DoCRA

Adopting Duty of Care Risk Analysis to drive GRC

Presented by:
Jennifer Urban Rathburn & Terry Kurzynski

June 5th, 2019

Presenters

Jennifer Urban Rathburn

Partner
Foley & Lardner LLP

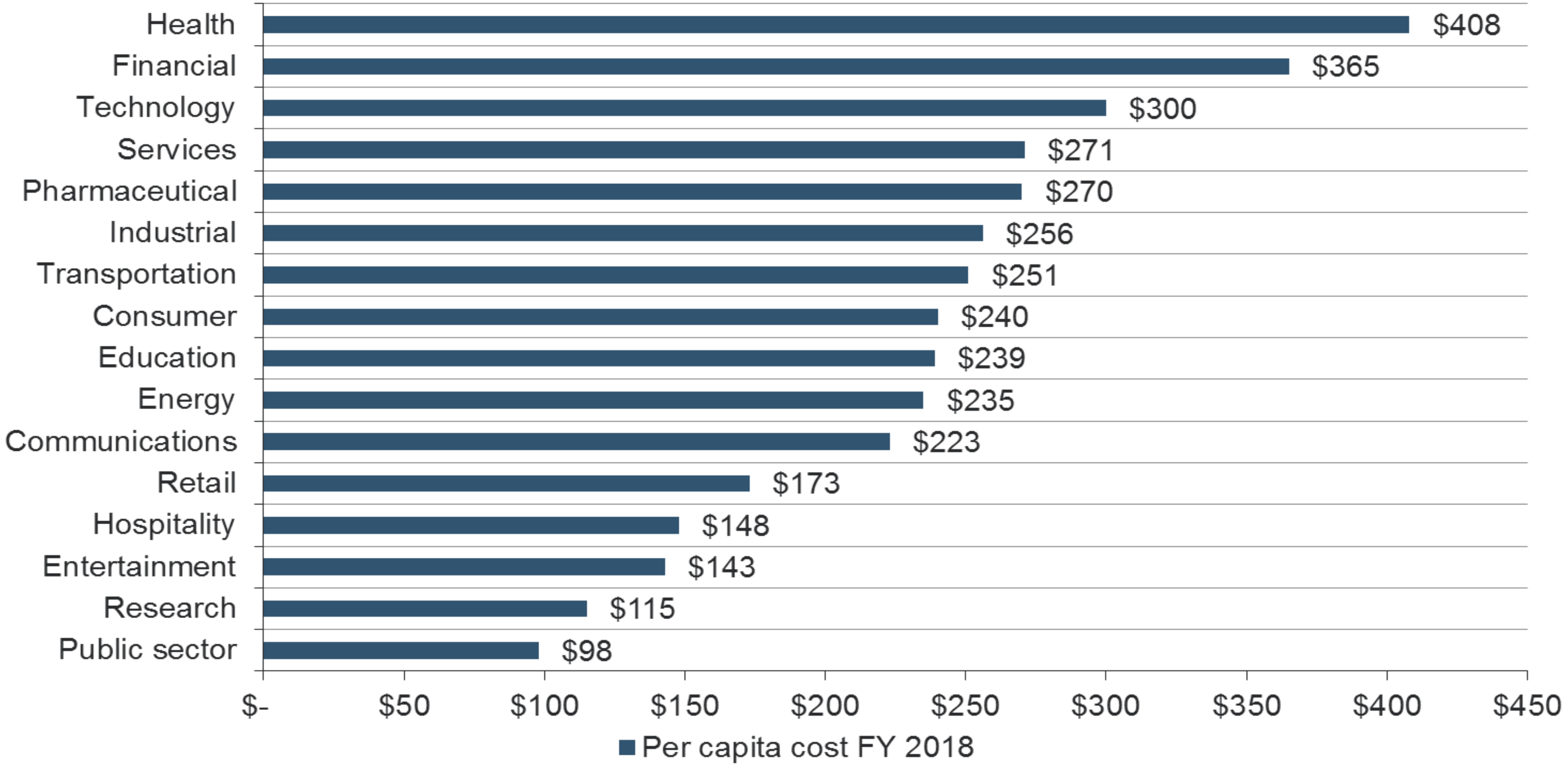
Terry Kurzynski,
CISSP, CISA, PCI QSA,
ISO 27001 Auditor

Board Member
The DoCRA Council

Jen Urban Rathburn

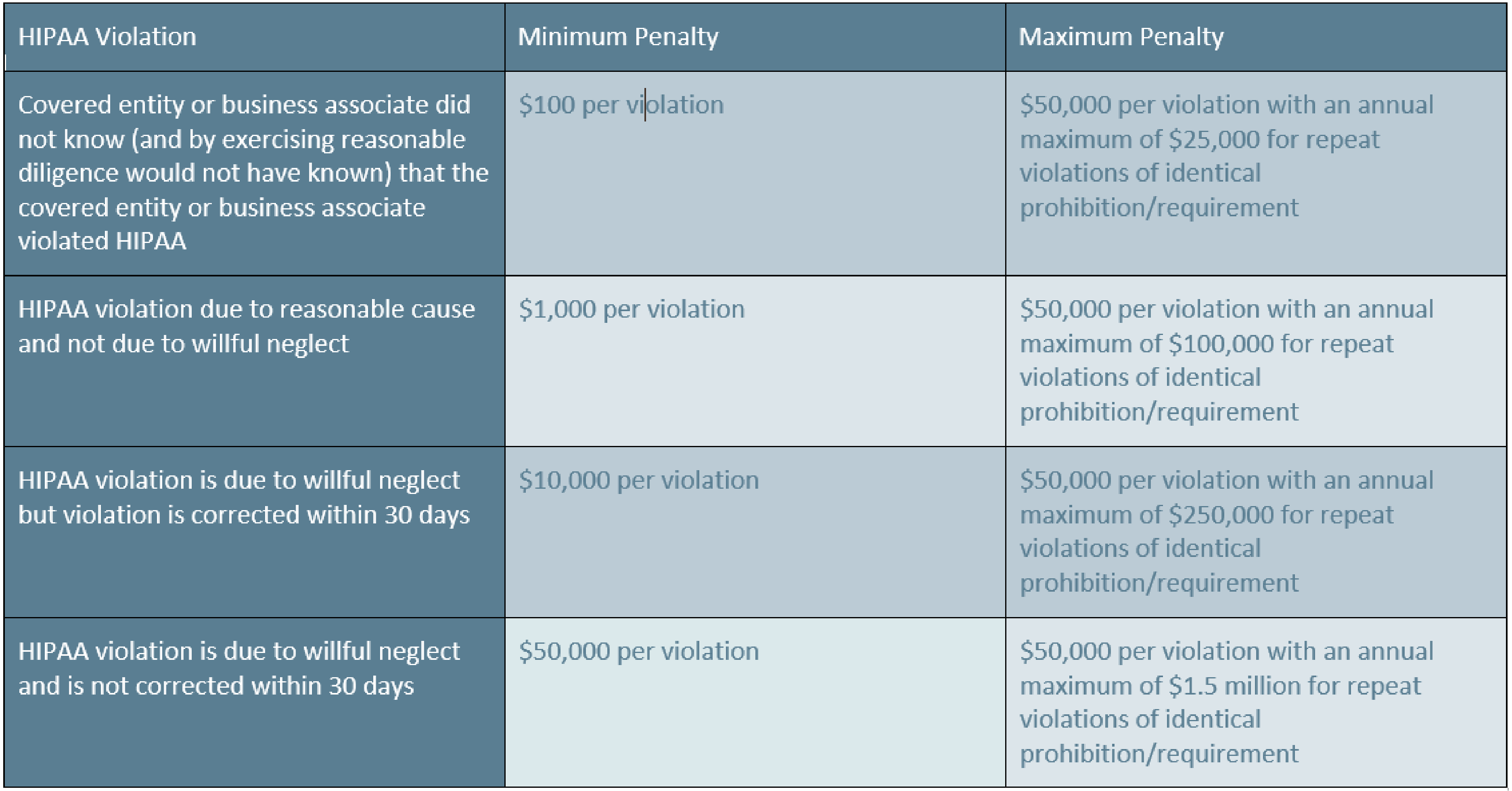
- Co-founder of the Midwest Cyber Security Alliance
- Partner with Foley & Lardner LLP
  - data protection programs
  - data incident management
  - breach response and recovery
  - monetization of data
  - prepare for and respond to data security incidents
  - compliance with U.S. and global privacy and data security laws
- Certified Information Privacy Professional/United States

Health Care Industry Has Highest Breach Costs



Source: Ponemon Institute© Research Report (sponsored by IBM Security), *2018 Cost of a Data Breach Study: United States* (July 2018)

Potential HIPAA Penalties



HIPAA Violation	Minimum Penalty	Maximum Penalty
Covered entity or business associate did not know (and by exercising reasonable diligence would not have known) that the covered entity or business associate violated HIPAA	$100 per violation	$50,000 per violation with an annual maximum of $25,000 for repeat violations of identical prohibition/requirement
HIPAA violation due to reasonable cause and not due to willful neglect	$1,000 per violation	$50,000 per violation with an annual maximum of $100,000 for repeat violations of identical prohibition/requirement
HIPAA violation is due to willful neglect but violation is corrected within 30 days	$10,000 per violation	$50,000 per violation with an annual maximum of $250,000 for repeat violations of identical prohibition/requirement
HIPAA violation is due to willful neglect and is not corrected within 30 days	$50,000 per violation	$50,000 per violation with an annual maximum of $1.5 million for repeat violations of identical prohibition/requirement

HITECH Act Section 13410(d); HHS Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties, April 30, 2019, available here.

Recent OCR Enforcement Action: Medical Records Service

- 3.5M records accessed by hacker
- OCR Director Roger Severino
  - "Entities entrusted with medical records must be on guard against hackers. The failure to identify potential risks and vulnerabilities to ePHI opens the door to breaches and violates HIPAA."
- $100,000 penalty to HHS
- Corrective Action Plan
  - (A) Conduct Risk Analysis
  - (B) Develop and Implement a Risk Management Plan

Cybersecurity Under HIPAA

- HIPAA compliance is required but **it will not ensure protection** from cyber attacks.

- **Risk Management Process Standard**
  - Implement policies and procedures to **prevent, detect, contain, and correct security violations**.

HIPAA Risk Analysis

- CEs and BAs must “conduct an **accurate and thorough assessment** of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of” ePHI.
- **Required** Implementation Specification.
- Should be **ongoing**, but at a minimum recommend **update** annually or when new technologies or business operations are implemented.

OCR “Guidance on Risk Analysis Requirements under the HIPAA Security Rule”

- **What Should You Do? Follow Guidance:**
  - Scope of the Analysis
  - Data Collection
  - Identify and Document Potential Threats and Vulnerabilities
  - Assess Current Security Measures
  - Determine the Likelihood of Threat Occurrence
  - Determine the Potential Impact of Threat Occurrence
  - Determine the Level of Risk
  - Finalize Documentation
  - Periodic Review and Updates to the Risk Analysis

- **Also see, OCR Privacy & Security Listserv**

  https://www.hhs.gov/hipaa/for-professionals/list-serve/index.html?language=es

HIPAA Risk Management and Evaluation

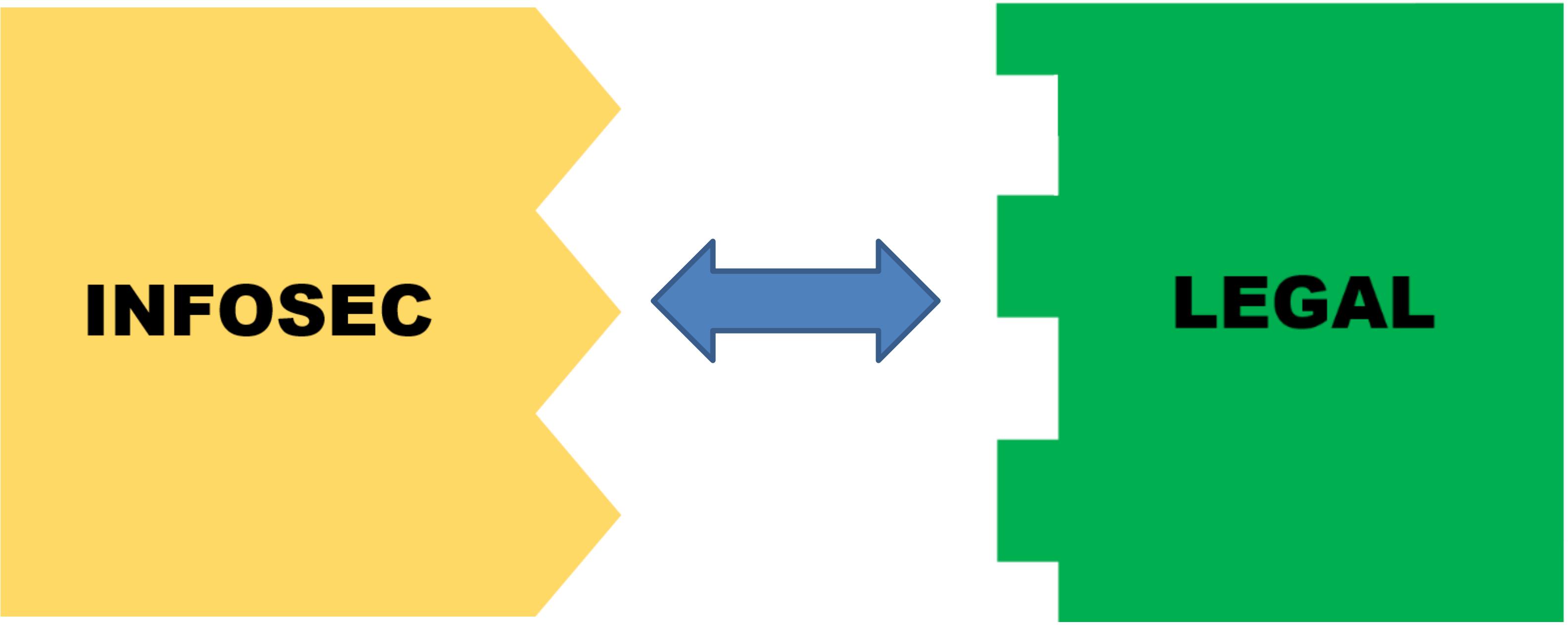
- **Risk Management Implementation Specification (Required)**
  - Implement security measures sufficient to **reduce risks and vulnerabilities to a reasonable and appropriate level**.
- **Evaluation Standard**
  - Perform a **periodic technical and nontechnical evaluation** that establishes the extent to which security policies and procedures meet the requirements of the HIPAA Security Rule.
  - Evaluation is based initially upon the initial standards implemented and, subsequently, **in response to environmental or operational changes** affecting the security of ePHI.

Five Cybersecurity Principles Every Board Director Needs to Know

1. Understand and Approach Cybersecurity as an Enterprise-wide Risk Management Issue, Not Just an IT Issue
2. Understand the Legal Implications of Cyber Risks as They Relate to the Company’s Specific Circumstances
3. Have Adequate Access to Cybersecurity Expertise and Give Cyber Risk Management Regular and Adequate Time on Board Meeting Agendas
4. Set the Expectation That Management Will Establish an Enterprise-wide Risk Management Framework With Adequate Staffing and Budget
5. Management Discussions Should Include Identification of Which Risks to Avoid, Which to Accept and Which to Mitigate or Transfer Through Insurance

“NACD Director's Handbook on Cyber-Risk Oversight” National Association of Corporate Directors (2017)

The Communication Gap



Preparing for a Data Breach

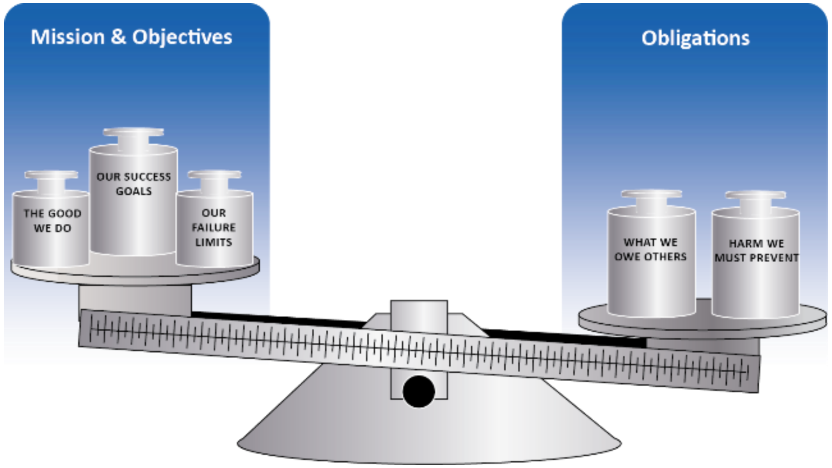
The day you are sued for a data breach, you will be asked a series of questions that you will want to be prepared for.

Multi-factor Balancing Test

- Judges use the multi-factor balancing test in negligence cases

- Was there a duty of care obligation?

- Was due care performed adequately?



DoCRA

Example of Multi-Factor Balancing Tests

(1) the injury is too remote from the **negligence**; or (2) the injury is too wholly out of proportion to the culpability of the **negligent** tortfeasor; or (3) in retrospect it appears too highly extraordinary that the **negligence** should have brought about the **HARM**; or (4) because allowance of recovery would place too ***unreasonable a burden*** on the **negligent** tortfeasor; or (5) because allowance of recovery would be too likely to open the way for fraudulent claims; or (6) allowance for recovery would enter a field that has no sensible or just stopping point.”) on the defendant of **taking precautions against the risk**, (9) the defendant’s ***ability to exercise due care***, (10) the *consequences* on society of imposing the burden on the defendant, (11) public policy, (12) the ***normal expectations*** of participants in the defendant’s activity, (13) the expectations of the parties and of society, (14) the goal of **preventing future injuries** by deterring conduct in which the defendant engaged, (15) the desire to avoid an **increase in litigation**, (16) THE DECISIONS OF OTHER JURISDICTIONS, (17) the BALANCE of the **foreseeable risk** of injury versus the ***burden*** of preventing it (i.e., the Learned Hand formula), (18) FAIRNESS, (19) logic and science, (20) the desire to limit the ***consequences*** of wrongs (expressed in New York as the desire **to curb the likelihood** of unlimited or insurer-like liability), (21) the hand of history, (22) ideals of morality and justice, (23) the convenience of administration of the resulting rule, (24) social ideas about where the plaintiff’s loss should fall, (25) whether there is social consensus that the plaintiff’s asserted interest is ***worthy of protection***, (26) community mores, (27) whether the ***injury is too remote*** from the defendant’s conduct, (28) whether the ***injury is out of proportion*** to the defendant’s wrong, (29) whether the ***imposition of a DUTY*** would open the way to fraudulent claims, (30) whether the recognition of a ***duty*** would enter a field with no sensible stopping point, (31) the ***cost and ability*** to spread the **risk of loss**, (32) the court’s experience, (33) the desire for a reliable, *PREDICTABLE*, and *CONSISTENT BODY OF LAW*, (34) public policies regarding the **expansion or limitation of new channels of liability**, (35) the potential for *DISPROPORTIONATE RISK* and reparation allocation, (36) whether one party *had superior knowledge* of the **relevant risks**, (37) whether either party had the ***right to control or had actual control*** over the **instrumentality of harm**, (38) the **degree of certainty** that the **plaintiff suffered injury**, (39) the moral blame attached to the defendant’s conduct, (40) the FORESEEABILITY OF THE PLAINTIFF, (41) economic factors, and (42) a consideration of which party could better **bear the loss**.

Multi-factor Balancing Test

- What they all have in common
  - Social Utility and Benefits for Each Party
  - Was the Risk Foreseeable
  - Potential Impact or Injury
  - Burden of Safeguards
  - Relationship Between the Parties

Terry Kurzynski

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

POLL QUESTION #1

Does your organization perform risk assessments?

- Does not exist
- Ad hoc/occasionally/as needed
- On a regular basis/recurring risk management in place

What we have learned so far …

- HIPAA Security is based on risk analysis
- Judges determine negligence based on multifactor balancing tests
- Information security frameworks almost universally require risk assessments

That is to say..
The Best Defense is a Good Risk Assessment

- A ***properly framed risk analysis*** and risk management program can help meet compliance requirements, limit liability and prioritize information security activities

Calming the Regulators Post-Breach

- A major research hospital breaches patient records, getting the attention of OCR.
- Investigation revealed:
  - Ongoing vulnerabilities that allowed the breach to occur.
  - Lack of a risk management program or risk assessments.
- Hospital conducts a risk assessment to identify controls that would be “reasonable” for them.
- OCR accepts these “reasonable” controls as the hospital’s corrective action plan!

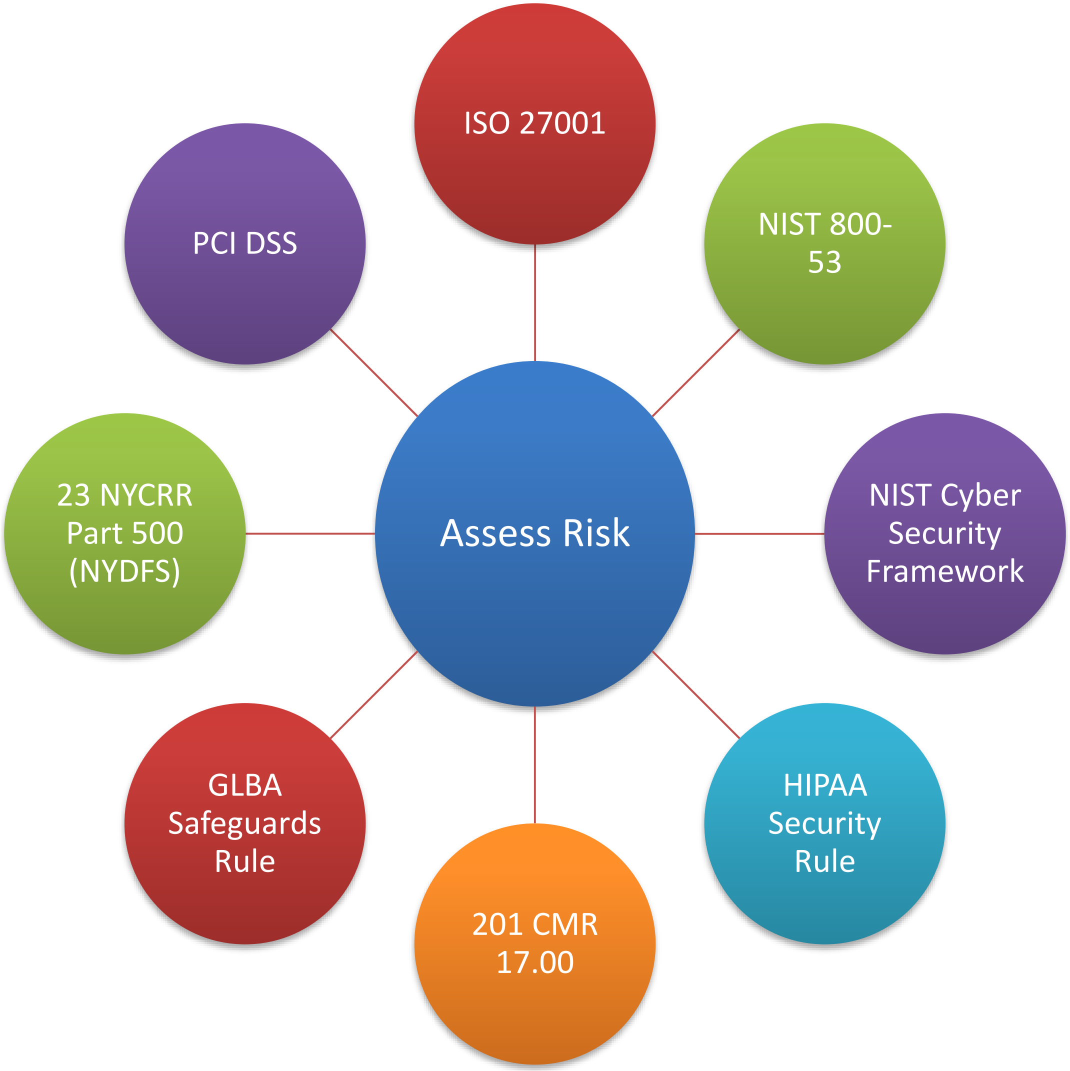
Calming the Security Auditors

- HHS auditors use NIST 800-53 to evaluate HHS vendor and find non-compliance access controls.
- Auditors require vendor to use very expensive multifactor authentication technology.
- Vendor's risk assessment shows that their current control is as reasonable as the auditor's costly requirement.
- HHS auditor concedes the point, and moves on.

Calming the Litigators

- Healthcare provider suffers a breach that includes patient data.
- Residents file a complaint with their state’s Attorney General.
- The AG reviews the provider’s risk assessment and sees a thorough evaluation of reasonable controls that were in place at the time of the breach.
- AG does not pursue the complaint, given the thoughtful definitions of acceptable risk.

Risk Assessments are Universally Required



Assess Risk

ISO 27001

NIST 800-53

NIST Cyber Security Framework

HIPAA Security Rule

201 CMR 17.00

GLBA Safeguards Rule

23 NYCRR Part 500 (NYDFS)

PCI DSS

Why is Risk So Difficult?

- The Threat-Vulnerability landscape is in constant motion
- Threat Actors are evolving and changing
- Many interested parties with expectations
- Difficult to measure the probability of any given threat-vulnerability pairing
- Tough to develop impact scoring that can be agreed upon by the business that will also pass the “balance test” in the court of law
- Prioritizing risk is a challenge
- Time consuming
- Appears to be out of date the minute it is published

Risky Business?

Issues with current risk methods

- There is no risk appetite statement.
- The risk assessment process does not involve key personnel.
- Only considers the company’s risk (not the public’s).
- Quantifies risk only terms of dollar limits.
- General counsel constrains the process with concerns over risk documentation.
- Lacks “a-ha” insights leaving decision makers not knowing what to do next to manage risk and how it may impact business plans and decisions.

POLL QUESTION #2

In the event of a breach, how do you feel your risk assessment method affects your liability

- Increase
- Decrease
- I Don’t know

In the Age of Information Security

Requires risk assessments to meet ***duty of care***

What is Duty of Care?

- 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.

Reasonable Person

- If someone applied appropriate safeguards, or "**due care**" and harm resulted, then their liability will be mitigated, or lowered.

- If someone applies something less than due care, then their liability will be higher. **(negligence)**

But the 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 put aside FTC order directing the now defunct LabMD to overhaul its data security program

What Courts Mean by “Reasonable Safeguard”

Safeguards should ***not be more burdensome than the risks they protect against***.

- “Calculus of Negligence” and “Multi-Factor Balancing Tests”
- Consider foreseeable threats, their likelihood and impact, the reason the risk is engaged, and the burden of alternative safeguards.

The “Calculus of Negligence”

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

R	=	L	x	I
Risk		**Likelihood**		**Impact**
		of occurrence		or the cost of the impact should the risk be realized

How Current Security Assessments Are Failing Us

	Evaluates Risk to Information Assets						Evaluates Due Care		
Method	**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**
DoCRA CIS RAM	●	●	●	●	●	●	●	●	●
IT Risk Assessments ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◑	●	○	○	◔
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◑	○	○	○	○	○	○	○
Maturity Model Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	○	○	○	○

How Assessment Models Answer the Question “Were Your Controls ***Reasonable***?”

Assessment Method	Response	Judge/Regulator Reply
Maturity Models	“The control was a ‘3’. We decided to not go to ‘4’.”	“I don’t know what that means.”
Gap Assessments	“The auditor said we were compliant.”	“Compliance is not a measure of reasonableness.”
ISO 27005 / NIST SP 800-30 / FAIR	“Management accepted the risk to the asset.”	“You didn’t consider the harm to the public?”
CIS RAM / DoCRA	“The control provided a reasonable balance between foreseeable harm and the burden to sustain the control.”	“That is due care.”

DoCRA

But First …

Today
HEALTH CARE
WEBSITE SECURITY
REP. DARRELL ISSA
R-California, Oversight & Government
Reform Committee - Chairman
C-SPAN3
c-span.org
HD

NIST SP 800-30 and the Designated Approving Authority

2.1 IMPORTANCE OF RISK MANAGEMENT

... The DAA or system authorizing official is responsible for determining whether the remaining risk is at an acceptable level or whether additional security controls should be implemented to further reduce or eliminate the residual risk before authorizing (or accrediting) the IT system for operation.

4.5 COST-BENEFIT ANALYSIS

… after the appropriate controls have been put in place for the identified risks, the DAA will sign a statement accepting any residual risk and authorizing the operation of the new IT system or the continued processing of the existing IT system.

Historic Impact Scoring

- The focus has been on the impact to the asset
- Narrative written that tries to communicate organizational risk to operations, budgets, reputation, or growth
- No framework to interpret impacts on the asset to the real impact on the organization … or 3rd parties

Traditional Risk Register

Impact Scoring on Asset

Analysis on Asset

Observations	Likelihood Exploi		rall Risk	Risk Analysis
Third Party vendor access/risk management does not exist. The HVAC system is on the network running Windows XP and is accessed remotely by the vendor	10		100	Unsecure networks and systems can introduce vulnerabilities and attack vectors increasing the risk of compromise.
Very little traffic from the internet is blocked at the firewall level.	1	10	0	Potential for compromise is high where most traffic is allowed to traverse the firewall and enter the ACME network.

If We Could Write The Perfect Standard …

that made as much sense to **judges** and **regulators** as it does to security experts and management, what would it include?

The Ideal Risk Assessment Standard Would Include

Component	Description
Standard of Care	A listing of known-effective controls
Identifies Vulnerabilities	Knowable and potential liabilities
Considers Threats	Foreseeable actions that create harm
Evaluates Harm to Self	Estimation of severity of the harm to the organization
Evaluates Harm to Others	Estimation of the gravity of the injury to others
Estimates Likelihood	Estimation of how foreseeable the harm is
Defines Acceptable Risk	A clear definition for the tolerance of all interested parties
Defines Reasonableness	A clear definition for when safeguards are too demanding
Evaluates Safeguard Risk	A test to determine whether safeguards are reasonable

That New Standard is Now Available to the Public

DoCRA

CIS Controls™

CIS RAM Version 1.0

Center for Internet Security®
Risk Assessment Method

For Reasonable Implementation and Evaluation of CIS Controls™

Why Business Management Likes Duty of Care Risk Analysis

Risk Management is About **Reciprocity**

Expect me to reduce the risk of harm to you.

But don’t expect me to break myself in the process.

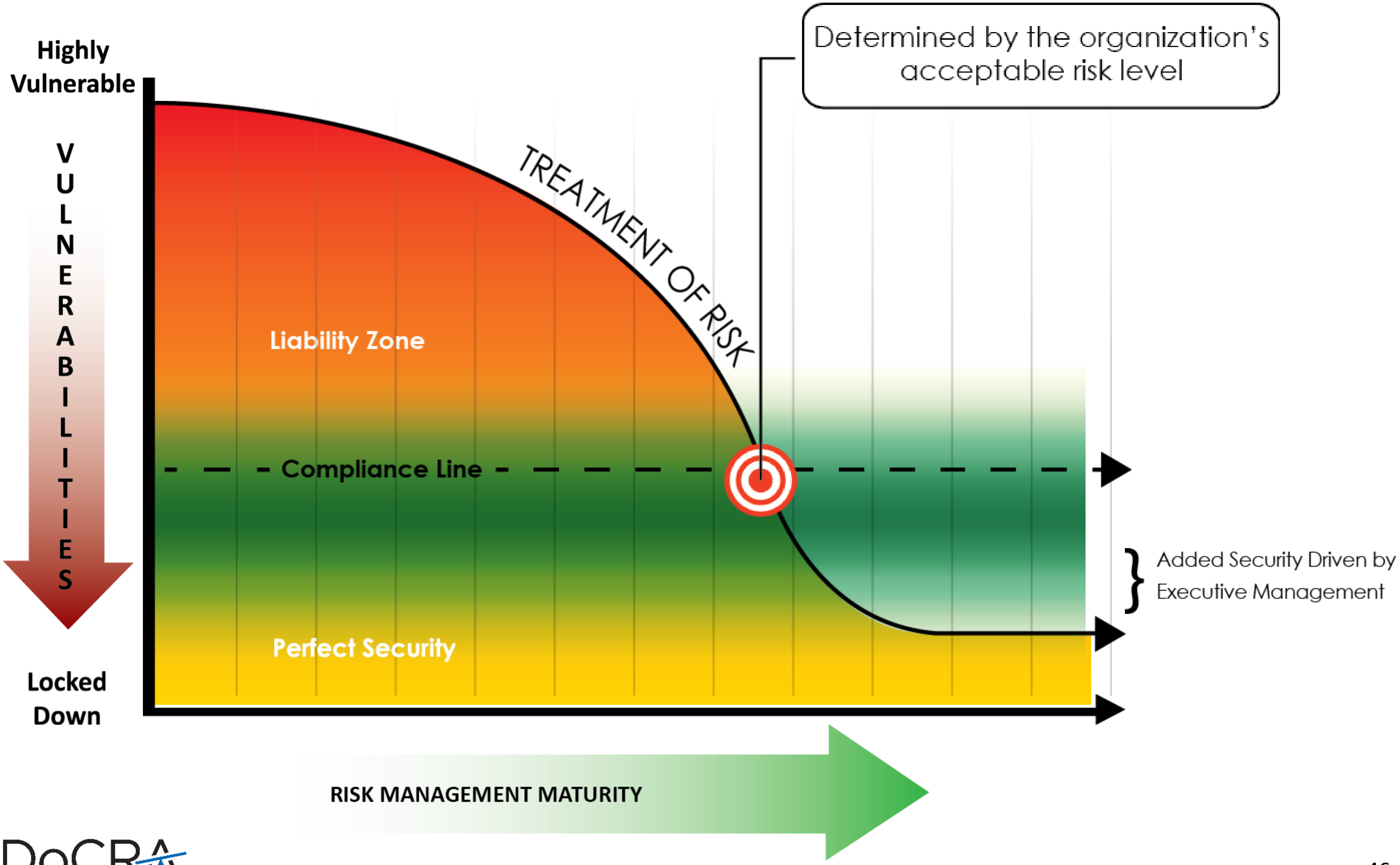
Because I would never expect you to break in order to protect me.

An *Incomplete* Risk Heat Map Considers *One Type* of Impact

		Impact				
		1 = Negligible	2 = Low	3 = Moderate	4 = High	5 = Disaster
Likelihood	5 = 1/Day	5	10	15	20	25
	4 = 1/Month	4	8	12	16	20
	3 = 1/Yr	3	6	9	12	15
	2 = 1-3 Yrs	2	4	6	8	10
	1 = > 3 Yrs	1	2	3	4	5

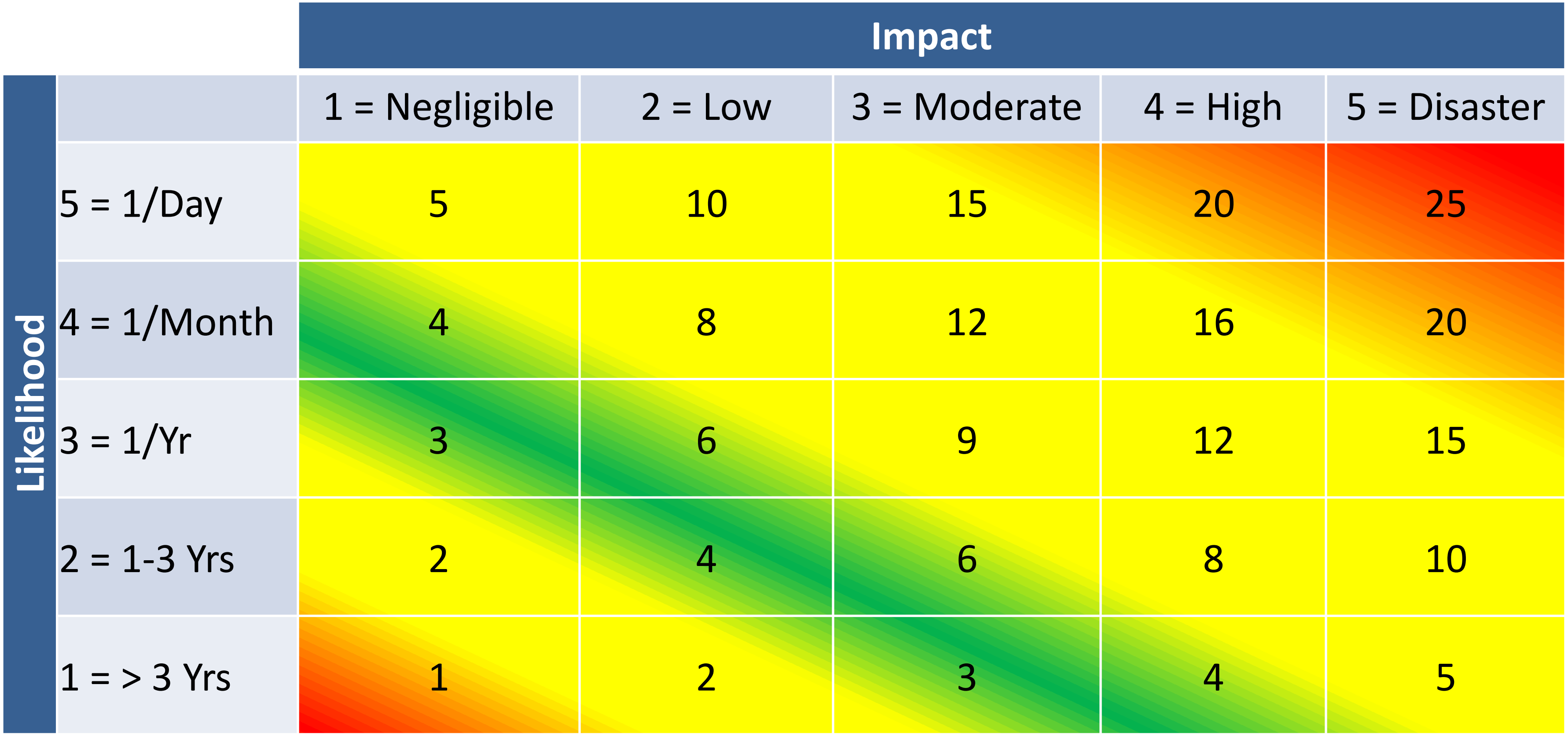
Is a risk score of ‘1’ a reasonable goal?

Reducing Liability Over Time



DoCRA

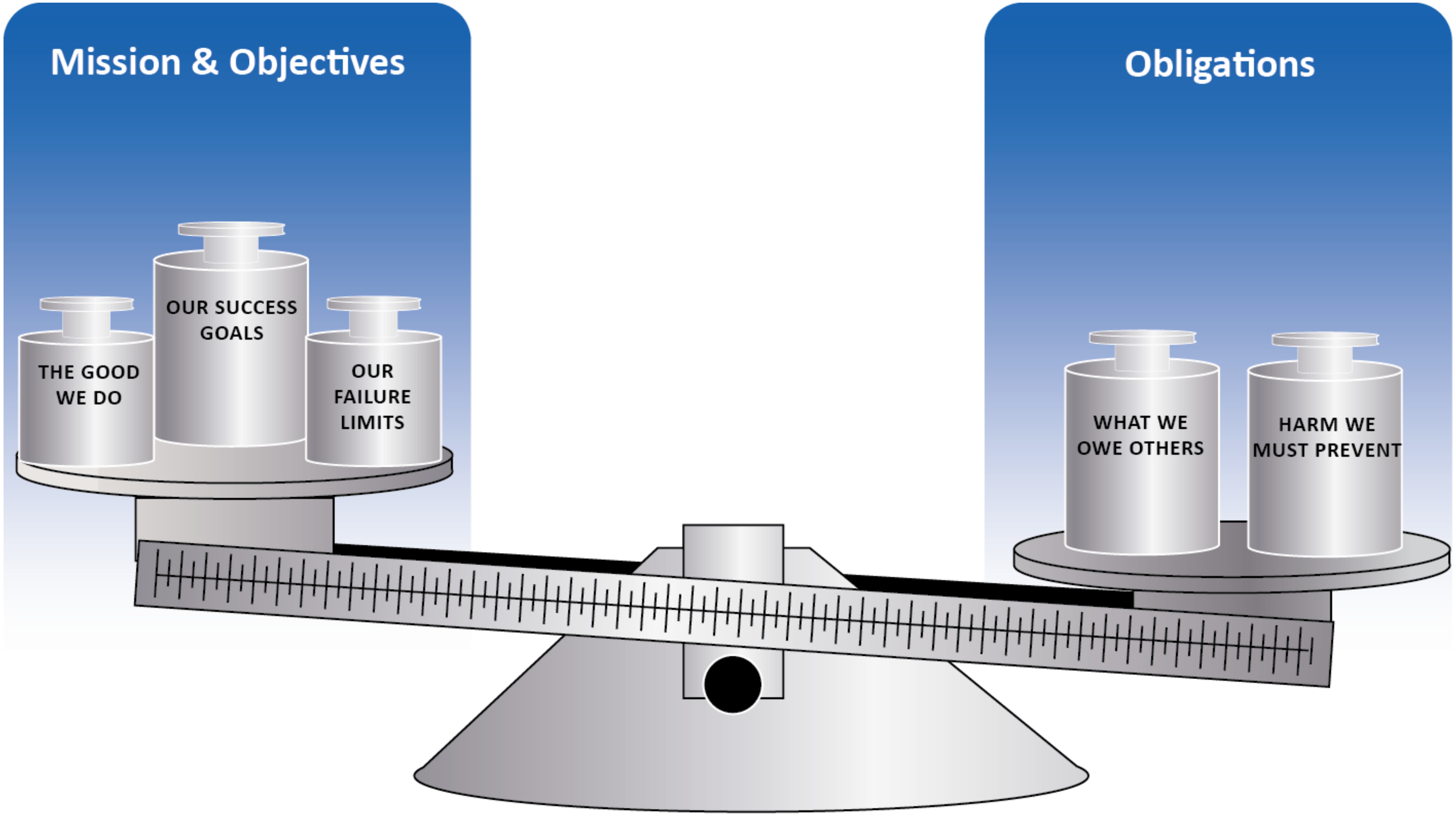
A ***More Accurate*** Risk Heat Map Balances Impacts ***Against Each Other***



		Impact				
Likelihood		1 = Negligible	2 = Low	3 = Moderate	4 = High	5 = Disaster
	5 = 1/Day	5	10	15	20	25
	4 = 1/Month	4	8	12	16	20
	3 = 1/Yr	3	6	9	12	15
	2 = 1-3 Yrs	2	4	6	8	10
	1 = > 3 Yrs	1	2	3	4	5

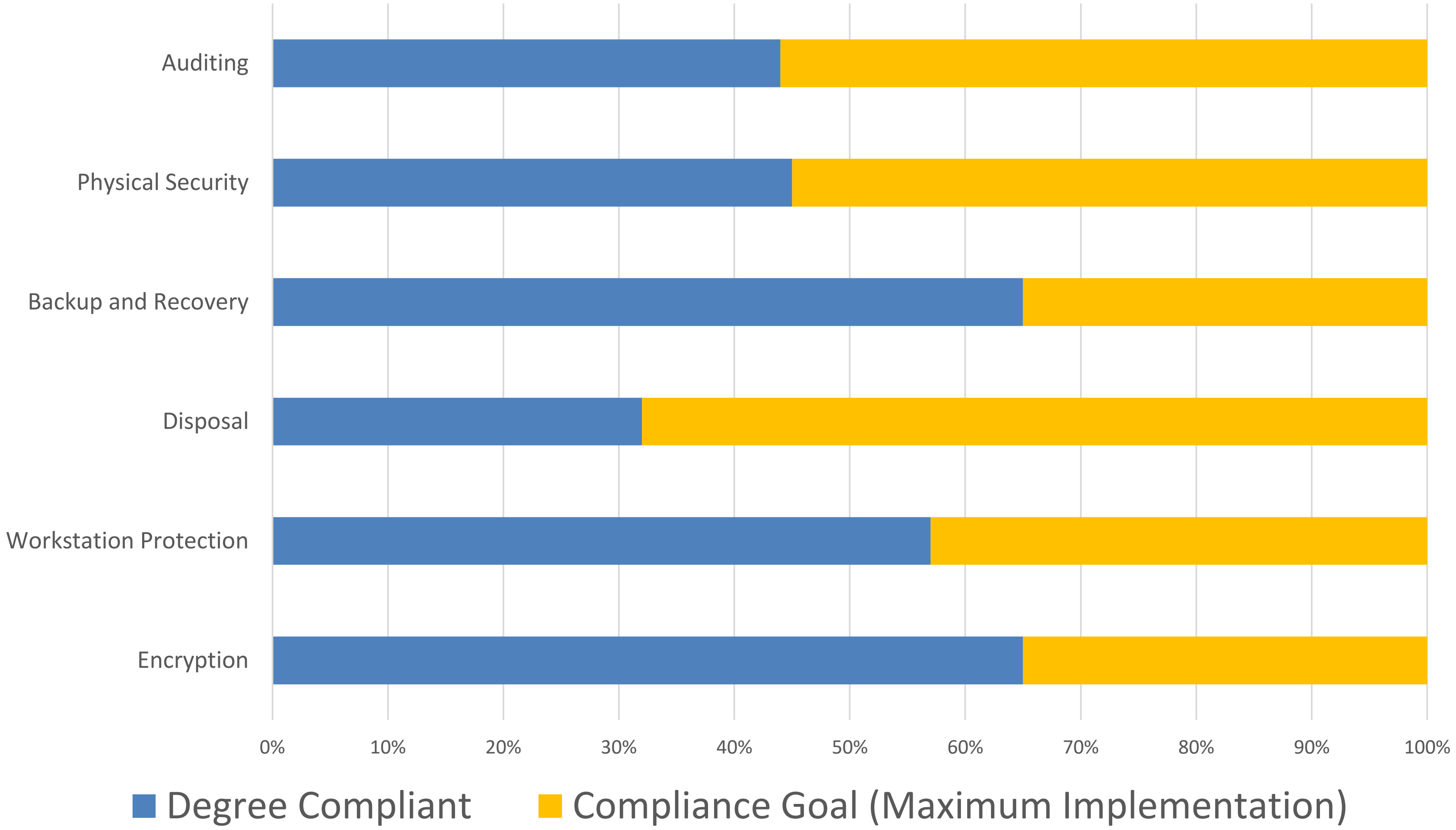
Maybe an information risk of ‘*1*’ creates an *unreasonable* business risk!

Risk Assessments are Questions of Balance



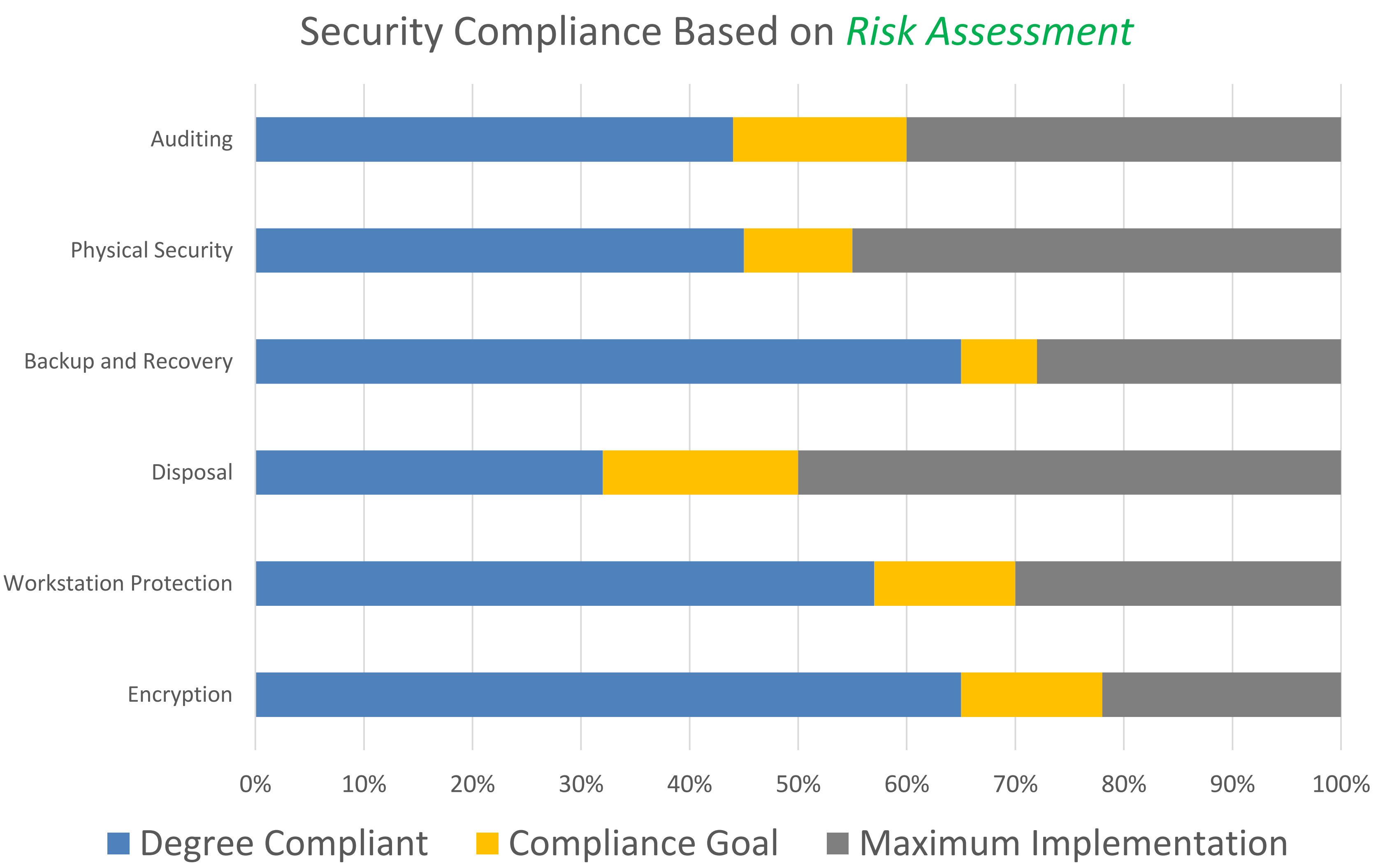
Efficiency of Risk-Based Compliance:
The **Expected** Response to Audit Findings

Compliance and Remediation Based on *Audits to Standards*



DoCRA

Efficiency of Risk-Based Compliance: The **Reasonable** Response to Risk Findings



DoCRA

POLL QUESTION #3

Our organization uses risk assessments as a cost benefit analysis for prioritizing risk treatments.

- Highly agree
- Somewhat agree
- Disagree
- I Don’t know

How Do We Calculate the Acceptable Risk Definition?

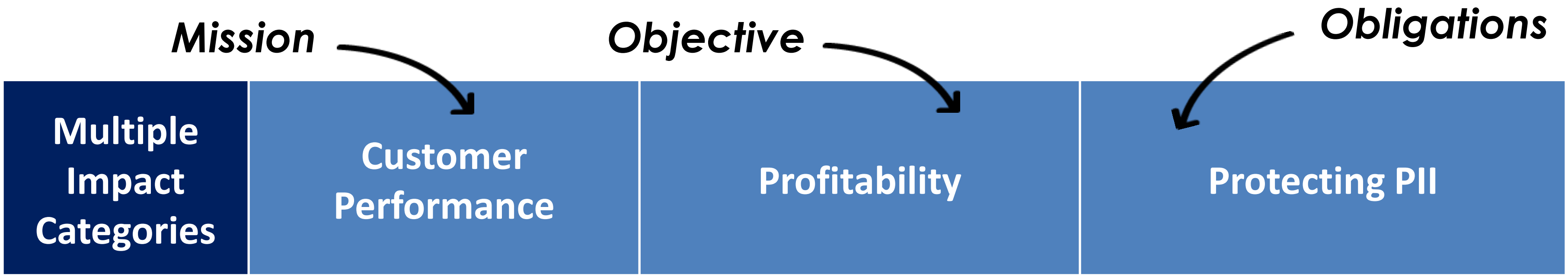
Acceptable Risk < Intolerable Impact X Expected at some point

1. Negligible impact
2. Tolerable impact
3. [✓ 3. Intolerable impact]
4. Requires major recovery
5. Maybe not recoverable

1. Not Foreseeable
2. Foreseeable, but not expected
3. [✓ 3. Expected at some point]
4. A common occurrence
5. Continuous

Calculated Acceptable Risk Definition

Duty of Care Risk Scoring



Mission

Objective

Obligations

Multiple Impact Categories

Customer Performance

Profitability

Protecting PII

- Identify the following to prepare risk criteria:
  - Your **<u>Mission</u>**: What you do for the world.
  - Your **<u>Objectives</u>**: What you do for yourself.
  - Your **<u>Obligations</u>**: The care you owe others.

Hospital's Full Risk Assessment Criteria

Impact Score	Mission "Health Outcomes"	Objectives "Balanced Budget"	Obligation "Patient Privacy"
1. Negligible	Health outcomes would not be effected.	Budget would not be effected.	Patients' privacy would not be harmed.
2. Low	Patients would feel inconvenienced.	Budget performance within planned variance.	Patients would be concerned, but no harm would result.
3. Medium	Some patient's health outcomes would suffer.	Budget variance would be recoverable within a year.	Few patients would suffer reputational or financial harm.
4. High	Many patient health outcomes would suffer.	Budget would be recoverable after multiple years.	Many patients would suffer reputational or financial harm.
5. Catastrophic	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 x 3 = **9**
Accept Risk	**Less than 9**

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

DoCRA

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

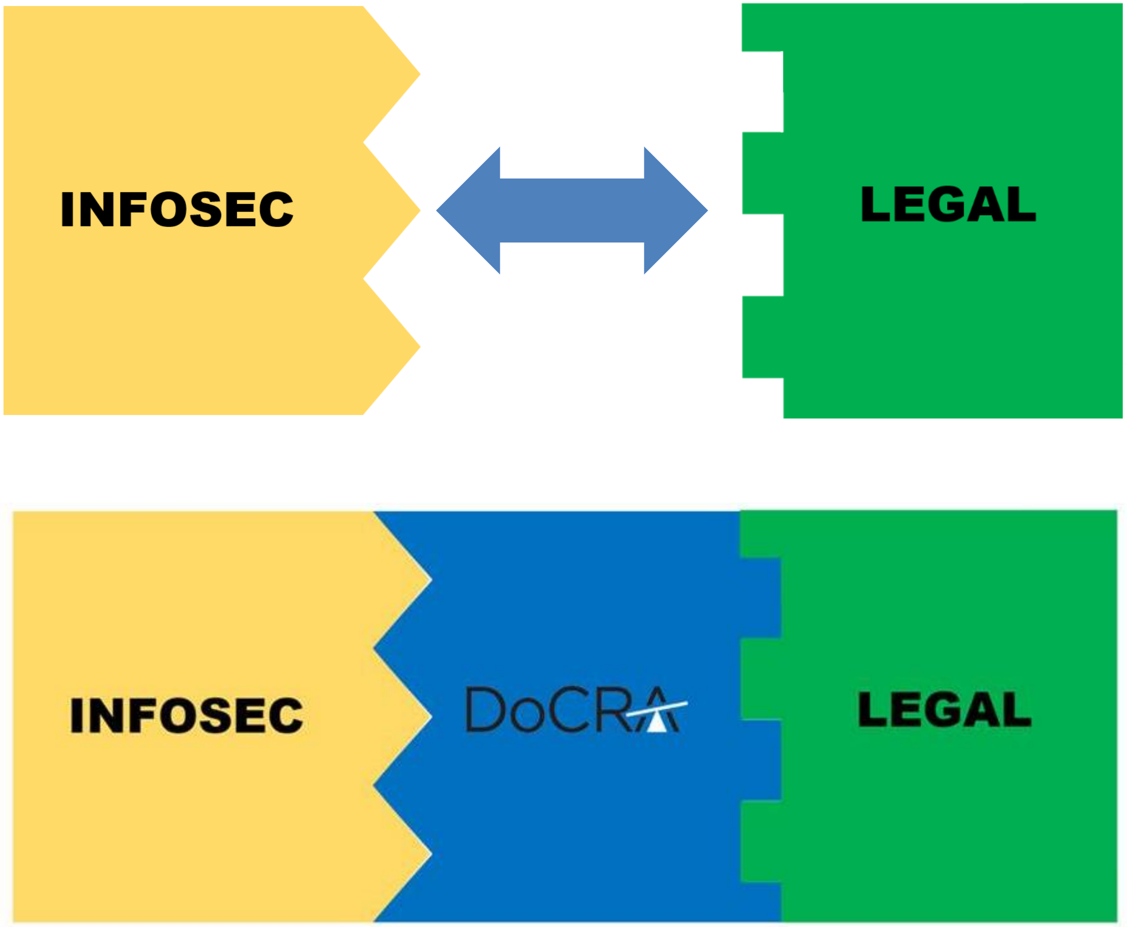
Likelihood	Risk Score: Max(Impact) x Likelihood
➡ 3	12

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

Solving The Communication Gap



INFOSEC

LEGAL

INFOSEC

DoCRA

LEGAL

Duty of Care Risk Analysis provides

- Method to evaluate risk by **calculating potential impact ("injury")** to
  - Organization's customers
  - Mission and business objectives
  - External entities
- Method to define **Acceptable Risk**
- Prioritized risks needing treatment

Security Assessments as Defense?

	Evaluates Risk to Information Assets						Evaluates Due Care		
Method	**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**
DoCRA CIS RAM	●	●	●	●	●	●	●	●	●
IT Risk Assessments ISO 27005, NIST SP 800-30, RISK IT	●	●	●	●	◑	●	○	○	◔
FAIR Factor Analysis for Information Risk	○	●	●	●	○	●	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	●	◑	○	○	○	○	○	○	○
Maturity Model Assessments 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'.

DoCRA

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.

Regulator: 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?

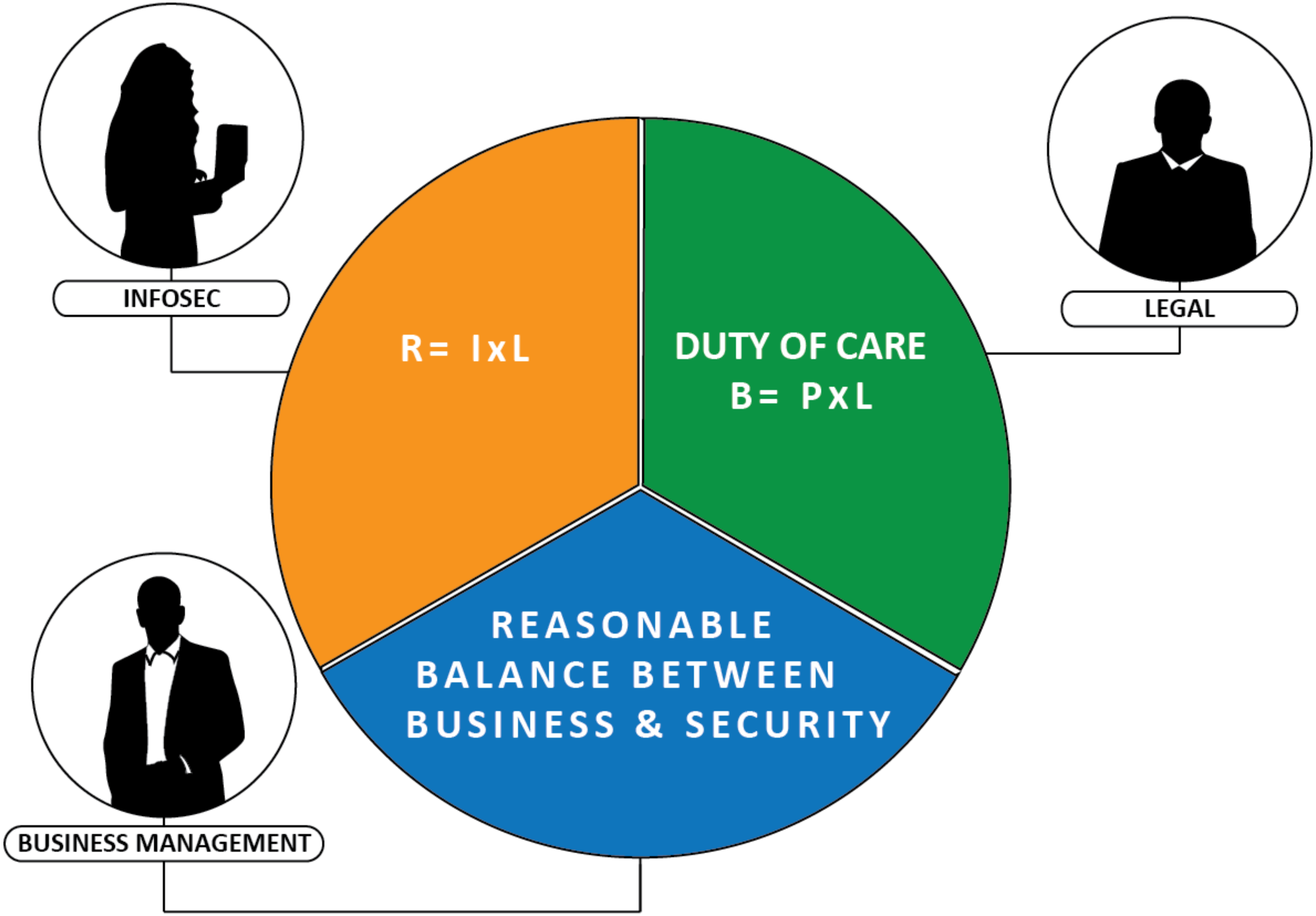
Regulator: Nice job evaluating the threat. I see the dollar value of your potential losses. But I don't think this control is appropriate for the risk.

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: …

Duty of Care Risk Assessments "DoCRA" Align the Organization



Summary

Develop and mature your risk management program

Update your risk assessment criteria to align with DoCRA

- **Defend proactively** against a breach
- **Align the needs** of the business, security, internal audit, the board, regulators and legal
- **Prioritizes risks** and risk treatments
- Declares an **acceptable level of risk** with simple math
- **Establish a Duty of Care Risk Analysis (DoCRA)** that will hold up in front of <u>all interested parties</u>

How Do Organizations Adopt CIS RAM/DoCRA?

- Download CIS RAM from 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.

POLL QUESTION #4

I would like to receive the *Duty of Care Risk Assessment (DoCRA) Checklist* and the *SANS Security Leadership Poster: Five Keys for Building a Cybersecurity Program*

- Yes
- No

Questions

Jennifer Urban Rathburn

Partner
Foley & Lardner LLP

Terry Kurzynski,
CISSP, CISA, PCI QSA,
ISO 27001 Auditor

Board Member
The DoCRA Council