DoCRA

Getting to Reasonable

A Test for “Reasonable Security” Controls

October 6th, 2020

HALOCK®

Presenter

Terry Kurzynski,

Board Member, The DoCRA Council

Senior Partner, HALOCK Security Labs

Terry Kurzynski

- *Board Member of the **DoCRA Council** ("Duty of Care Risk Analysis")*
- Founding Partner of **HALOCK Security Labs** (1996)
- CISSP since 2002
- ISO 27001 Auditor, CISA, PCI QSA
- Contributing author of the CIS® (Center for Internet Security) Risk Assessment Method (CIS RAM)
- Litigation support for large cyber breaches
- On Retainer for several Office of Attorney Generals
- Over 25 years of experience in IT and Security
- University of Wisconsin with a B.S. in Computer Science

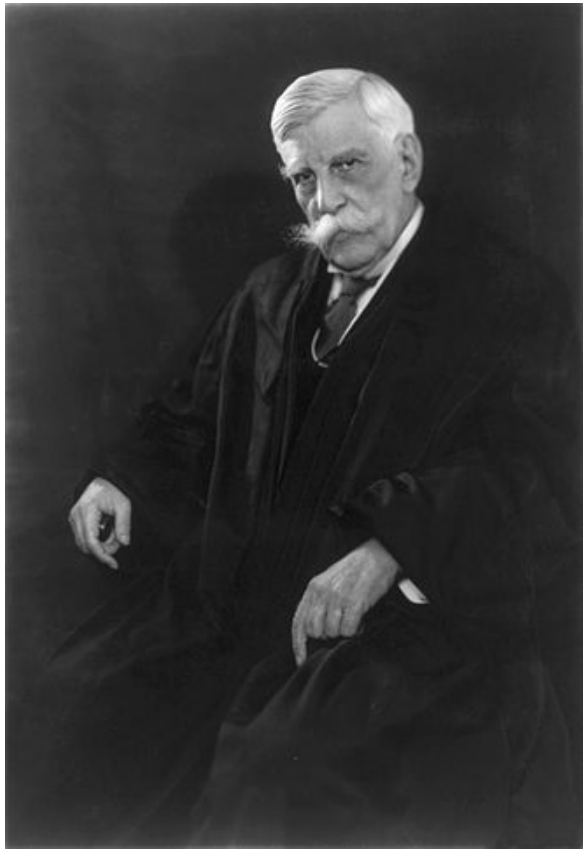
The Breach

- If you are breached and your case goes to litigation, the judge will determine whether you had a “duty of care.”
- The legal concepts of “**duty of care**” and “due care” require that organizations demonstrate they used controls to ensure that risk was reasonable to the organization and appropriate to other interested parties at the time of the breach.

The reasonable person…

"For society to function, a certain average of conduct, a sacrifice of individual peculiarities going beyond a certain point, is necessary to the general welfare."

- Oliver Wendell Holmes, Jr.



In Business We Call it **Duty of Care**

Directors and Officers are expected to act like a reasonable prudent person.

United States of America
v.
JOSEPH SULLIVAN

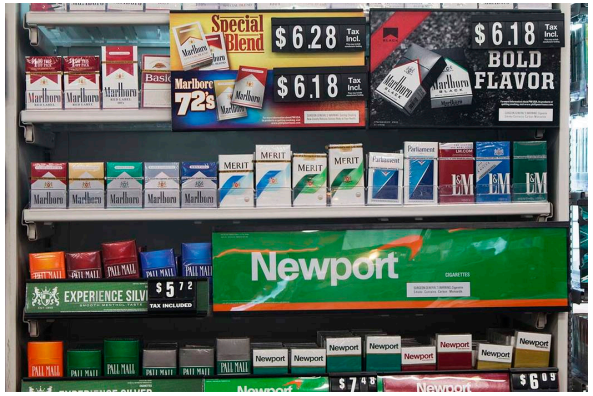
Joe Sullivan, former CISO of Uber

- Two felony counts
- Attempted to cover up a 2nd breach

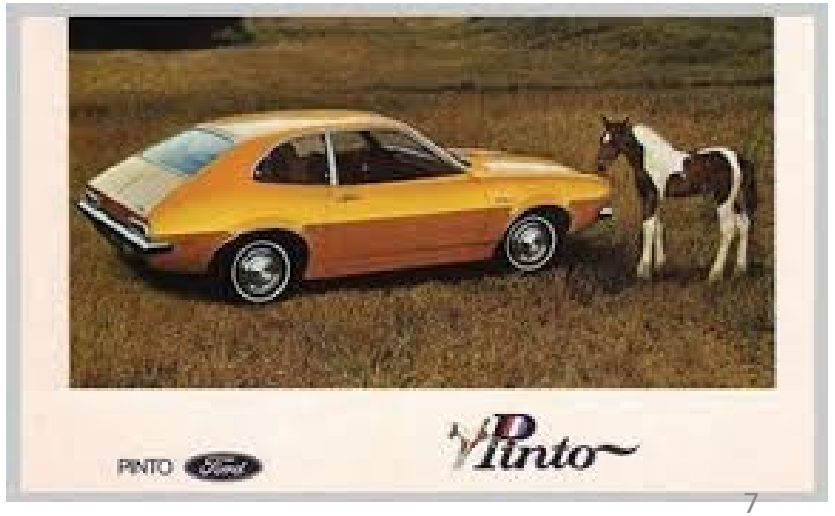
Count One: Obstruction of Justice
Max. Penalties: 5 years in prison; $250,000 fine; 3 years of supervised release; $100 special assessment; restitution; forfeiture

Product Negligence

Must prove that the company had a duty of care and ignored it



Volkswagen



The Problem

- Information security and privacy regulations use “reasonableness” as the standard of care
- Parties allege that the breached organization did not use reasonable security to protect consumer data.
- The definition of reasonable is not agreed-upon, and has been contested.

FTC Failed to Define Reasonable

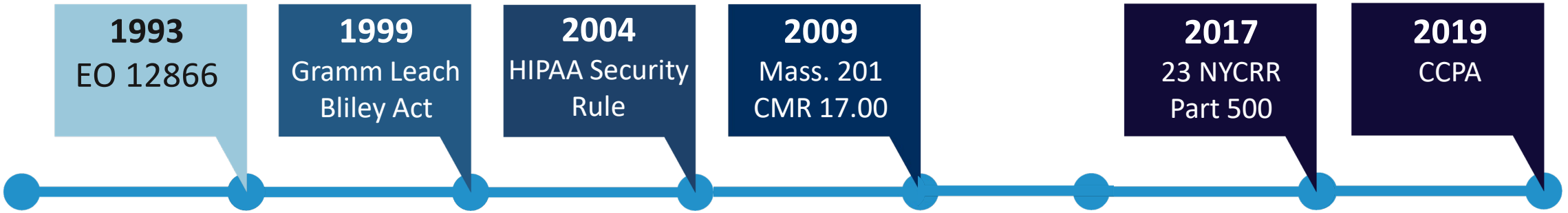
- 2013 FTC files complaint against LabMD for failing to protect the security of consumers' personal data
- FTC alleges that "LabMD failed to provide reasonable and appropriate security for personal information."
- 2014 House Committee hearing; "FTC doesn't have a comprehensive information security program to refer to."
- 2016 LabMD filed a petition for review
- June 2018 Federal appeals court reverses FTC order directing the now defunct LabMD to overhaul its data security program

Something We Did Not Understand About Laws and Regulations

- United States laws and regulations were developed in an entrepreneurial society …
- Laws and regulations needed to make sense to business
- … or laws would cease to be relevant.
- So regulations changed to force business to be smarter about risk …

Regulations Are Business Friendly … Seriously

- Ever since 1993, **Executive Order 12866** required the regulations ***balance cost and benefit***.
- Controls must not cost more than the risk to others.
- That's why security regulations ask for "reasonable controls" and "risk analysis."
- But they failed to clearly define "reasonable" for organizations.



And then there is Healthcare.gov

The Sedona Conference Working Group 11

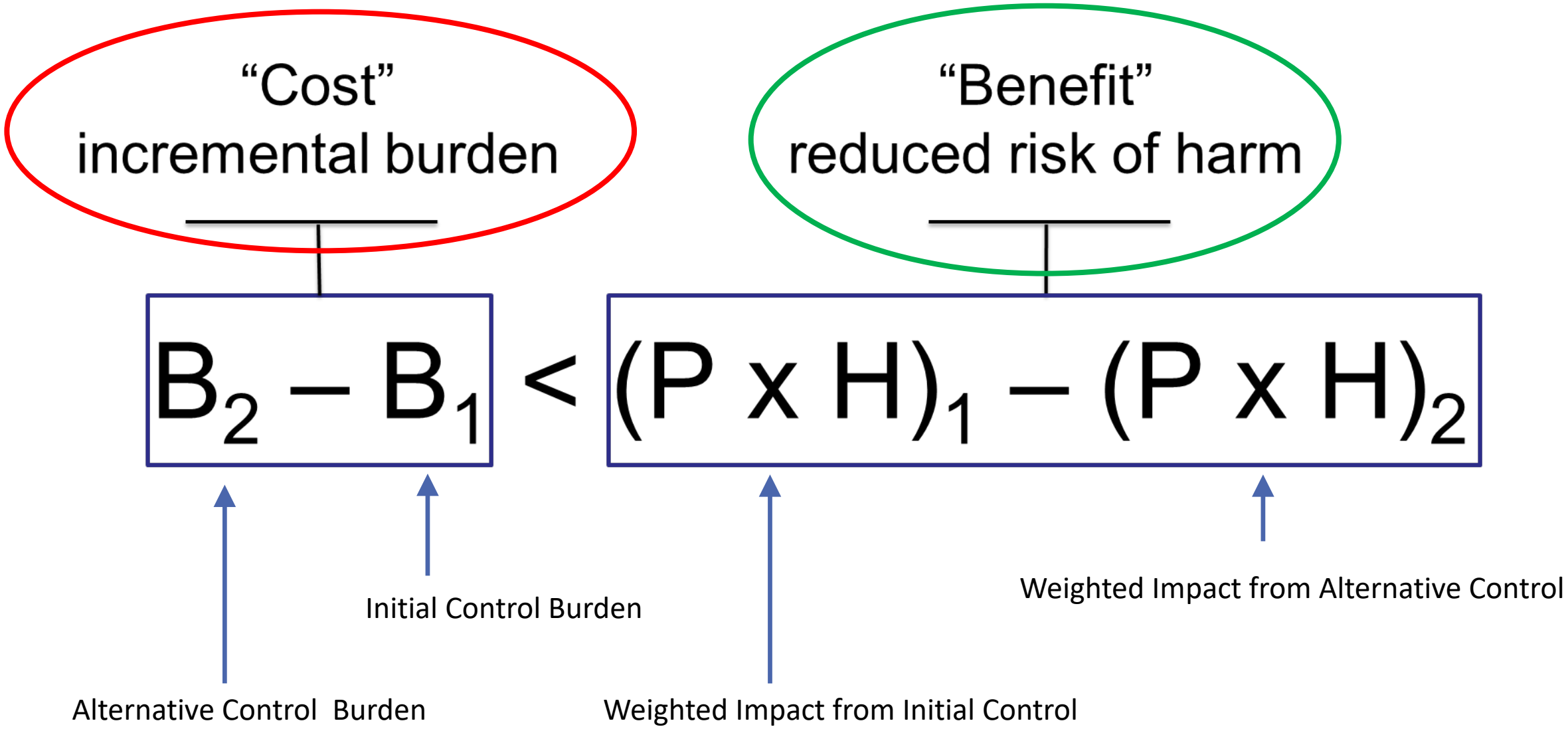
- The Sedona Conference is an influential legal think tank
- The mission of Working Group 11 is to identify and comment on trends in data security and privacy laws
- The research and published papers help organizations prepare for and respond to data breaches and …
- Assist attorneys and judicial officers in resolving the questions of legal liability and damages

Commentary on a Reasonable Security Test

Sedona Conference WG11 has published its
"**Commentary on a Reasonable Security Test**"

- Download the paper: https://thesedonaconference.org/node/9702
- Commentary is open for public comment and suggestions through **November 18th, 2020**
- Send comments to comments@sedonaconference.org

The Solution: a test for reasonable security controls



What is Burden?

$$B_1 < (P \times H)_1$$

- **Burden** is the reduction of any positive result that may be enjoyed by the defendant or covered entity.
  - Finances, efficiencies, corporate growth, strategic goals, etc.
- **Burden** includes "utility," which may include any benefit that the conduct-at-risk created for others:
  - The public, other constituencies, even the plaintiffs.
- **Security controls** can encumber business and operations, harming multiple parties. The consequences of those burdens should be included in the test.

$$B_2 < (P \times H)_2$$

What is Harm?

$$B_1 < (P \times H)_1$$

- Automobile Mfg has a faulty gas tank that results in death 100% after rear-end collision.
- Hospital gets hit with Ransomware and patient records are not accessible, person dies.
- Credit Card issuing bank has card fraud liabilities due to a retailer breach.
- Cloud platform is breached, and hundreds of businesses are vulnerable along with their customers PII exposed.
- Hospitality organization makes an acquisition and acquired organization is breached, exposing millions of PII records.

$$B_2 < (P \times H)_2$$

When is the Test to be Applied?

- An adjudicator, or parties in a dispute, may use the test.
- A plaintiff or regulator would allege that a security control is not reasonable if an alternative control would have reduced the risk to others more than it would have burdened the defendant or covered entity.

Conforms to the Calculus of Negligence

Includes criteria for multifactor balancing tests:

- Costs of controls includes financial, utility, public good
- Liability includes probability and magnitude of harm to others
- Controls should not introduce other risks

B	<=	P	x	L
Burden or cost of treating the risk		**Probability** of occurrence		**Liability** or the cost of the impact should the risk be realized

Injunctive Relief Orders use of "reasonable"

Information Security Safeguards*

7.1 As part of the Information Security Program, Orbitz shall include risk management, which at a minimum includes:

a. Documented criteria for reasonable safeguards that appropriately protect Consumers while not being more burdensome to Orbitz than the risks they address. These criteria shall include:

i. Obligations owed to Consumers for protecting their Personal Information,

ii. The social utility of Orbitz's handling of Consumers' Personal Information,

iii. The foreseeability and magnitude of harm caused by security threats,

iv. The burden to Orbitz's utility and objectives posed by safeguards,

v. The overall public interest in the proposed solution.

*Orbitz December 13, 2019 Injunctive Relief (excerpt)

What Judges and Regulators Look For*

- Did you think through the likelihood of potential incidents?
- Did you think about the magnitude of harm that would come to others who could foreseeably have been harmed?
- Did you consider the value in engaging in the risk to begin with? Was it worth the risk to you and to others?
- What safeguards did you consider that could have reduced the likelihood and impact?
- Would those safeguards have been more costly than the risk?
- Would the safeguards have created other risks?

* Questions vary by state

Risk Assessments, may be used to assess reasonableness (if they have the criteria)

- Estimate the likelihood of potential incidents.
- Estimate the magnitude ***of harm that would come to yourself and others who could foreseeably be harmed***.
- Estimate the ***value in engaging in the risk*** to begin with.
- Design risk treatments that could reduce the likelihood and impact.
- Evaluate the ***burden of safeguards***
  - *Ensure the safeguards* ***would not be more costly than the risk.***
  - *Ensure that the safeguards* ***would not create other risks.***
- **Create a definition of *Acceptable Risk* in plain language for all interested parties.**

If It Does Not Make Sense to the Business, It Won't Make Sense to Judges

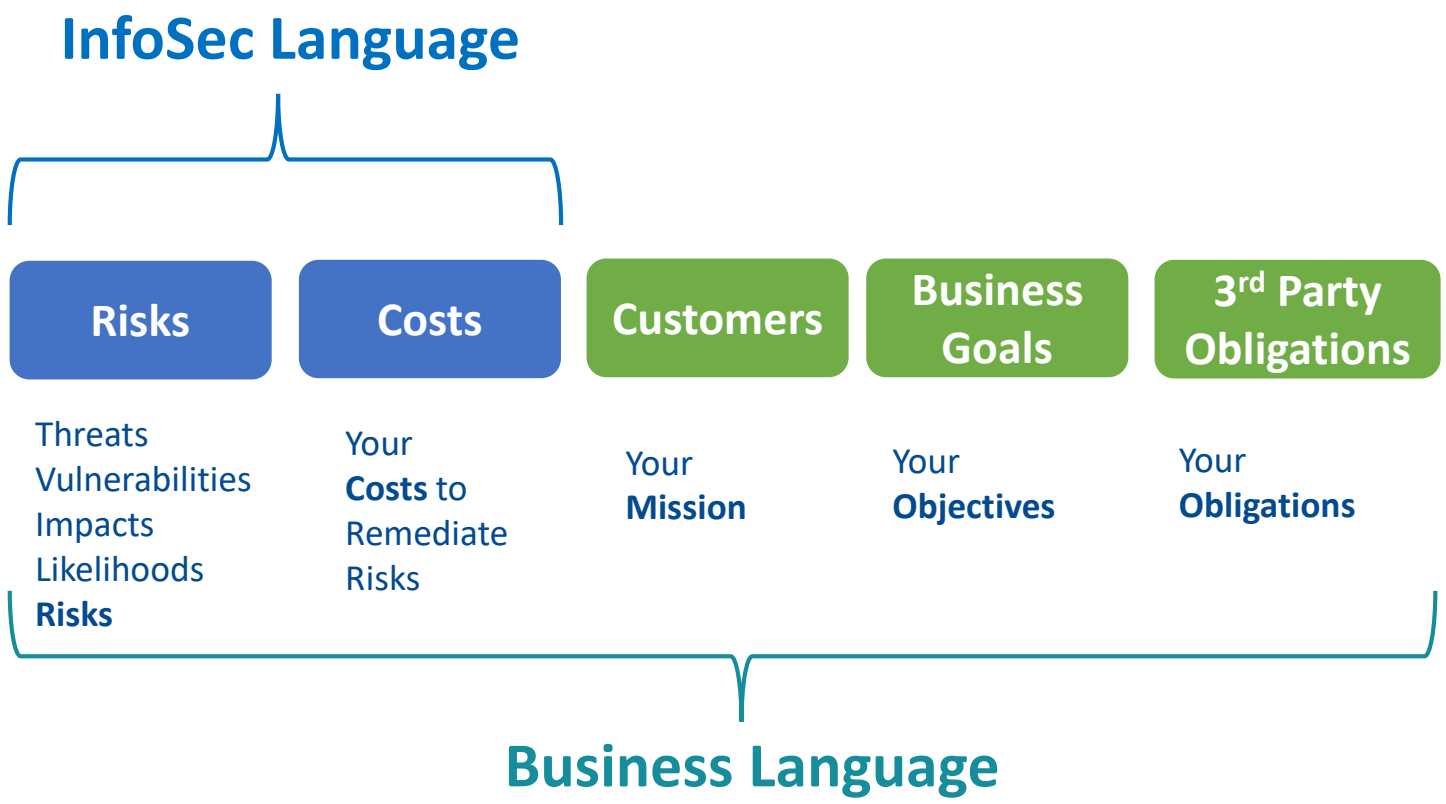
We have been speaking different languages.

Information Security

speaks in *risks and costs*.

Business

speaks in terms beyond *risks and costs*.



What is the **Duty of Care Risk Analysis** (“**DoCRA**”) Standard?

A freely available standard for conducting risk assessments.

A method for demonstrating reasonableness.

Prevails in litigation and regulation.

Originally developed by HALOCK Security Labs to help clients establish a goal for “enough” security.

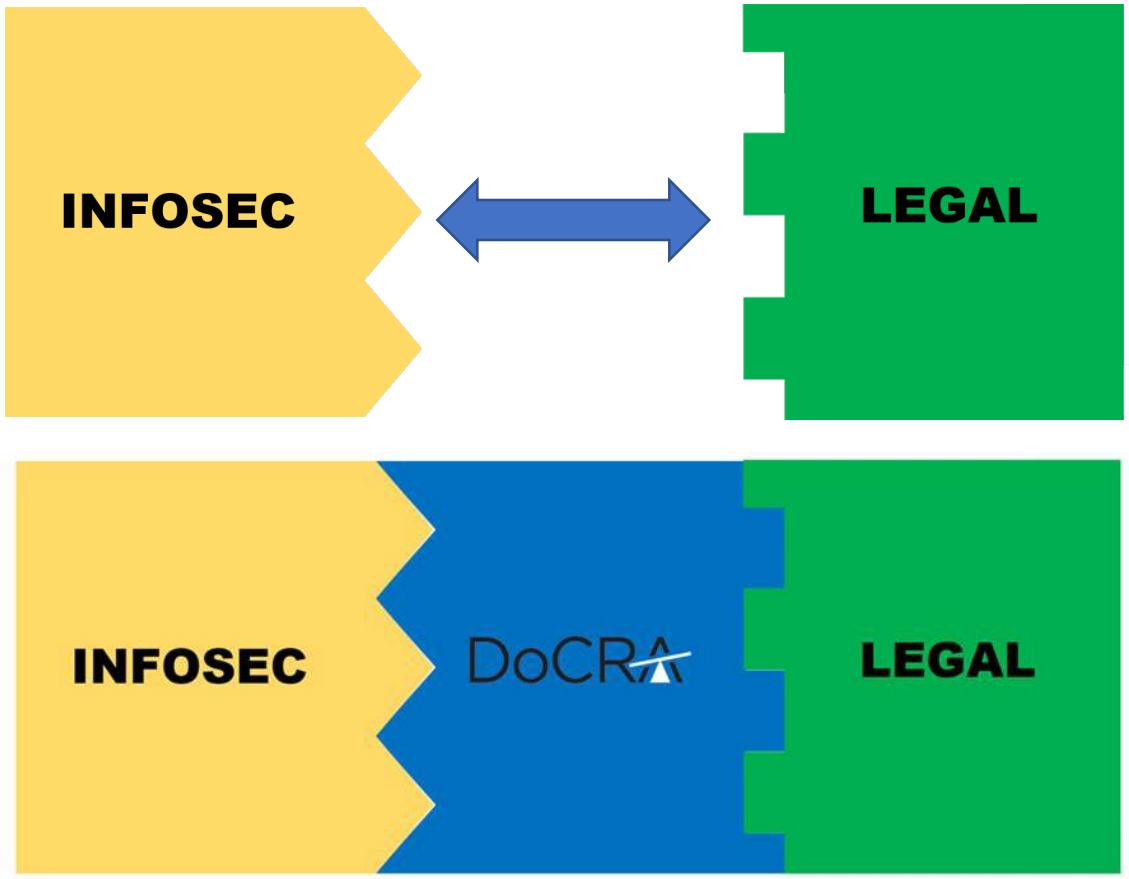
DoCRA based Risk Assessments

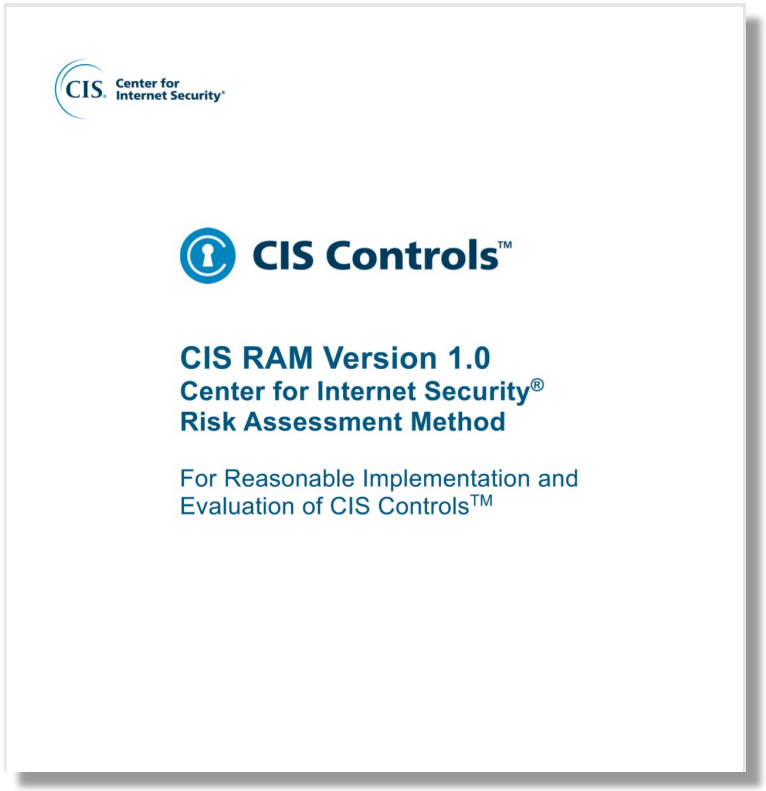
- Legally defensible position by defining what is legally “reasonable”
- Repeatable Process to evaluate “invest” or “accept the risk” for risk mitigation
- Common language between InfoSec and business / regulators / legal system

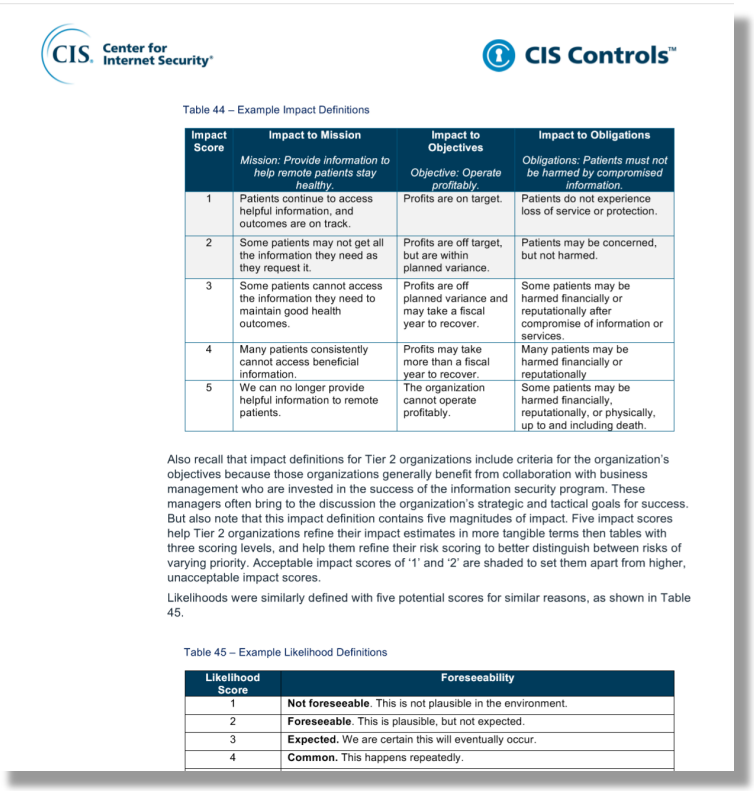
DoCRA Standard

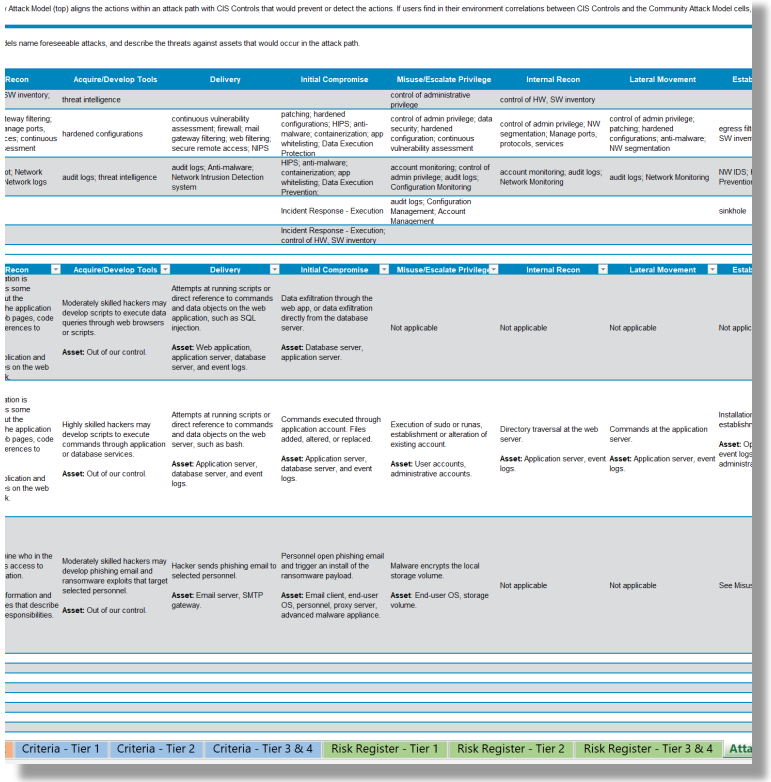
Use your current risk assessment method	NIST SP 800-30 ISO 27005 CIS RAM RISK IT FAIR Applied Information Economics (Hubbard)
Just follow these three principles	- Risk analysis **must consider the interests of all parties** that may be harmed by the risk. - Risks must be reduced to a level that authorities and potentially affected parties would find **appropriate**. - Safeguards must **not be more burdensome than the risks** they protect against.

Solving The Communication Gap









DoCRA Practically Applied: CIS RAM

HALOCK®

Basic Framework (DoCRA impact criteria)

	Our Profit	Patient Privacy
Negligible	*Profit plan is unaffected.*	*No reputational or financial harm.*
Acceptable	*Profit plan within planned variance.*	*Encrypted or unusable information cannot create harm.*
Unacceptable	*Not profitable. Recoverable within the year.*	*Recoverable reputational or financial harm among few patients.*
High	*Not profitable. Recoverable in multiple years.*	*Reputational or financial harm among many patients.*
Catastrophic	*Cannot operate profitably.*	*Cannot protect patients from harm.*

Harm to us (objective)

Harm to others (obligation)

Rexnord Impact Table

	Mission	Objectives	Obligations
	We work every day to be the leading global provider of high value, mission-critical solutions that help customers safely, reliably, and productively keep their goods and assets moving.	**To be a leading marketer and world class manufacturer of power transmission, aerospace, and specialty components, products & systems and provide superior growth and command sustainable competitive advantage.** **To support annual operational and fiscal goals.**	**Personnel information.** **Customer information.** **Protect investor interests.**
1. Negligible		• Targets set in strategic plans remain on target. • Annual operational and fiscal goals remain on target.	• CUI and customer information remains accessible only to approved parties. • Personnel information remains accessible only to approved parties. • Corporate value and stock prices are unaffected.
2. Low	• We would not expect to see customer satisfaction surveys describe a negative perception.	• Strategic plans would be off target, but within planned variance. • Annual operational and fiscal goals would be off target, but within planned variance.	• Compromise of information assets may cause concern to customers but would not result in harm. • Compromise of information assets may cause concern to personnel but would not result in harm. • Compromise of information assets may cause concern to investors but would not result in harm.
3. Medium	• Some customers would report that Rexnord could not help them safely, reliably, productively keep their goods and assets moving.	• Strategic plans or annual operational and fiscal goals would be off target and outside of planned variance. • This would require countermeasures to recover.	• At least one customer would experience harm (financial, safety, etc.) as a result. • A small set of personnel suffer harm such as identity theft, reputational damage, or financial harm. • Company reputation or stock value would decrease short-term.
4. High	• Many customers would report that Rexnord could not help them safely, reliably, productively keep their goods and assets moving.	• Strategic plans or annual operational and fiscal goals would be severely off target, and would require material investment or lost opportunity to recover. • Would result in Business Unit failure.	• Multiple customers would experience harm (financial, safety, etc.) as a result. • A material count of personnel suffer harm such as identity theft, reputational damage, or financial harm. • Company reputation or stock value would decrease long-term.
5. Catastrophic	• Rexnord would not be able to help customers safely, reliably, productively keep their goods and assets moving.	• Rexnord could not operate as a profitable organization.	• Multiple customers would experience significant harm (financial, safety including loss of life, etc.) as a result. • Personnel suffering irreparable harm including loss of life. • Company reputation or stock value would suffer permanent, terminal loss of value.

Hmm, did C.I.A disappear?

To meet Due Care, define your **Purpose**:

- **Mission**: What makes the risk worth it for others?
- **Objectives**: What are your indicators of success?
- **Obligations**: What care do you owe others?

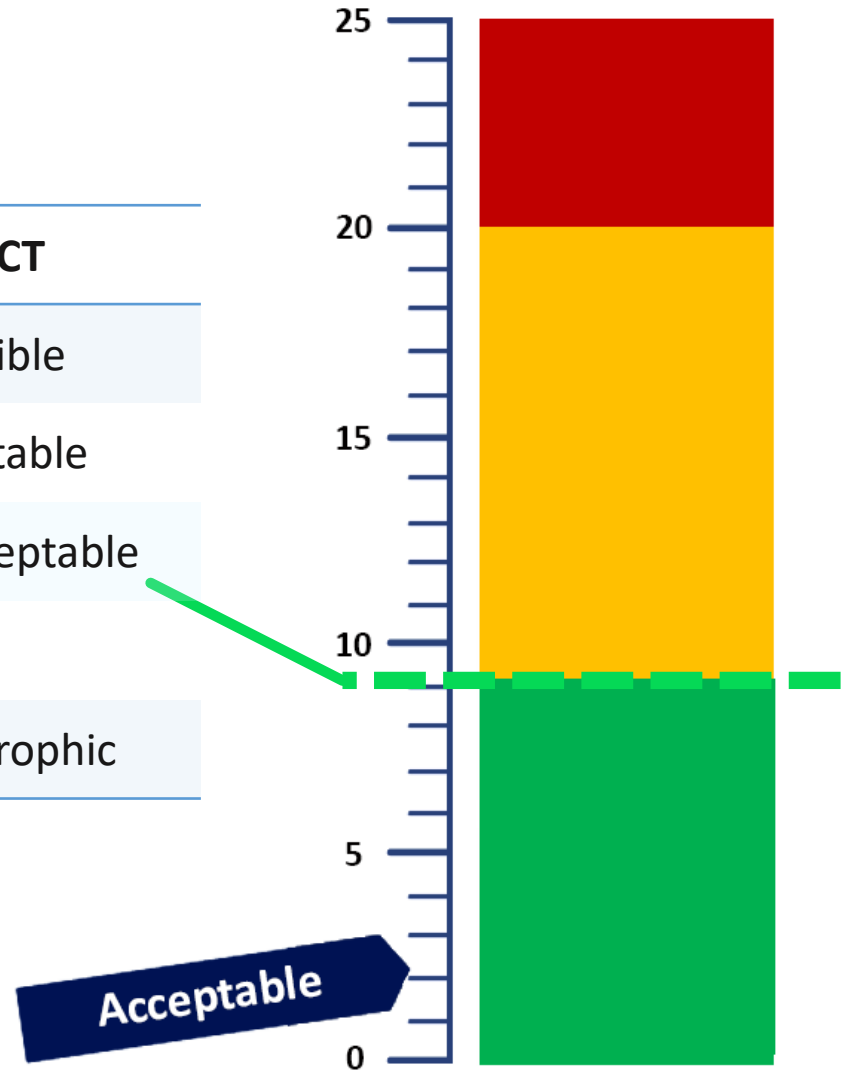
Some Common Impact Criteria

Industry Example	Mission	Objectives	Obligations
Commercial Bank	Customer performance	Return on assets	Customer information
Nonprofit Healthcare	Health outcomes	Balanced budget	Patient privacy
University	Educate students	Five-year plan	Student financials
Manufacturer	Custom products	Profitability	Protect customer IP
Electrical generator	Provide power	Profitability	Public safety

Defining Acceptable Risk

	LIKELIHOOD
1	Not possible
2	Not foreseeable
3	Foreseeable
4	Expected
5	Common

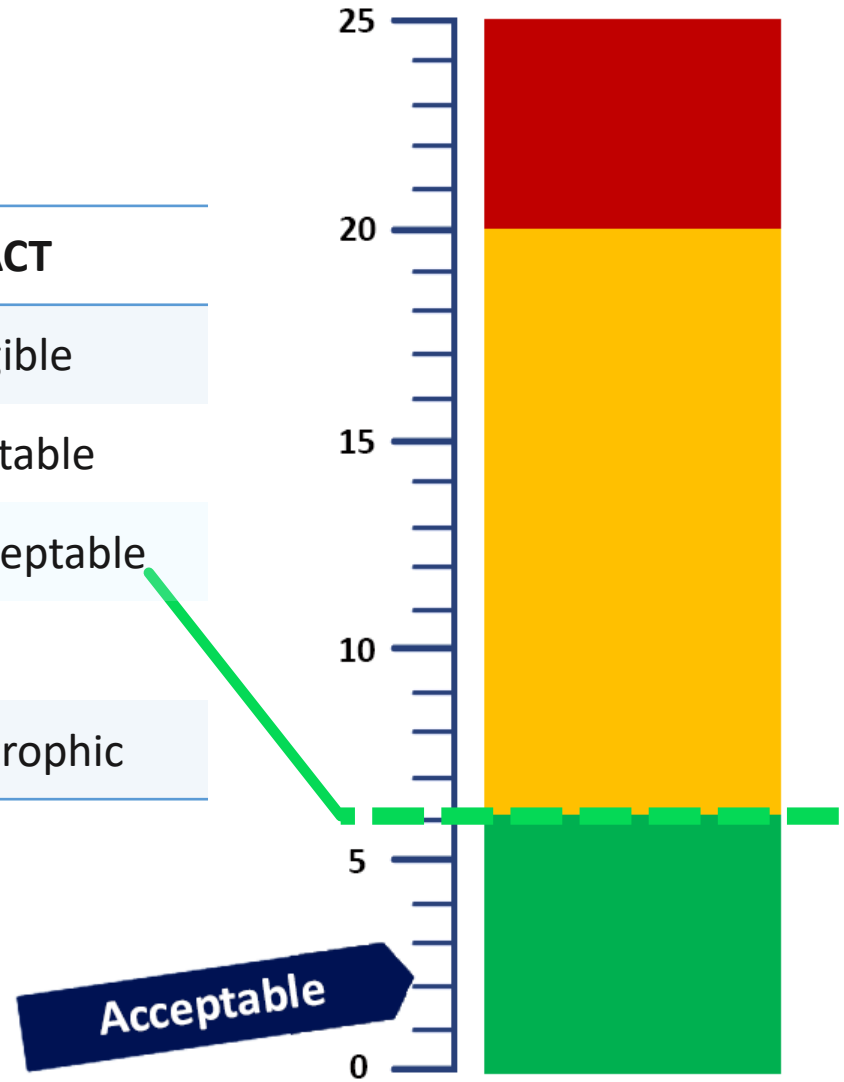
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



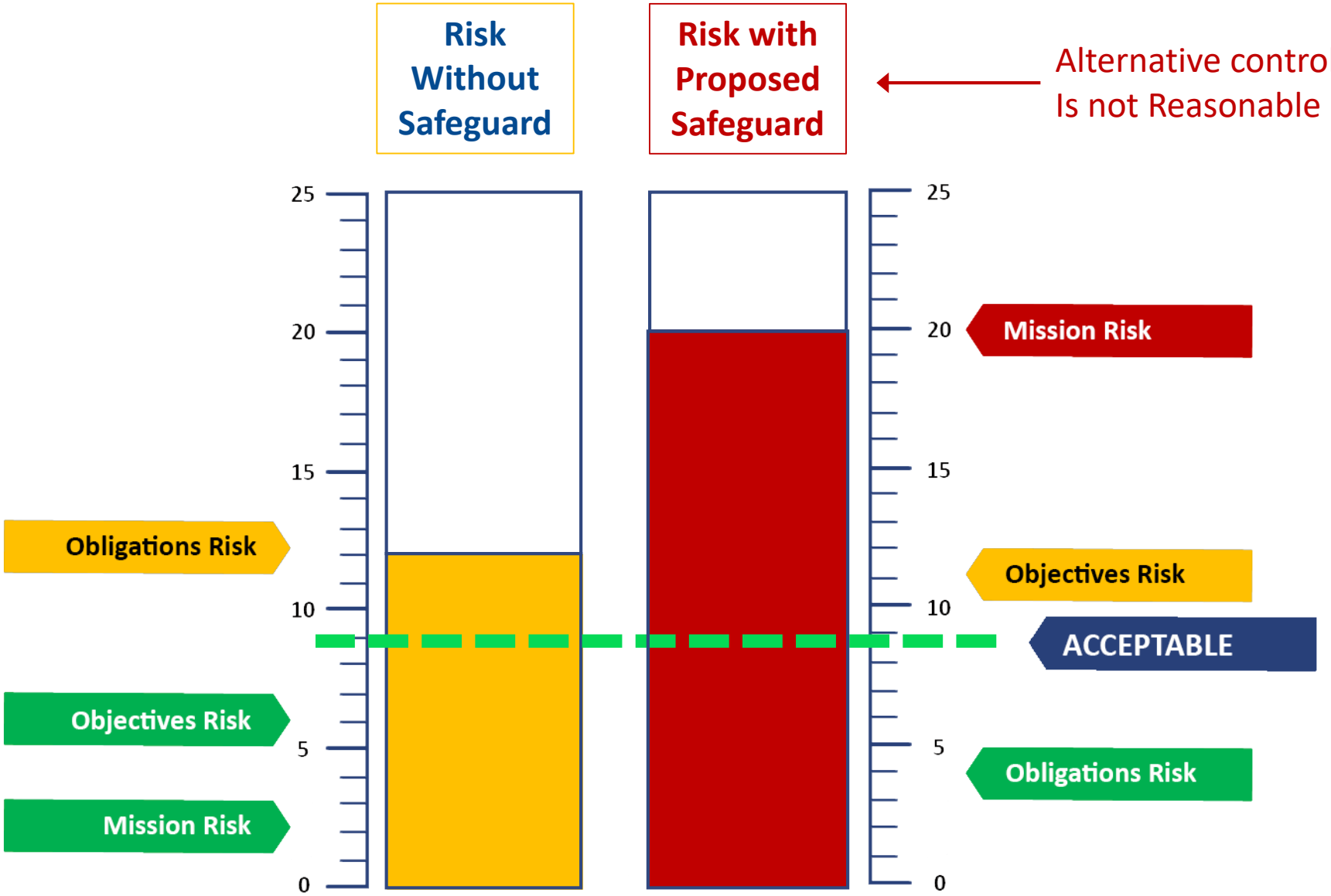
Defining Acceptable Risk

	LIKELIHOOD
1	Not possible
2	Not foreseeable
3	Foreseeable
4	Expected
5	Common

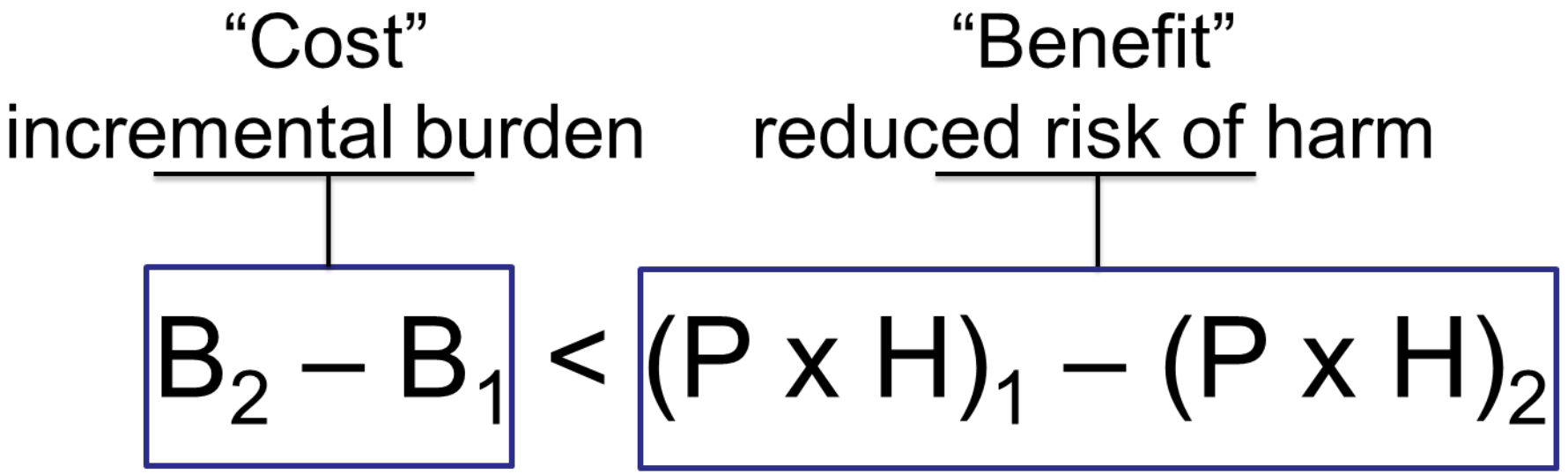
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



Some Safeguards are NOT Reasonable



Alternative control is unreasonable



Incremental burden		Reduced risk
$1,800,000	**>**	**Between $283,500 and $1,620,000**

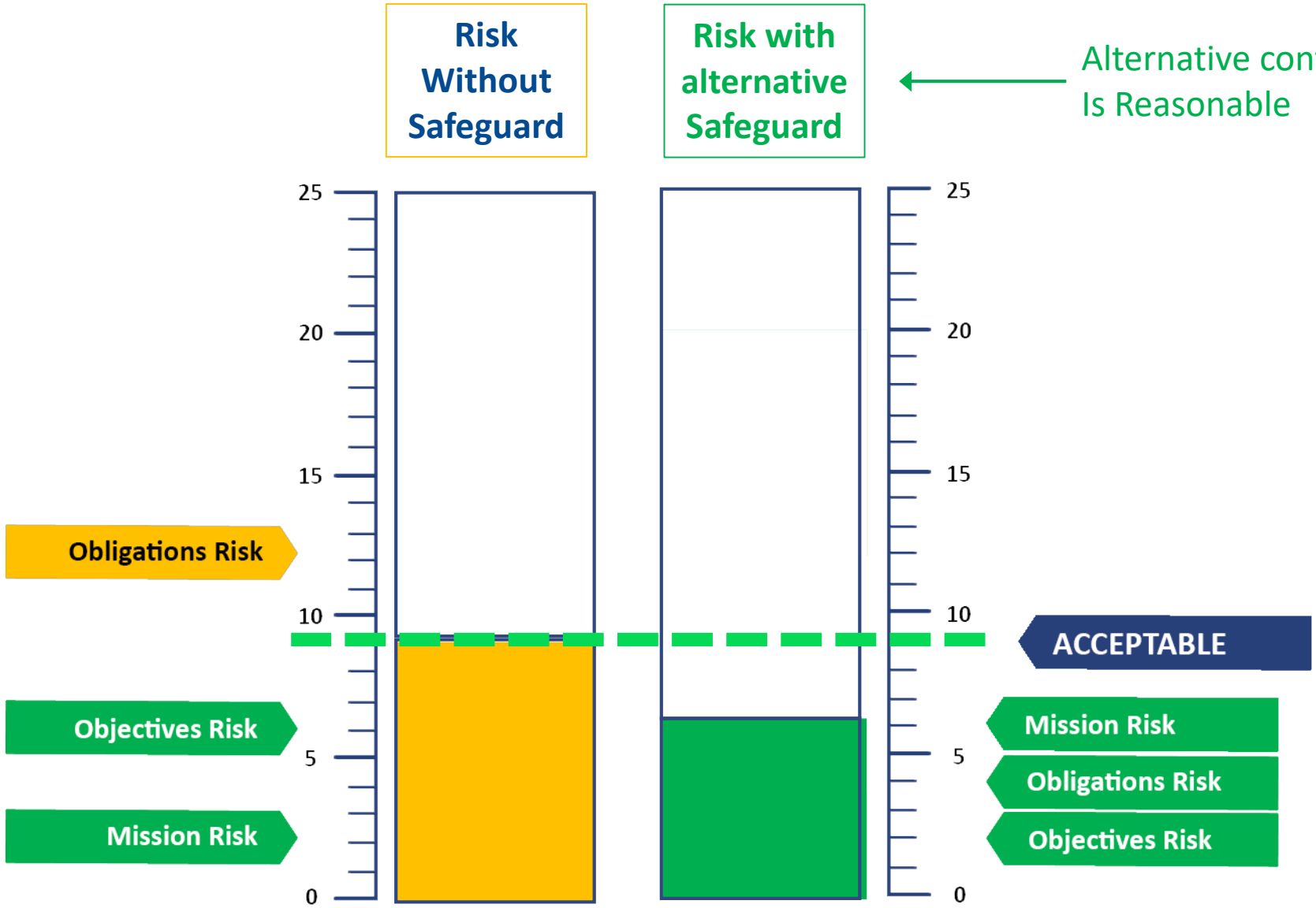
But This is Not Always About Economics

Incremental burden		Reduced risk
$1,800,000	>	Between $283,500 and $1,620,000

Risk is not always expressed in economic terms. Sometimes, we are comparing un-like things. DoCRA also lets us evaluate unlike things by using risk scores.

Incremental burden		Reduced risk
7	>	4

Demonstrating Reasonable Safeguards



Alternative Control is reasonable

"Cost" incremental burden

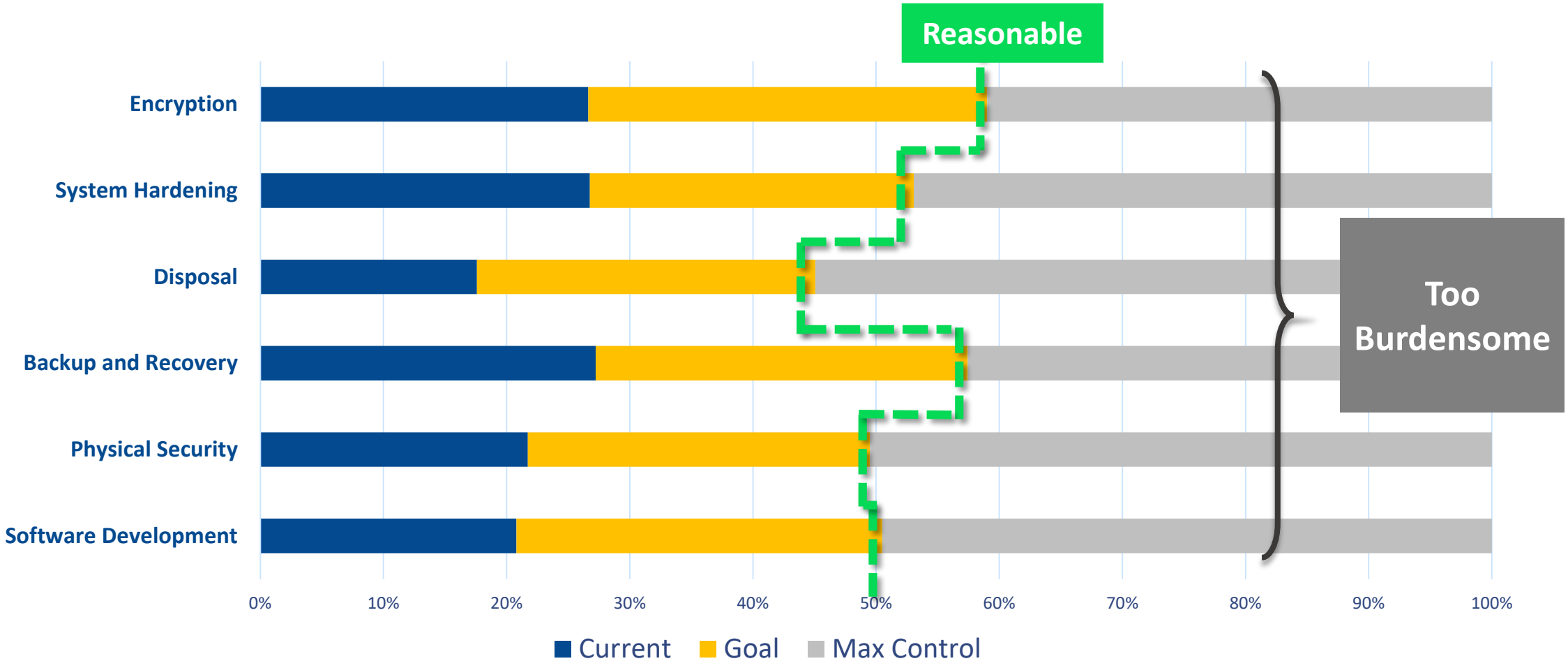
"Benefit" reduced risk of harm

$$B_2 - B_1 < (P \times H)_1 - (P \times H)_2$$

Incremental burden		Reduced risk
$46,300	**<**	**Between $77,700 and $1,283,625**

HALOCK

Compliance through the lens of Reasonable

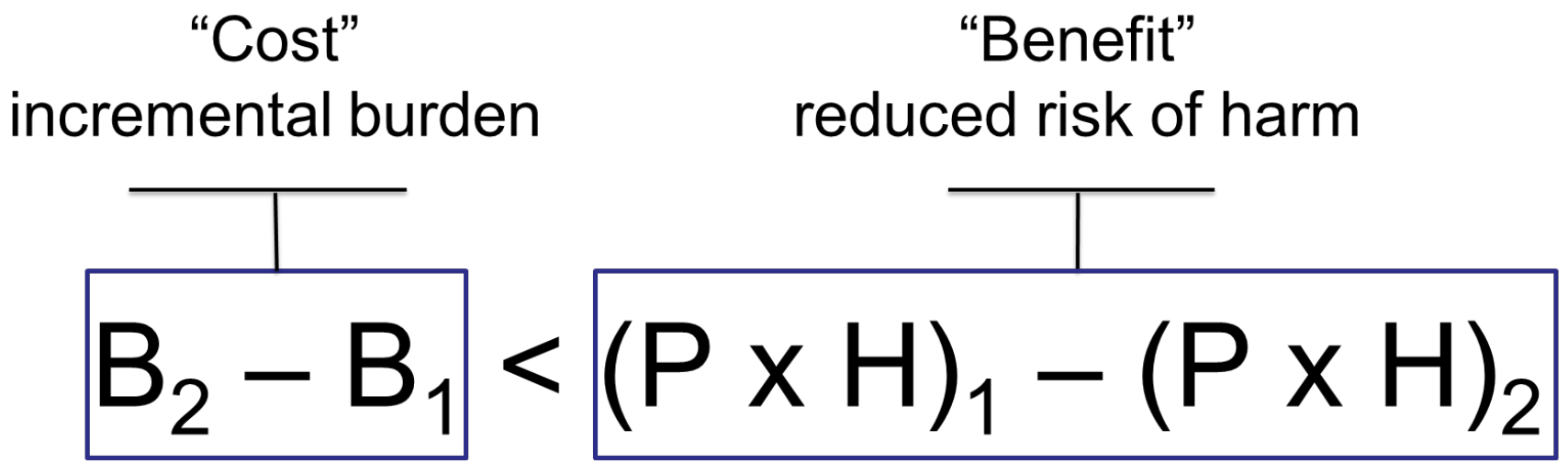


Summary

- Organizations have a duty of care to protect data in the care.
- Organizations need to perform risk assessments.
- Reasonable controls can be applied through use of effective risk analysis based on **DoCRA**.
- Free risk methods and tools available from the Center for Internet Security (**CIS RAM**).
- Use the **Reasonable Security** test to prioritize your actions.

Helpful links

- https://thesedonaconference.org/node/9702
- www.DoCRA.org
- https://learn.cisecurity.org/cis-ram
- https://www.halock.com/cis-ram-pages-210.php



Thank You

Terry Kurzynski

TerryK@halock.com