Duty of Care in Action

In the case of a security breach and litigation, or regulatory audit, your organization'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

Although a major retailer successfully achieved information security certifications (PCI DSS), a US District Court permitted banks to sue the retailer after determining that **due care** was not achieved. In other words, "reasonable" controls were not in place to prevent a foreseeable negative impact to the banks and the public.

Case 2

The Federal Trade Commission (FTC) has consistently required since 2002 "the design and implementation of reasonable safeguards to control the risks identified through risk assessment." A Risk Assessment (such as the CIS RAM), and appropriate risk treatment, is required by the FTC even if there are other security certifications in place.

Case 3

A major medical center was being sued for not appropriately protecting information. A Superior Court utilized the "duty of care" balance test and found that the medical center was in the right, and that they did not have a duty to protect breached employees.

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
844-570-4666

halock.com

CIS Center for Internet Security®

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

cisecurity.org

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, organizations 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 organizations devote the right amount of resources to maintain security.

About HALOCK

HALOCK is a U.S.-based 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

Center for Internet Security, Inc. (CIS®) 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.

CIS RAM

For "Reasonable" Implementation of the CIS Controls

CIS (Center for Internet Security) and HALOCK Security Labs are providing the CIS Risk Assessment Method (CIS RAM) to help organizations implement the CIS Controls reasonably.

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 "reasonable." Organizations must use safeguards to ensure that risk is reasonable to the organization and appropriate to other interested parties at the time of the breach. The CIS RAM method can help your organization demonstrate "due care."

What is CIS RAM?

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

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 likelihood of an impact to customers, business objectives, and external entities (regulators, vendors, etc.).
- CIS RAM provides a method to "draw a line" at an organization'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 organizations with a concise and defendable process to accept or address risk.

Justification for CIS RAM

- Helps organizations prioritize and implement CIS Controls reasonably.
- Provides a method to develop risk criteria that demonstrates **due care** as expected by authorities.
- Creates consensus among interested parties.
- Provides instructions, worksheets, and exercises to guide you through your risk assessment. Three different sets of materials support the tiers of risk maturity found in the NIST Cybersecurity Framework.
- Integrates with **CIS Community Attack Model** to model complex threats.

The 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 organizations face. Too often organizations rely on gap assessments to determine the severity of their vulnerabilities. **The CIS RAM enables you to apply just the right amount of security — not too much, not too little** — striking a balance between keeping you safe and ensuring your organization 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 rise calculations, and translate risks into prioritized initiatives.
Attorneys / Judges ➡	CIS RAM allows you to achieve a **reasonable** implementation of 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 organization agreed to.