CIS RAM V2.1

For Reasonable Implementation of the CIS Critical Security Controls

From The Center for Internet Security, Inc. (CIS®) and HALOCK Security Labs, CIS Risk Assessment Method (RAM) now simplifies your path toward reasonable security with evidence-based guidance.

HALOCK®

CIS® Center for Internet Security®

CIS Controls®

What is "Reasonable" Security?

If you are breached and your case goes to litigation, you will be asked to demonstrate "due care." This is the language judges use to describe "reasonableness." Enterprises must use safeguards to ensure that risk is reasonable to the enterprise and appropriate to other interested parties at the time of the breach. CIS RAM can help your enterprise demonstrate "due care."

What is CIS RAM?

CIS and HALOCK Security Labs have co-developed the CIS Risk Assessment Method (RAM) to help enterprises justify investments for reasonable implementation of the CIS Controls. CIS RAM helps enterprises define their acceptable level of risk, and to prioritize and implement the CIS Controls to manage that risk.

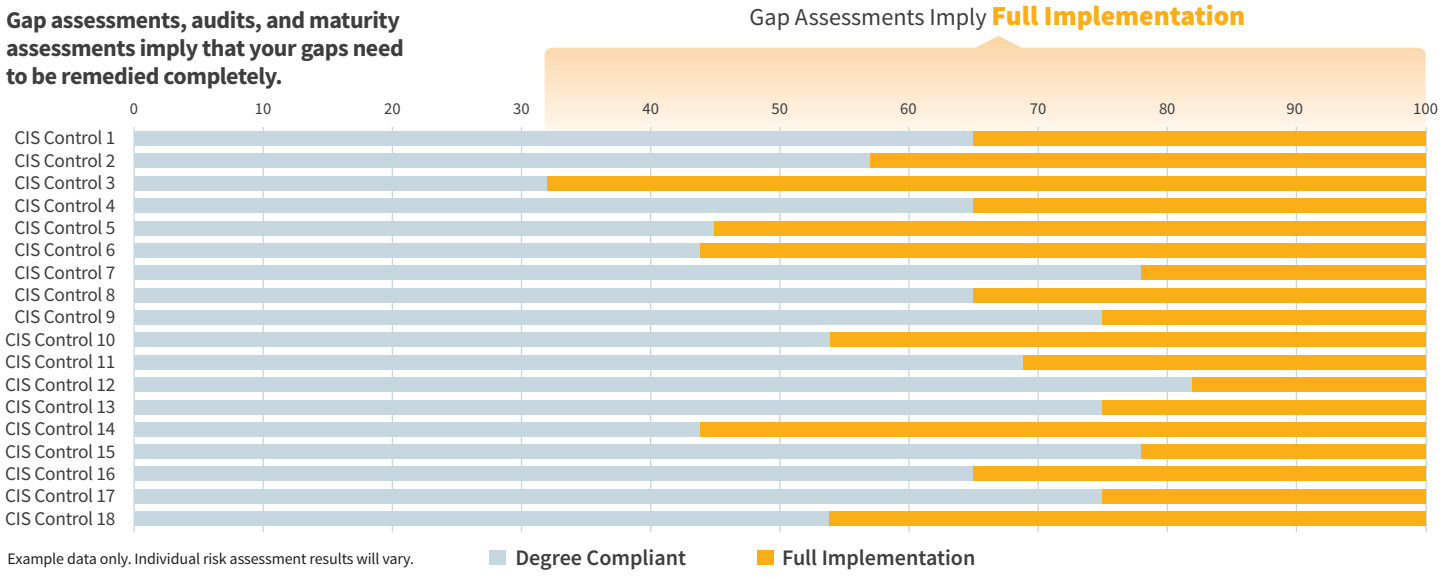
An Industry with Many Interested Parties – Each with a Unique Set of Challenges

Information security professionals need to satisfy many interested parties, all of which have vastly different concerns. Addressing the concerns of these interested parties creates a set of unique challenges.

THE PROBLEM

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

Gap assessments, audits, and maturity assessments imply that your gaps need to be remedied completely.



Example data only. Individual risk assessment results will vary.

CIS RAM is the Solution

CIS RAM addresses these challenges in the following ways:

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

New in CIS RAM 2.1

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

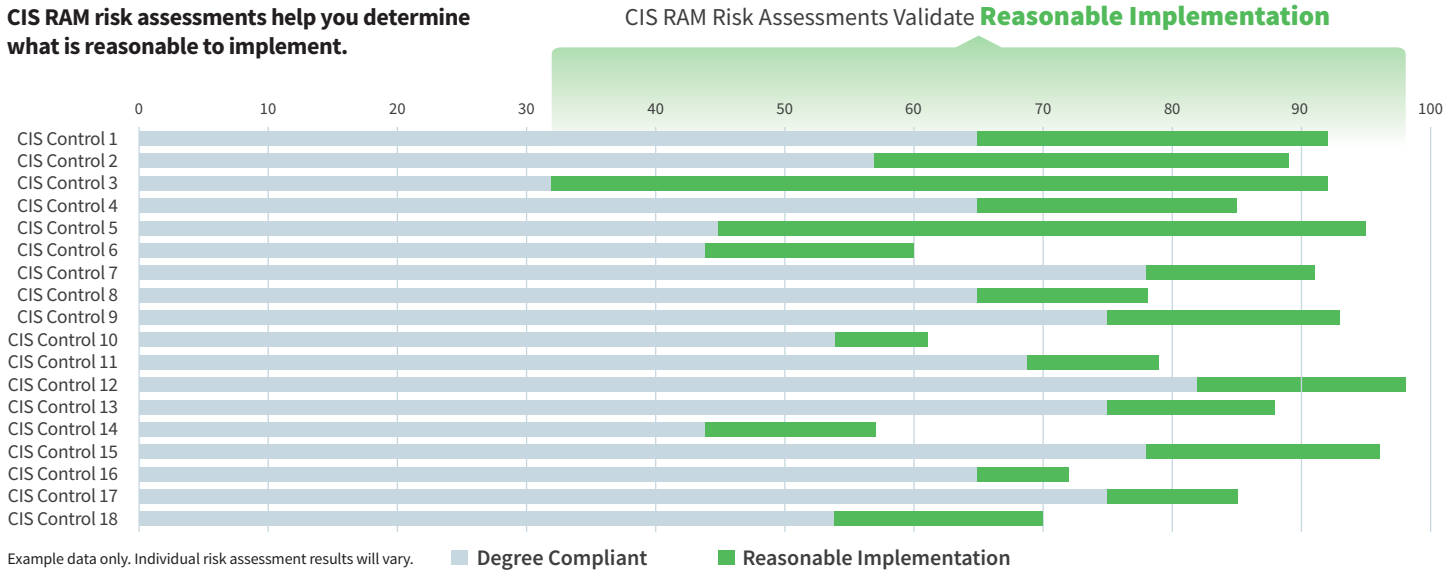
CIS RAM Helps You Apply the Right Amount of Security

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

THE SOLUTION

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

CIS RAM risk assessments help you determine what is reasonable to implement.



Duty of Care in Action

In the case of a security breach and litigation, or regulatory audit, your enterprise's security certifications (PCI DSS, ISO 27001, etc.) may help, but your ability to prove due care through a strong Risk Assessment will matter even more.

Case 1

Pennsylvania Office of Attorney General states CIS RAM's principles as an indication of reasonable security in two settlements. The Commonwealth required Orbitz/Expedia and Earl Enterprises to evaluate risk to themselves and to others, and to balance costs of controls against risks.

Case 2

The Sedona Conference issued its *Commentary on a Reasonable Security Test*. The influential think tank's paper demonstrates to lawyers and regulators how CIS RAM can be used to determine the reasonableness of security controls.

Case 3

After drawing the attention of the Department of Health and Human Services for a HIPAA violation, a mid-sized hospital chain showed the Department how their CIS RAM risk analysis balanced patient safety and privacy against the cost of controls. The Department decided to not pursue formal monitoring.

About CIS RAM

CIS RAM was authored by HALOCK Security Labs in partnership with the CIS to establish reasonable implementation of the CIS Controls. By leveraging CIS RAM, enterprises can methodically build what is reasonable and appropriate security safeguards ("reasonable" controls) for their specific environment. Not only does CIS RAM provide standardized methods to achieve compliance, but it also ensures enterprises devote the right amount of resources to maintain security.

About HALOCK

HALOCK is a U.S.-based risk management and information security consultancy that is privately owned and operated out of its headquarters in Schaumburg, IL. From mid-sized to the Fortune 100, HALOCK'S clients span a variety of industries including financial services, healthcare, legal, education, energy, SaaS/cloud, enterprise retail, and many others. HALOCK strives to be your security partner, providing both strategic and technical security offerings. HALOCK combines strong thought leadership, diagnostic capabilities, and deep technical expertise with a proven ability to get things done. HALOCK helps clients prioritize and optimize their security investments by applying just the right amount of security to protect critical business assets while satisfying compliance requirements and corporate goals.

About 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 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.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

halock.com

CIS. Center for Internet Security®

CIS
31 Tech Valley Drive
East Greenbush, NY 12061
518-266-3460

cisecurity.org