelihood that certain threats could create magnitudes of impact.
2. Risks and safeguards are evaluated using the same criteria so they can be compared.
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 numeric 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.

---

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

10. Risk assessments cannot evaluate all foreseeable risks. Risk assessments re-occur to identify and address more risks over time.

Risk Assessment Process

CIS RAM Express 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 Controls that would prevent or detect foreseeable threats.
- Evaluating the Risks: Estimate the likelihood and impact of security breaches to arrive at the risk score, then determine whether identified risks are acceptable.
- Recommending Safeguards: Propose CIS Controls that would reduce unacceptable risks.
- Evaluating Recommended Safeguards: Risk-analyze the recommended safeguards to ensure that they pose acceptably low risks without creating an undue burden.

Developing the Risk Assessment Criteria

CIS RAM Express evaluates risk using "Risk = Impact x Likelihood." This calculation will evaluate both currently observed risks and recommended safeguards so 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 "likelihood." Readers should refer to *CIS_RAM_Workbook* for criteria examples.

Impacts will consider the organization's mission (the benefit that interested parties gain from the organization), their objectives (the organization'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 Definition Guidelines

Impact Score	Impact to Mission *State the organization's mission*	Impact to Objectives *State the organization's objectives*	Impact to Obligations *State harm that may come to others.*
1	Describe a negligible impact to the mission.	Describe a negligible impact to the objectives.	Describe a negligible impact to the obligations.
2	Describe an acceptable impact to the mission.	Describe an acceptable impact to the objectives.	Describe an acceptable impact to the obligations.
3	Describe an unacceptable impact to the mission.	Describe an unacceptable impact to the objectives.	Describe an unacceptable impact to the obligations.
4	Describe a high impact to the mission.	Describe a high impact to the objectives.	Describe a high impact to the obligations.
5	Describe an unrecoverable impact to the mission.	Describe an unrecoverable impact to the objectives.	Describe an unrecoverable impact to the obligations.

Impact magnitude definitions should describe harm that is equally acceptable or unacceptable for all potentially affected parties. In other words, an impact score of '3' should describe an impact that is as undesirable to the organization's mission as it would be to their objectives and their obligations. Organizations 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.

Organizations may also define likelihood using a five-scale table. Likelihood scoring uses the familiar concept of "foreseeability" to ease estimation and communication, and to adopt the language used by legal authorities and regulators. The full CIS RAM describes techniques for using analysis such as probability to refine likelihood estimation.

Table 2 - Likelihood Definition Guidelines

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

Developing the Risk Acceptance Criteria

Organizations will now have the basis for risk acceptance. By selecting the likelihood of an impact that they would start to invest against, they would conversely define risk levels that they would accept. For example, an organization that would invest against risks that are "Expected, but not common" (Likelihood 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 3 - Risk Acceptance Criteria Example

Impact Threshold	x	Likelihood Threshold	=	Risk Threshold
3	x	3	=	9
… therefore …				
Acceptable Risk			**<**	**9**

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

Modeling the Risks

Risks are modeled by associating information assets with the CIS Controls that protect them, the vulnerabilities that may be present, and the threats that may compromise the information assets. While the full CIS RAM document describes three different ways to model risks, CIS RAM Express describes the method associated with "Tier 2" organizations.

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. List the CIS Controls that would be appropriate for protecting that information asset or asset class.
    a. This may lead to tens of controls for each information asset or asset class which would quickly overwhelm most organizations. The organization may reduce its effort by first performing a simple “Tier 1” risk assessment as described in CIS RAM. This enables them to first evaluate all CIS Controls as they are generally applied to the environment, then only evaluating specially configured controls for each asset.
3. Describe whether and how the controls are implemented in the environment.
4. Consider any vulnerabilities that may exist related to each control. The risk assessor should take care to consider what may go wrong, even with controls that are implemented completely. Errors in administration, new threats, intentional harm, failed systems, and insufficient skills or resources are common vulnerabilities for controls that are completely implemented.
5. Identify threats that could compromise the information assets or asset classes because of the vulnerabilities.

Table 4 - "Tier 2" Risk Assessment Threat Model Guidelines

Risk Analysis	Value
CIS Control	Identify a control from CIS Controls V7.
Description	Describe the controls as written in CIS Controls.
Information Asset	State the information asset or asset class that is being assessed.
Control	Describe whether and how the CIS Control is applied to the asset.
Vulnerability	State any vulnerabilities that may be exploited by a threat.
Threat	Describe an action that may compromise the asset’s security.

At this point, the risk assessor has formed a story about the security of its information assets: A set of valuable assets should be protected by CIS Controls. Some controls indicate vulnerabilities that may allow foreseeable threats to compromise the assets. But the organization still needs to know the acceptability and relative importance of the risks. The risk assessor is now ready to estimate the likelihood and impact of those risks.

Evaluating the Risks

Because the risk assessor has impact and likelihood criteria already defined, they can select likelihood and impact values based on the descriptions in the definitions.

Estimating likelihood and impact can be challenging for many risk assessors. While laws and regulations do not require “accurate” risk forecasting, organizations are best served by sound estimations. Guidance for estimating likelihood and impact is provided in the “Risk Analysis Techniques” chapter of CIS RAM, and includes method for systematic heuristics, and integration with probability analysis.

Table 5 - "Tier 2" Risk Evaluation Guidelines

Risk Analysis	Value
Threat Likelihood	Estimate the likelihood of the compromise (1 - 5).
Mission Impact	Estimate the impact to the mission that would result (1 - 5).
Objectives Impact	Estimate the impact to the objectives that would result (1 - 5).
Obligations Impact	Estimate the impact to the obligations that would result (1 - 5).
Risk Score	Multiply the likelihood score by the highest impact score.
Risk Acceptability	Risk acceptability of the risk score is automatically determined.

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 recorded as accepted by management. No ad hoc decisions need to be made.

Recommending Safeguards

Risks that evaluate to unacceptably high scores must be reduced by improving a control, or by applying new controls (known as “safeguards” when used for risk treatment). For example, if a software development team is not well trained and produces vulnerable web applications they may improve CIS Control 18.6 by training their team, or they may introduce another safeguard such as a web application firewall according to CIS Control 18.10.

Each organization and environment will need to make choices about which CIS Control they will use to address a risk, but will also need to evaluate their recommended controls 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 work-arounds, 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 organization’s mission, objectives, and obligations. All of the CIS Controls that the organization would use to address the risks are good controls. But 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 the table below. Example risk registers that evaluate risks and recommendations can be found in *CIS_RAM_Workbook.*

Table 6 - "Tier 2" Safeguard Evaluation Guidelines

Risk Analysis	Value
Risk Score	The score of the original risk evaluation.
Risk Acceptability	Risk acceptability of the original risk score.
Recommended Safeguard	Describe how a CIS Control will be used to address the risk.
Safeguard Risk	Identify new risks to the mission, objectives, or obligations.
Safeguard Threat Likelihood	Estimate the likelihood that the safeguard risk would occur.
Safeguard Mission Impact	Estimate the impact to the mission that would result (1 - 5).
Safeguard Objectives Impact	Estimate the impact to the objectives that would result (1 - 5).
Safeguard Obligations Impact	Estimate the impact to the obligations that would result (1 - 5).
Safeguard Risk Score	Multiply the likelihood score by the highest impact score.
Safeguard Risk Acceptability	Risk acceptability of the risk score is automatically determined.

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 all potentially affected parties would find appropriate*. 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 remain useful in two important ways:

1. Organizations 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's worse?
2. If a customer, a client, a legal authority, or a regulator requires a specific safeguard, organizations 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 and CIS RAM *Express Edition* provide a model of cybersecurity risk analysis that helps organizations 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.

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

Recommended Next Steps

CIS RAM Express readers may develop enough understanding of a DoCRA-based risk assessment by reading this document, and using templates and examples that are provided in *CIS_RAM_Workbook*. However, the concepts and processes described in CIS RAM *Express Edition* will be new and challenging to many readers. CIS RAM *Express Edition* readers should as a next step read the full CIS RAM document, and follow its guidance and exercises to create their risk assessment.

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

Helpful Resources

CIS (Center for Internet Security)
CIS (Center for Internet Security, Inc.) is a forward-thinking, non-profit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats. Our CIS Controls™ and CIS Benchmarks™ are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continuously refined and verified by a volunteer, global community of experienced IT professionals. CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities. (www.cisecurity.org)

HALOCK Security Labs
Established in 1996, HALOCK Security Labs is an information security professional services firm based in Schaumburg, IL. 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 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 approaches 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 sub-categories of controls with those of other control documents, including the CIS 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. (http://www.isaca.org/Knowledge-Center/Risk-IT-IT-Risk-Management/Pages/default.aspx)

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
Fair Institute maintains and educates risk analysists 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.

Contact Information

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

HALOCK Security Labs
1834 Walden Office Sq. Ste 200
Schaumburg, IL 60173
847.221.0200
cisram@halock.com