



# CIS RAM: This Math Will Save You

Presented by: Chris Cronin  
HALOCK Security Labs

August 29, 2018

# Chris Cronin

- Partner at HALOCK Security Labs
- Chair, the DoCRA Council
- Principal Author of [CIS RAM](#) and [DoCRA Standard](#)
- Information Security Focus for 15 Years
  - Risk Analysis
  - Risk Management
  - Incident Response
  - Fraud Investigations
  - Governance
  - ISO 27001 Certifications

# Purpose of Today's Presentation

- Everyone needs a risk assessment.
- Your risk assessment must be based on your Duty of Care or you are exposed.
- CIS<sup>®</sup> has published a method based on **Duty of Care Risk Analysis (“DoCRA”)** to protect you.



**ALTERNATIVE  
TITLE**

# The Questions a Judge Will Ask You the Day You Are Sued for a Data Breach

Presented by: Chris Cronin  
HALOCK Security Labs

August 29, 2018



**ALTERNATIVE  
TITLE**

# Translating Cyber Security For the Board Room

Presented by: Chris Cronin  
HALOCK Security Labs

August 29, 2018



**ALTERNATIVE  
TITLE**

# How Your Security Assessments Annoy Your Regulator

Presented by: Chris Cronin  
HALOCK Security Labs

August 29, 2018

# How Current Security Assessments Are Failing Us

Evaluates Risk to Information Assets

Evaluates Due Care

Method	Evaluates Risk to Information Assets						Evaluates Due Care		
	Standard of Care	Identifies Vulnerabilities	Considers Threats	Evaluates Harm to Self	Evaluates Harm to Others	Estimates Likelihood	Defines Acceptable Risk	Defines Reasonableness	Evaluates Safeguard Risk
<b>DoCRA</b> CIS RAM	●	●	●	●	●	●	●	●	●
<b>IT Risk Assessments</b> ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◐	●	○	○	◐
<b>FAIR</b> Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
<b>Gap Assessments</b> Audits, "Yes/No/Partial"	●	◐	○	○	○	○	○	○	○
<b>Maturity Model Assessments</b> CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

# CIS RAM



## CIS RAM Version 1.0 Center for Internet Security® Risk Assessment Method

For Reasonable Implementation  
Evaluation of CIS Controls™

Version 1.0 – April 2018

**Community Attack Model (Top)** The Community Attack Model (top) aligns the actions within an attack path with CIS Controls that would prevent or detect the actions. If users find in their environment correlations between CIS Controls and the Community Attack Model cells, they should add those controls.

**Attack Path Models (Bottom)** Attack Path Models name foreseeable attacks, and describe the threats against assets that would occur in the attack path.

CIS Community Attack Model	Initial Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
<b>Identify</b>	control of HW, SW inventory, Network logs	threat intelligence		control of administrative privilege	control of HW, SW inventory				Incident Response - Planning
<b>Protect</b>	firewall, mail gateway filtering, web filtering, manage ports, protocols, services, continuous vulnerability assessment	hardened configurations	continuous vulnerability assessment, firewall, mail gateway filtering, web filtering, secure remote access, HPS	patching, hardened configurations, HPS, anti-malware, containerization, app whitelisting, Data Execution Protection	control of admin privilege, data security, hardened configuration, continuous vulnerability assessment	control of admin privilege, NW segmentation, Manage ports, protocols, services	control of admin privilege, patching, hardened configurations, anti-malware, NW segmentation	egress filtering, control of HW, SW inventory	egress filtering, NW segmentation, data security
<b>Detect</b>	firewall, honeypot, Network authentication, Network logs	audit logs, threat intelligence	audit logs, Anti-malware, Network Intrusion Detection system	HPS, anti-malware, containerization, app whitelisting, Data Execution Prevention	account monitoring, control of admin privilege, audit logs, Configuration Monitoring	account monitoring, audit logs, Network Monitoring	audit logs, Network Monitoring	NW IDS, Host Intrusion Prevention	Data Execution Prevention, HPS, Network Monitoring
<b>Respond</b>	honeypot			Incident Response - Execution, Management, Account	Incident Response - Execution, control of HW, SW inventory			sinkhole	Incident Response - Execution



Table 44 – Example Impact Definitions

Impact Score	Impact to Mission	Impact to Objectives	Impact to Obligations
	<b>Mission:</b> Provide information to help remote patients stay healthy.	<b>Objective:</b> Operate profitably.	<b>Obligations:</b> Patients must not be harmed by compromised information.
1	Patients continue to access helpful information, and outcomes are on track.	Profits are on target.	Patients do not experience loss of service or protection.
2	Some patients may not get all the information they need as they request it.	Profits are off target, but are within planned variance.	Patients may be concerned, but not harmed.
3	Some patients cannot access the information they need to maintain good health outcomes.	Profits are off planned variance and may take a fiscal year to recover.	Some patients may be harmed financially or reputationally after compromise of information or services.
4	Many patients consistently cannot access beneficial information.	Profits may take more than a fiscal year to recover.	Many patients may be harmed financially or reputationally.
5	We can no longer provide helpful information to remote patients.	The organization cannot operate profitably.	Some patients may be harmed financially, reputationally, or physically, up to and including death.

Also recall that impact definitions for Tier 2 organizations include criteria for the organization's objectives because those organizations generally benefit from collaboration with business management who are invested in the success of the information security program. These managers often bring to the discussion the organization's strategic and tactical goals for success. But also note that this impact definition contains five magnitudes of impact. Five impact scores help Tier 2 organizations refine their impact estimates in more tangible terms than tables with three scoring levels, and help them refine their risk scoring to better distinguish between risks of varying priority. Acceptable impact scores of '1' and '2' are shaded to set them apart from higher, unacceptable impact scores.

Likelihoods were similarly defined with five potential scores for similar reasons, as shown in Table 45.

Table 45 – Example Likelihood Definitions

Likelihood Score	Foreseeability
1	<b>Not foreseeable.</b> This is not plausible in the environment.
2	<b>Foreseeable.</b> This is plausible, but not expected.
3	<b>Expected.</b> We are certain this will eventually occur.
4	<b>Common.</b> This happens repeatedly.
5	<b>Current.</b> This may be happening now.

The organization believes that the threat model they documented above – that hackers could hack into diary device controllers using something similar to a Blueborne attack - is foreseeable, and perhaps may be expected to occur. While the scenario would likely not be expected for most organizations, our example organization operates in environments where competitors and

Version 1.0 – April 2018

67

Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Establish Persistence	Execute Mission Objectives
Users may click data providers	Attempts at running scripts or direct reference to commands and data objects on the web application, such as SQL injection.	Data exfiltration through the web app, or data exfiltration directly from the database server.	Not applicable	Not applicable	Not applicable	Not applicable	Data exfiltration through the web app, or data exfiltration directly from the database server.
Web application	Asset: Web application, application server, database server, and event logs.	Asset: Database server, application server.					Asset: Database server, application server.
May kube application	Attempts at running scripts or direct reference to commands and data objects on the web server, such as bash.	Commands executed through application account. Files added, altered, or reduced.	Execution of sudo or su, establishment or alteration of existing account.	Directory traversal at the web server.	Commands at the application server.	Installation of executables, establishment of new accounts.	Initiation of executables, daemons, services, processes.
Web application	Asset: Application server, database server, and event logs.	Asset: Application server, database server, and event logs.	Asset: User accounts, administrative accounts.	Asset: Application server, event logs.	Asset: Application server, event logs.	Asset: Operating systems, event logs, user accounts, administrative accounts.	Asset: Executable processes, daemons, services, event logs.
Users may click and trust target	Hacker sends phishing email to selected personnel.	Personnel open phishing email and trigger an install of the ransomware payload.	Malware encrypts the local storage volume.	Not applicable	Not applicable	See Misuse/Escalate Privilege.	Hackers require payment for release of information back to us.
Web application	Asset: Email server, SMTP gateway.	Asset: Email client, end-user OS, personnel, proxy server, advanced malware appliance.	Asset: End-user OS, storage volume.				Asset: Out of our control.



# What is CIS RAM?

- Detailed instructions for conducting cyber security risk assessments.
- Instructions for defining acceptable risk.
- Aligned with judicial and regulatory understanding of “reasonable” and “appropriate.”
- Workbook with templates and examples.
- Based on new **Duty of Care Risk Analysis** (“DoCRA”) standard.

# Where You'll See CIS RAM / DoCRA

- Announced by CIS in April, 2018.
- SANS Institute and CIS Posters.
- Law suits by states' Attorneys General after security breaches.
- Adoption by MS-ISAC member states.
- Other adoption steps in progress ...

# CIS RAM and DoCRA 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.

# Being Judged



# Oops

- How do *you* determine when cyber security risk is acceptable?
- What if that's your judge?
- What if that's your regulator?
- What if that's your CEO or a Board Director?
- Not a comfortable feeling, right?

# What is Risk Analysis?

- **Risk Analysis:** What is the likelihood of harm to ourselves and others that is caused by a threat?
- **Acceptable risk:** The likelihood of harm that ourselves and others would accept.

# Let's Illustrate ... *simple*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Profit plan is on track</i>	<i>No financial harm</i>
<u>Unacceptable</u>	<i>Not profitable</i> 	<i>Money lost or credit rating hurt</i> 

# Let's Illustrate ... *terrible*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Up to \$5,000,000</i>	<i>Up to \$5,000,000</i>
<u>Unacceptable</u>	<i>Over \$5,000,000</i>	<i>Over \$5,000,000</i>

**DON'T ASSUME OTHERS' RISK TOLERANCE EQUALS YOURS!**

# Let's Illustrate ... *simple*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Acceptable</u>	<i>Profit plan is on track</i>	<i>No financial harm</i>
<u>Unacceptable</u>	<i>Not profitable</i>	<i>Money lost or credit rating hurt</i>

Be Prepared to  
Compare Unlike Things

# Let's Illustrate ... *practical*

	<u>Our Profit</u>	<u>Customer Financial Privacy</u>
<u>Negligible</u>	<i>Profit plan is unaffected.</i>	<i>No financial harm.</i>
<u>Acceptable</u>	<i>Profit plan within planned variance.</i>	<i>Encrypted or unusable information cannot create harm.</i>
<u>Unacceptable</u>	<i>Not profitable. Recoverable within the year.</i>	<i>Recoverable money lost or credit rating hurt among few customers.</i>
<u>High</u>	<i>Not profitable. Recoverable in multiple years.</i>	<i>Financial harm among many customers.</i>
<u>Catastrophic</u>	<i>Cannot operate profitably.</i>	<i>Cannot protect customers from harm.</i>

# Establishing Impact Definitions

- To evaluate balance well, define these things:
  - Your **Mission**:  
What makes the risk worth it for others?
  - Your **Objectives**:  
What are your indicators of success?
  - Your **Obligations**:  
What care do you owe others?

# Some Common Impact Criteria

Industry Example	Mission	Objectives	Obligations
<b>Commercial Bank</b>	Financial performance	Return on assets	Customer financials
<b>Hospital</b>	Health outcomes	Balanced budget	Patient privacy
<b>University</b>	Educate students	Five year plan	Student financials
<b>Manufacturer</b>	Custom products	Profitability	Protect customer IP
<b>Electrical generator</b>	Provide power	Profitability	Public safety

# Bank's Full Risk Assessment Criteria

Impact Score	Mission "Financial Performance"	Objectives "Return on Assets"	Obligation "Customer Financials"
1. Negligible	Customer returns at or above market.	Maintain RoA targets.	Customer finances not harmed.
2. Low	Customer returns at market by end of fiscal year.	RoA performance within planned variance.	Customer info released, but cannot cause harm.
3. Medium	One product underperforms against market after a year.	Missed RoA targets up to 1%	Recoverable harm caused to few customers.
4. High	Multiple products under perform for multiple years.	Missed RoA targets up to 5% for multiple years.	Recoverable harm caused to thousands or more customers.
5. Catastrophic	Cannot meet market returns.	Cannot earn sufficient RoA to operate.	We cannot safeguard financial information.

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Foreseeable but unexpected
3	Expected, but rare
4	Expected occasionally
5	Common

Plain Language	Score
Invest against risk	3 x 3 = <u>9</u>
<b>Accept Risk</b>	< <u>9</u>

# Hospital's Full Risk Assessment Criteria

Impact Score	Mission "Health Outcomes"	Objectives "Balanced Budget"	Obligation "Patient Privacy"
<b>1. Negligible</b>	Health outcomes would not be effected.	Budget would not be effected.	Patients' privacy would not be harmed.
<b>2. Low</b>	Patients would feel inconvenienced.	Budget performance within planned variance.	Patients would be concerned, but no harm would result.
<b>3. Medium</b>	Some patient's health outcomes would suffer.	Budget variance would be recoverable within a year.	Few patients would suffer reputational or financial harm
<b>4. High</b>	Many patient health outcomes would suffer.	Budget would be recoverable after multiple years.	Many patients would suffer reputational or financial harm.
<b>5. Catastrophic</b>	Patients could not rely on positive health outcomes.	We would not be able to financially operate.	We would not be able to safeguard patient information.

Likelihood Score	Likelihood Definition
1	Not foreseeable
2	Foreseeable but unexpected
3	Expected, but rare
4	Expected occasionally
5	Common

Plain Language	Score
Invest against risk	$3 \times 2 = \underline{6}$
<b>Accept Risk</b>	$< \underline{6}$

# Hey! You're Using Ordinals!

- “Selecting values ‘1’ through ‘5’ may be simple, but they do not indicate probability.”
- CIS RAM and DoCRA can be conducted using probability analysis too.
  - Just stick with the principles and practices listed in CIS RAM and the DoCRA Standard.

# Example 1 – Inappropriate Risk

CIS Control 1.1 - Utilize an Active Discovery Tool			
Asset	All routable devices	Owner	IT
Vulnerability	Sporadic asset scans	Threat	Undetected compromised systems
Risk Scenario	Irregular asset scans may not identify compromised systems that join the network and attack routable systems.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 2		➡ 3	➡ 3
Likelihood		Risk Score: Max(Impact) x Likelihood	
➡ 3		9	

Safeguard	Implement NAC, and a system assessment process for alerted devices.		
Safeguard Risk	A moderate cost would have minimal impact on the budget. Installation of the tool is likely not disruptive.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 1		➡ 2	➡ 1
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
➡ 4		8	

# Example 2 – Unreasonable Safeguard

Control 14.4 - Encrypt All Sensitive Information in Transit			
Asset	Web applications	Owner	Product Management
Vulnerability	Inter-server PII in plain text	Threat	Sniffers can capture PII
Risk Scenario	Hackers place packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 3		➡ 3	➡ 4
Likelihood		Risk Score: Max(Impact) x Likelihood	
➡ 3		12	

Safeguard	Encrypt all data between application servers and database servers.		
Safeguard Risk	IPS would not be able to inspect inter-server data to detect attacks or exfiltration.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 3		➡ 3	➡ 4
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
➡ 4		16	

# Example 3 – Reasonable Safeguard

Control 14.4 - Encrypt All Sensitive Information in Transit			
Asset	Web applications	Owner	Product Management
Vulnerability	Inter-server PII in plain text	Threat	Sniffers can capture PII
Risk Scenario	Hackers place packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 3		➡ 3	➡ 4
Likelihood		Risk Score: Max(Impact) x Likelihood	
➡ 3		12	

Safeguard	Create a VLAN limited to the application server, database server, IPS sensor.		
Safeguard Risk	Promiscuous sniffer would be detected by IPS if on those servers.		
Mission Impact		Objectives Impact	Obligations Impact
➡ 1		➡ 2	➡ 1
Likelihood		Safeguard Risk Score: Max(Impact) x Likelihood	
➡ 4		8	

# Why do Judges Like Duty of Care Risk Analysis?

- Gives judges a clear-cut definition of whether a defendant was negligent.
- Judges by law have to balance the defendant's burden against harm to others.
- Encoded as the “Hand Rule” or “Calculus of Negligence.”
  - A risk is reasonable if “Burden < Probability x Likelihood”
- Multi-factor balancing tests are how **duty of care** and **due care** are determined.

# Multi-Factor Balancing Tests Used in Courts

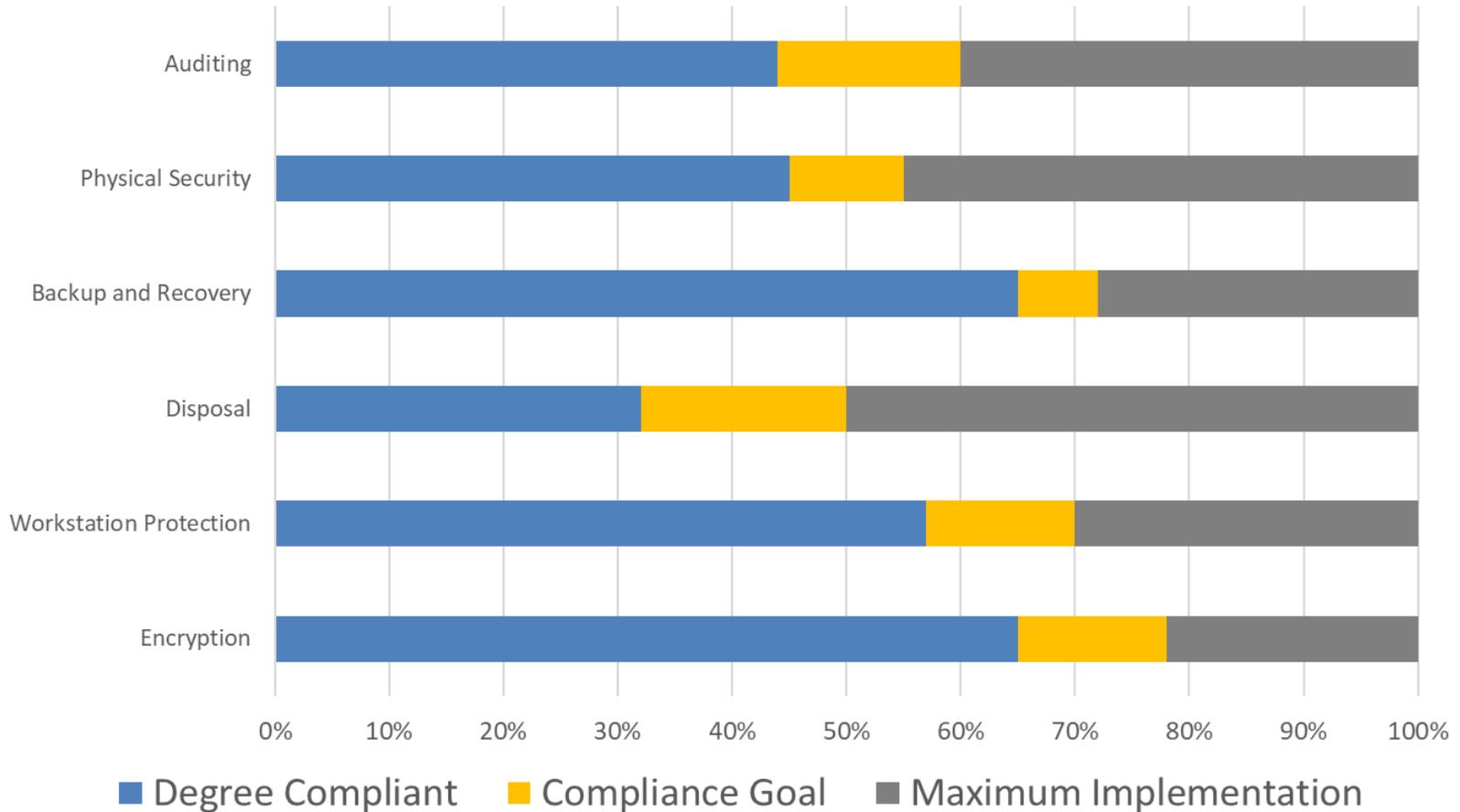
- What controls and vulnerabilities were in place?
- What was the impact and likelihood of the defendant's harm?
- What was the plaintiff's relationship to the defendant?
- What benefit came with the risk?
- Were alternative safeguards evaluated?
- Would the alternatives have created a burden that was greater than the risk?

# Why do Regulators Like Duty of Care Risk Analysis?

- Since 1993 regulations are required to balance cost and benefit.
- “Executive Order 12866” has been in effect for the past 25 years.
  - HIPAA Security Rule
  - Gramm Leach Bliley Act
  - Federal Trade Act
  - 23 NYCRR Part 500, and most state regulations.
- Regulations have since then included the terms “risk,” “reasonable,” and “appropriate” to indicate the cost-benefit standard for compliance.

# Why do Executive Like Duty of Care Risk Analysis?

Security Compliance Based on *Risk Assessment*



# Are You Sure? My Regulators Tell Me What To Do.

- Have you demonstrated due care yet?
- If you don't analyze risk to find reasonable controls ... then they don't have much choice but to tell you what to do.

# How Are Other Security Assessments Failing Us?

Evaluates Risk to Information Assets

Evaluates Due Care

Method	Evaluates Risk to Information Assets						Evaluates Due Care		
	Standard of Care	Identifies Vulnerabilities	Considers Threats	Evaluates Harm to Self	Evaluates Harm to Others	Estimates Likelihood	Defines Acceptable Risk	Defines Reasonableness	Evaluates Safeguard Risk
<b>DoCRA</b> CIS RAM	●	●	●	●	●	●	●	●	●
<b>IT Risk Assessments</b> ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◐	●	○	○	◐
<b>FAIR</b> Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
<b>Gap Assessments</b> Audits, "Yes/No/Partial"	●	◐	○	○	○	○	○	○	○
<b>Maturity Model Assessments</b> CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

# How Will a Judge Interpret Maturity Model Assessments?

**Judge:** Plaintiff claims that your data breach could have been stopped if you had used a DLP system. You were not using one. Can you explain why?

**You:** When we evaluated our data leakage controls, we were at a '3' and we decided that we didn't need to go to '4'.

**Judge:** Why? Was the burden of the control greater than the risk to the plaintiff?

**You:** Ummm. We agreed not to go to '4'.

# How Will a Regulator Interpret Gap Assessments?

**Regulator:** Why are you not segmenting your PII network from your corporate network?

**You:** When we identified that gap our CISO accepted the risk.

**Judge:** What standard did you use to accept risk?  
Did your clients agree with this acceptance criteria?

**You:** ... No.

# How Will a Regulator Interpret FAIR Assessments?

**Regulator:** Nice job evaluating the threat. I see the dollar value of your potential losses. But I don't think this control is appropriate for the risk.

**You:** Well, you can see by this heat map over here, our probable loss is low.

**Regulator:** Your probable loss? I'm here to protect the public, not your profits.

**You:** ...

# How Do Organizations Adopt CIS RAM/DoCRA?

- Download CIS RAM from [cisecurity.org](https://cisecurity.org)
- Upgrade your current security assessments with duty-of-care components.
  - Develop risk assessment and acceptance criteria
  - Adding threat models to analysis
  - Evaluate harm to others
  - Evaluating safeguards to determine reasonableness
- Starting fresh with a new [DoCRA](#)-based risk assessment.



# Questions

Chris Cronin  
ccronin@halock.com

<https://learn.cisecurity.org/cis-ram>

# Resources

[CIS RAM Download](#)

[CIS RAM Executive Prospectus](#)

[CIS RAM FAQ](#)

[Duty of Care Risk Analysis Standard \(DoCRA\)](#)