DoCRA

The Questions a Judge Will Ask You When You are Sued for a Data Breach

Getting to Reasonable Security

HALOCK®

Presenters

Aaron DeMaster

Cyber Security Manager
Rexnord Corporation

Terry Kurzynski,

Board Member, The DoCRA Council

Senior Partner, HALOCK Security Labs

Aaron DeMaster

- **President of the Midwest Cyber Security Alliance**
- Cyber Security Manager at Rexnord Corporation
- CRISC and CISM
- CISA, ISO 27001 Auditor, CompTIA Security +
- Retail, Healthcare, Financial, and Manufacturing industries
- Information Security since 2010

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

Who is Rexnord?

- Headquartered in Milwaukee, WI
- Global organization 70+ locations
- Parent company for several brands
- 5000+ Employees
- Manufacturer of gears, bearings, couplings, chain, & water systems
- Critical Business Systems
  - IoT
  - ERP – SAP, Axapta, Navision
  - E-commerce – Azure & IBM Cloud
  - Financial systems

REXNORD aerospace

FALK®

Link-Belt®

ZURN®

BERG

highfield

Rexnord Corporation Case Study
Problem Statement

- **Maturity Model Assessments lacked meaning**
  - “what does that mean?” - Rexnord Executive
- **Internal Audit Findings not prioritized**
  - Internal Audit provided a list of corrective actions based on IT General Controls
  - Cyber Security was performing NIST CSF maturity assessments
- **Executive Management desires comparison to peer companies**
  - Peer companies were being breached
  - Information about peer company maturity of controls was hard to come by
- **Investment/Remediation Justification and Support**
  - Lack of insights on impacts/benefits to the business
  - Lack of leadership support on cyber security initiatives

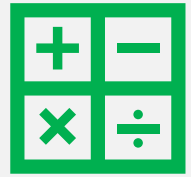
But There are More (Problems)

- Defending your security program after a breach
- Legal community is looking for something different then what the Cyber Security community is providing
- Satisfying lots of interested parties:
  - Executive Management
  - Regulators
  - Clients and Business Partners
  - Attorneys/Judges
  - Internal Audit
  - Information Technology
  - Cyber Security

Topics

THE AGE OF RISK AND HOW WE GOT HERE

STORIES OF BREACHES, LAWSUITS, AND REDEMPTION



THE RISK EQUATION YOU SHOULD KNOW

The Age of Risk

The Age of Controls

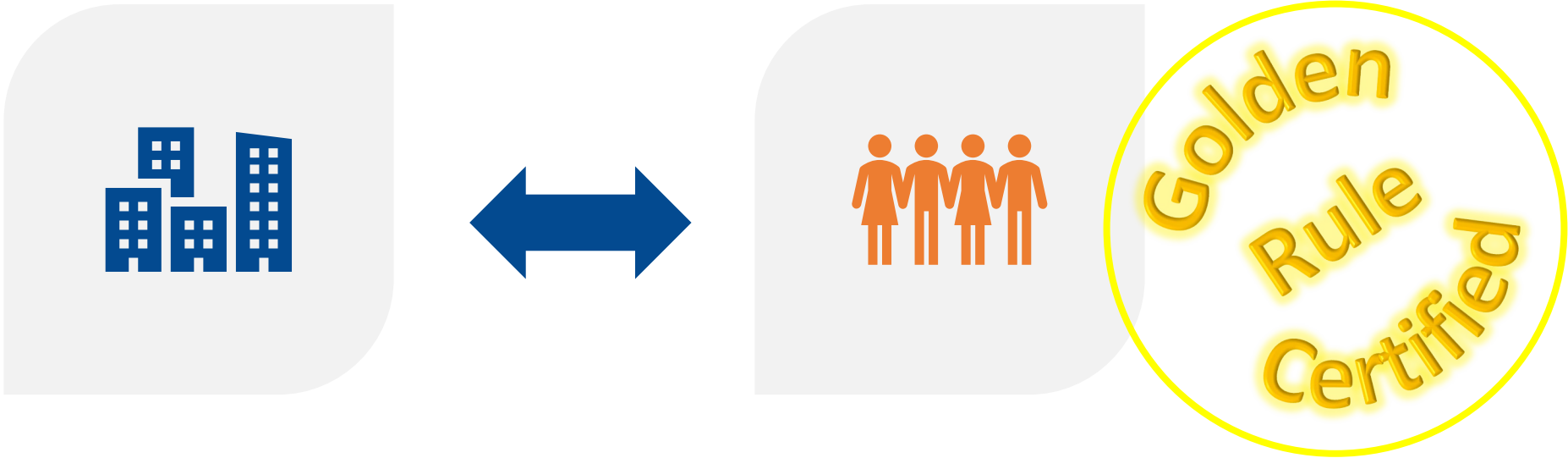
The Age of Compliance

The Age of Risk

How We Evaluate Controls in the Age of Risk

- Think through the **likelihood** and **impact** of threats
- Reduce unacceptably high risks …
- … using controls that are no more burdensome than the risks

Our Security Objectives in the Age of Risk



WE LOOK OUT FOR YOU

YOU LOOK OUT FOR US

How Do We Accomplish That?

PROTECT OTHERS FROM FORESEEABLE HARM

BUT WE **DON'T HARM OURSELVES** MORE IN THE PROCESS

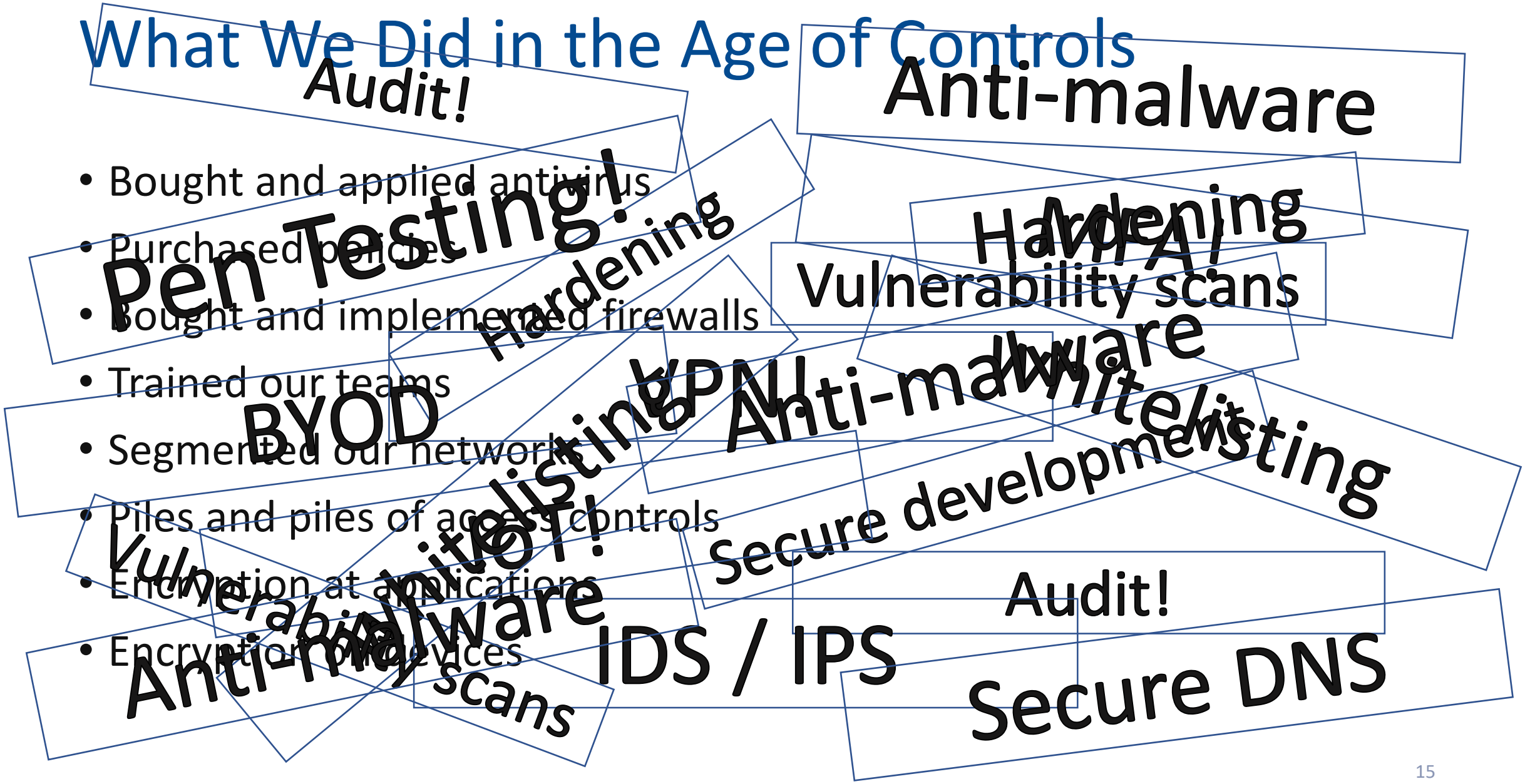
Who Brought Us to the Age of Risk?

Laws and Regulations	Standards and Frameworks
GLBA Safeguards Rule	NIST Risk Management Framework (800 Series)
HIPAA Security Rule	NIST Cybersecurity Framework
SOX Audit Standard 5	ISO 27000 Family
201 CMR 17.00	CIS Controls / CIS RAM
23 NYCRR Part 500	CobiT / RISK IT
CCPA	SOC 2
GDPR (implicit)	SOC for Cybersecurity
Federal Trade Commission	
Courts	

The Age of Controls

What We Did in the Age of Controls

- Bought and applied antivirus
- Purchased policies
- Bought and implemented firewalls
- Trained our teams
- Segmented our networks
- Piles and piles of access controls
- Encryption at applications
- Encryption on devices



To: CIO

From: CFO

Where does this end?

Do we have a plan, or do we just keep buying more tech?

The Board Room in the Age of Controls

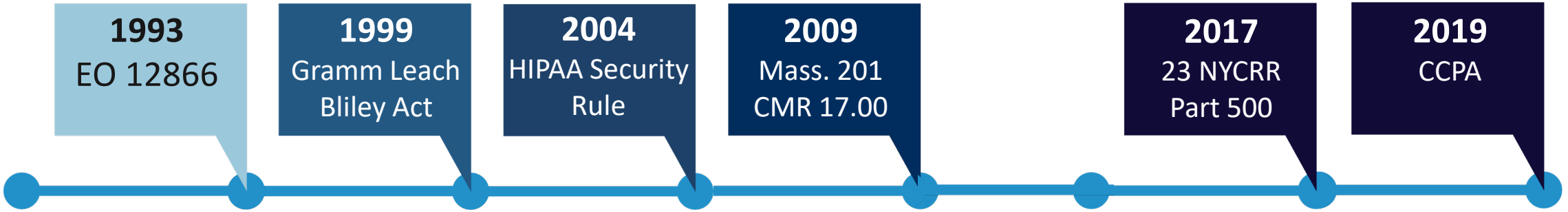
- “These security requisitions don’t make sense to me.”
- “Why are we spending this money?”
- “How do we compare to our peers. Shouldn’t we just do what they do?”
- “Information security is an insurance policy I don’t want to pay for.”
- “I just read an article about breaches on copy machines. Stop everything you’re doing and fix this copy machine problem!”
- “And if we get breached … You’re fired!”

Something We Did Not Understand About Laws and Regulations

- United States laws and regulations were developed in an entrepreneurial society …
- … so we had to shape laws and regulations so they made 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."



Courts Look for the “Reasonable Person”

- Someone who thinks through the likelihood and impact of threats that might create harm …
- … designs safeguards that are **not more burdensome than those risks**

The risk to those who are protected by controls.

The burden to us when we apply the controls.

Communicating Controls in the Controls Age From the Board Room to the Court Room

The Case of the Negligent Retailer

- Major credit card breach.
- Highly sophisticated attack.
- Retailer had no DLP to block the exfiltration of card data.
- The reason management gave CIO for not funding DLP …
  - *“We don’t have enough money for all the things you want to buy.”*
- The reason the CIO gave the judge for not using DLP …
  - *“We were not given the necessary funds.”*

The Case of the Negligent Retailer

- Finding … **Negligent**, with nine figures in total damages.
- What the judge would have accepted from the retailer.

"The DLP would have harmed our business more than the likelihood of harm to others. So we used 'x' control instead."

Courts Look for the “Reasonable Person”

- Someone who thinks through the likelihood and impact of threats that might create harm …
- … designs safeguards that are **not more burdensome than those risks**

The risk to those who are protected by controls.

The burden to us when we apply the controls.

Lesson of the Case of the Negligent Retailer

If your security needs don’t make sense to business, they won’t make sense to **judges** either.

The Age of Compliance

What We Did in the Age of Compliance

- Selected a controls framework
  - NIST
  - ISO
  - Center for Internet Security
  - PCI DSS
  - HITRUST
  - SOC 2
- Ignored their risk assessment requirements.
- Ran gap maturity assessments instead
- Developed remediation plans
- Attained certifications

Gap Assessments and Audits

NIST 800-53	Control Title	NIST CSF	Compliant
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		
AC-2	ACCOUNT MANAGEMENT	PR.AC-4, DE.CM-1	
AC-3	ACCESS ENFORCEMENT	PR.PT-3	
AC-4	INFORMATION FLOW ENFORCEMENT	PR.AC-5, PR.DS-5, PR.PT-4	
AC-5	SEPARATION OF DUTIES	PR.AC-4, PR.DS-5	
AC-6	LEAST PRIVILEGE	PR.AC-4, PR.DS-5	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS		
AC-8	SYSTEM USE NOTIFICATION		
AC-11	SESSION LOCK		
AC-12	SESSION TERMINATION		
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION		
AC-17	REMOTE ACCESS	PR.PT-4, PR.AC-3	
AC-18	WIRELESS ACCESS	PR.PT-4	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	PR.AC-3	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	PR.AC-3	
AC-21	INFORMATION SHARING	PR.IP-8	

Adding Value in the Age of Compliance:

Multi-color icons were more appealing than “pass/fail” text.

Pseudo-Risk Assessments

NIST 800-53	Control Title	NIST CSF	Risk
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		
AC-2	ACCOUNT MANAGEMENT	PR.AC-4, DE.CM-1	
AC-3	ACCESS ENFORCEMENT	PR.PT-3	
AC-4	INFORMATION FLOW ENFORCEMENT	PR.AC-5, PR.DS-5, PR.PT-4	
AC-5	SEPARATION OF DUTIES	PR.AC-4, PR.DS-5	
AC-6	LEAST PRIVILEGE	PR.AC-4, PR.DS-5	
AC-7	UNSUCCESSFUL LOGON ATTEMPTS		
AC-8	SYSTEM USE NOTIFICATION		
AC-11	SESSION LOCK		
AC-12	SESSION TERMINATION		
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION		
AC-17	REMOTE ACCESS	PR.PT-4, PR.AC-3	
AC-18	WIRELESS ACCESS	PR.PT-4	
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	PR.AC-3	
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	PR.AC-3	
AC-21	INFORMATION SHARING	PR.IP-8	

Adding Value in the Age of Compliance:

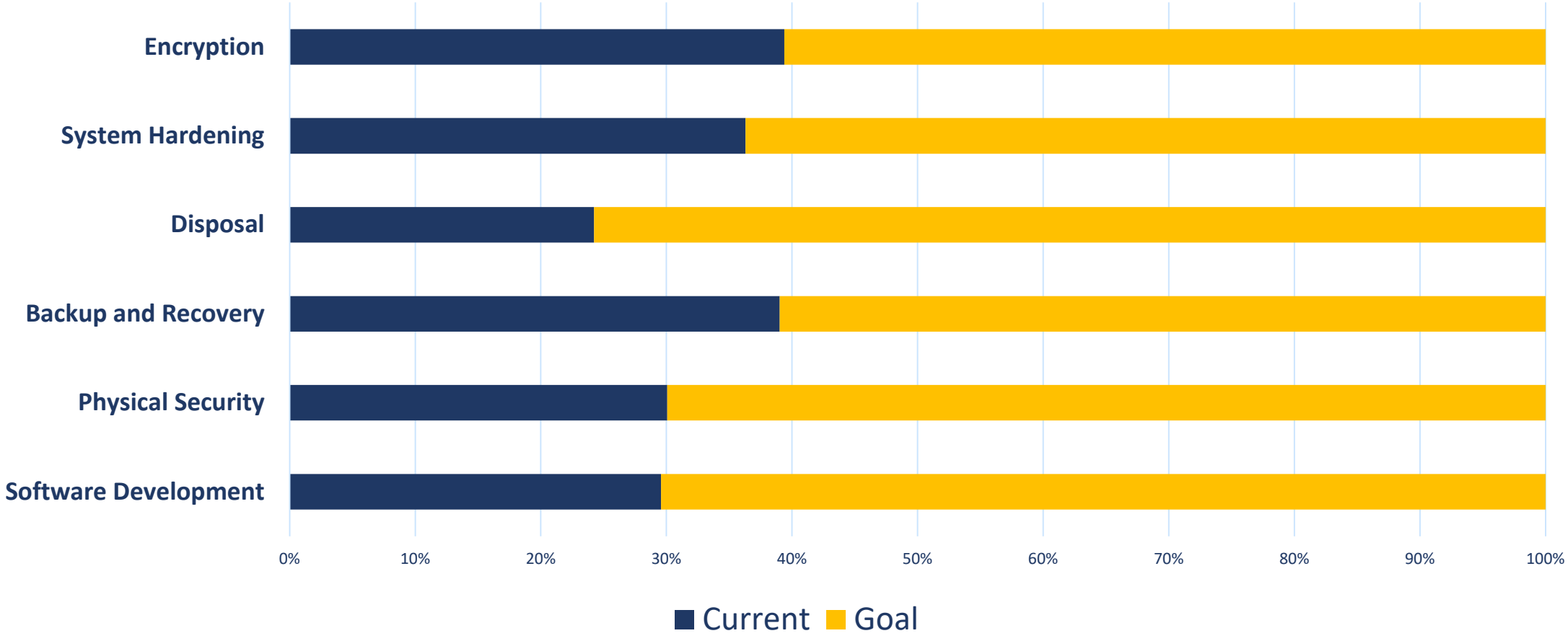
Changed "Compliant" to "Risk" so it became a risk assessment.

Maturity Assessments

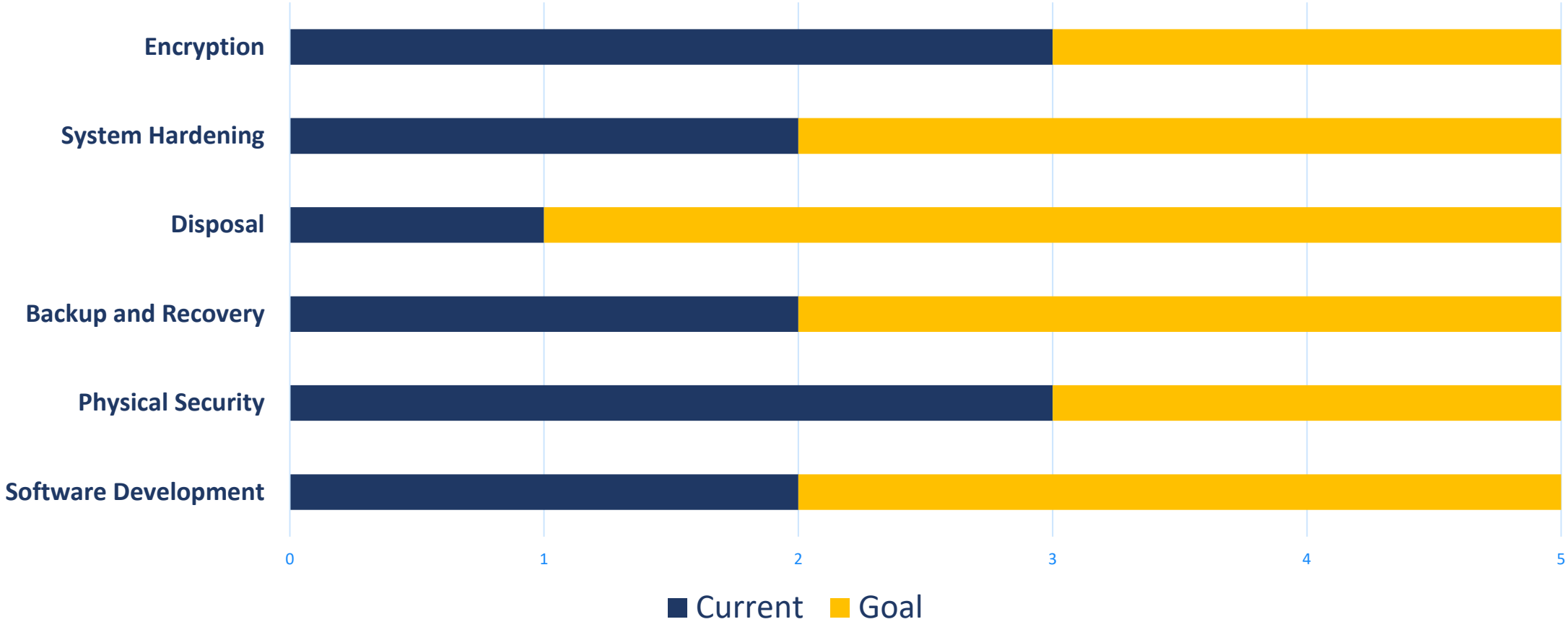
NIST 800-53	Control Title	NIST CSF	Maturity
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		5
AC-2	ACCOUNT MANAGEMENT	PR.AC-4, DE.CM-1	1
AC-3	ACCESS ENFORCEMENT	PR.PT-3	2
AC-4	INFORMATION FLOW ENFORCEMENT	PR.AC-5, PR.DS-5, PR.PT-4	1
AC-5	SEPARATION OF DUTIES	PR.AC-4, PR.DS-5	2
AC-6	LEAST PRIVILEGE	PR.AC-4, PR.DS-5	5
AC-7	UNSUCCESSFUL LOGON ATTEMPTS		5
AC-8	SYSTEM USE NOTIFICATION		3
AC-11	SESSION LOCK		4
AC-12	SESSION TERMINATION		5
AC-14	PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION		1
AC-17	REMOTE ACCESS	PR.PT-4, PR.AC-3	2
AC-18	WIRELESS ACCESS	PR.PT-4	1
AC-19	ACCESS CONTROL FOR MOBILE DEVICES	PR.AC-3	1
AC-20	USE OF EXTERNAL INFORMATION SYSTEMS	PR.AC-3	2
AC-21	INFORMATION SHARING	PR.IP-8	5

Maturity scores!
Um …. OK!
What's our target?

Our Roadmaps from the Compliance Age



Maturity Reports From the Compliance Age



Why Stand-Alone Maturity Assessments Hurt Us

Common starting point

Score	Definition
1	Unpredictable, poorly controlled, reactive
2	Project-based and reactive
3	Organization-based and proactive
4	Measured and controlled
5	Continuous improvement

Why Stand-Alone Maturity Assessments Hurt Us

Score	Definition
1	Unpredictable, poorly controlled, reactive
2	Project-based and reactive
3	Organization-based and proactive
4	Measured and controlled
5	Optimize / Continuous improvement

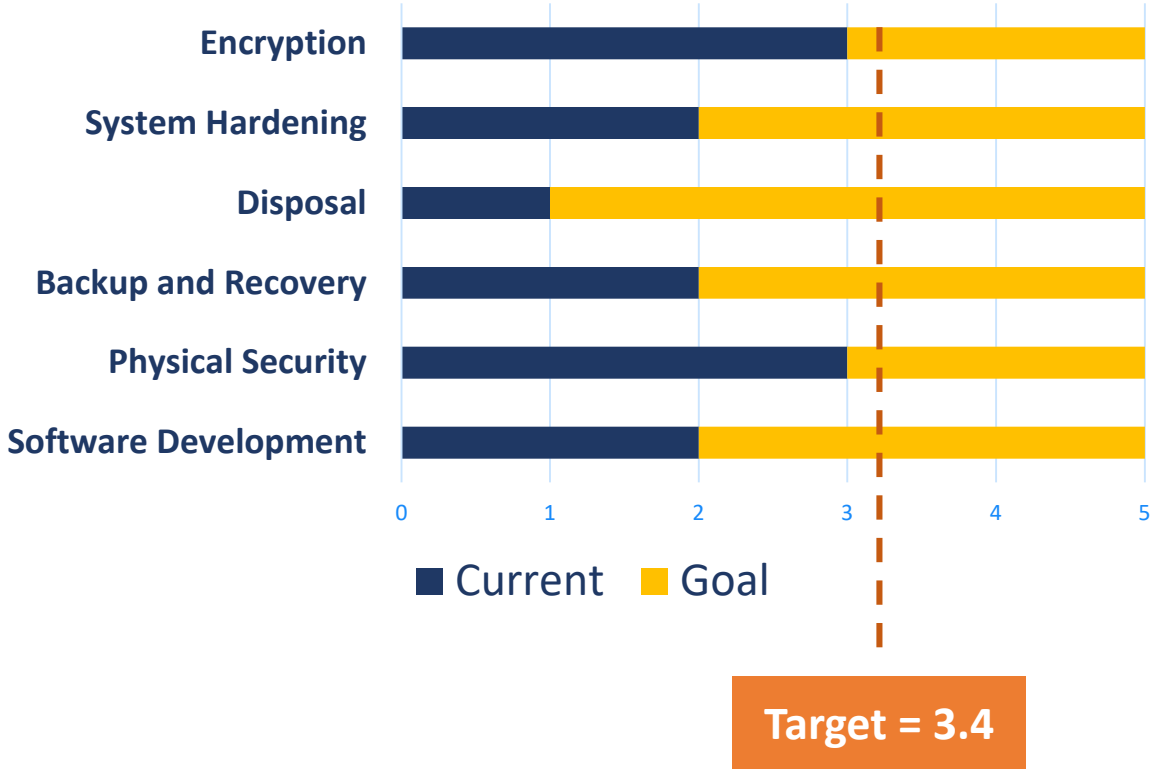
Common recommended target.

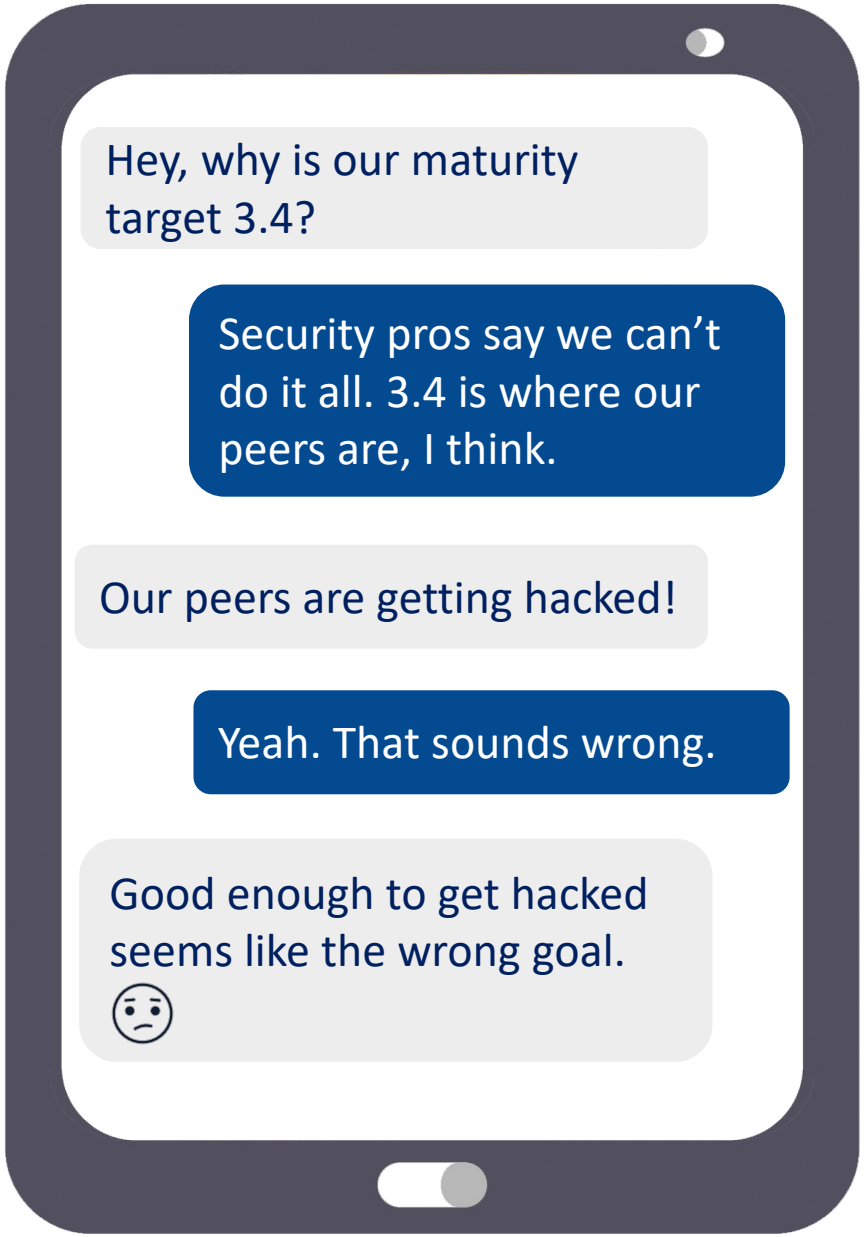
But why not here?

If You Were Using Maturity Models, and You Did Not Intend to Optimize …

- Were there parts of your organization that you optimized or improved?
  - Customer satisfaction, time-to-delivery, reduced cost, increased quality, reduced infection rates, reduced waste, increased market insight, increased return-on-assets, decreased value-at-risk, reduced spoilage, improved patient outcomes, graduation rates, retention rates, reduced turnover, reduced cost of compliance, reduced cost-of-sales, increased efficiency, higher blended rate, lower inventory, faster time-to-sale, precision in manufacturing, faster time-to-productivity …
- Then you needed a solid reason why you were not optimizing or continuously improving security.
- Judges wanted to know why you made the choice to do worse with security.

The Limits of Maturity Reports





Communicating Controls in the Compliance Age From the Board Room to the Court Room

The Case of the Hacked HITRUST Certified Payer

- Major PHI breach.
- Highly sophisticated attack on servers.
- Company did not include 10s of Millions of patient records in the scope of their PHI security program.

Regulator: “How secure was your system?”

Payer: “We were a 3.1 out of 5.”

Regulator : “Come again?”

Payer: “Three-point-one mature. Out of five. Meaning, we were HITRUST certified.”

Regulator : “HITRUST certified does not mean HIPAA compliant. Would additional controls have been more burdensome than the risk to the plaintiff?”

Payer: “Ummmm.”

The Case of the Hacked HITRUST Certified Payer

- Finding … **Negligent**, with eight figures in regulatory fines and nine figures in civil settlements.

- What the **regulator** would have considered from the payer.

  “The server was partially hardened, but securing it completely would have prevented people from using it for its purpose.”

Courts and **Regulators** Look for the "**Reasonable Person**"

- Someone who thinks through the likelihood and impact of threats that might create harm …
- … designs safeguards that are **not more burdensome than those risks**

The risk to those who are protected by controls.

The burden to us when we apply the controls.

Lesson of the Case of the Hacked HITRUST Certified Payer

If your security needs don’t make sense to business, they won’t make sense to **judges** either.

The Age of Risk

So What Are the Questions a Judge Will Ask When I Am Sued For a Data Breach?*

- 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

Sounds Like A Risk Assessment

- Estimate the likelihood of potential incidents.
- Estimate the magnitude of impact.
- Estimate the value in engaging in the risk to begin with.
- Design risk treatments that could reduce the likelihood and/or impact.

With some modification your Risk Assessment can meet **Due Care**

- 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.
- *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 Executives.***

Courts Look for the "**Reasonable Person**"

- Someone who thinks through the likelihood and impact of threats that might create harm …
- … designs safeguards that **are not more burdensome than those risks**

The risk to those who are protected by controls.

The burden to us when we apply the controls.

Why Other Assessments Come Up Short

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

** Provided by the DoCRA Council - www.docra.org. July 2018*

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

A freely available standard for conducting risk assessments.

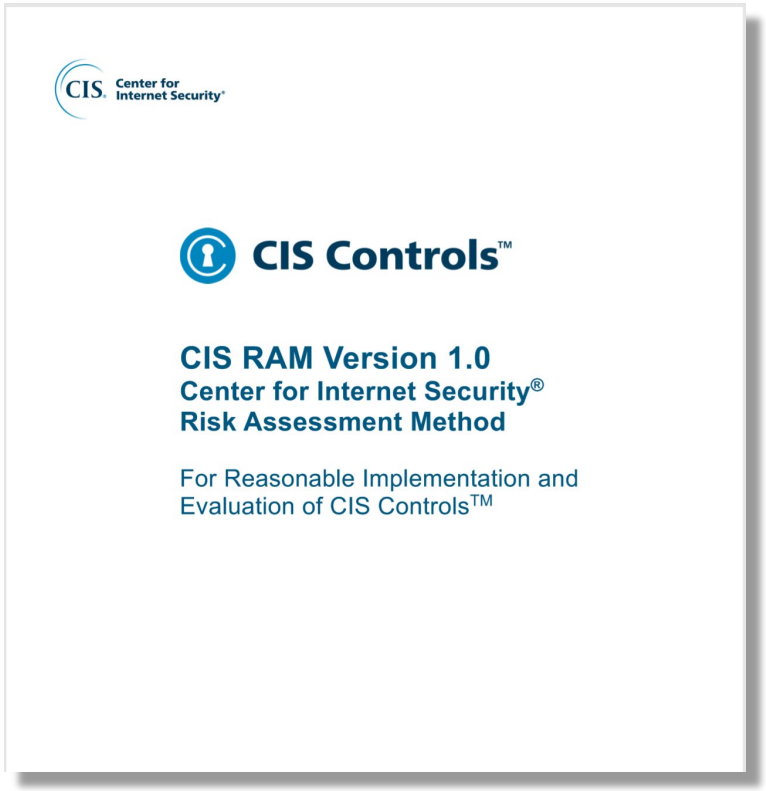
A method for demonstrating reasonableness.

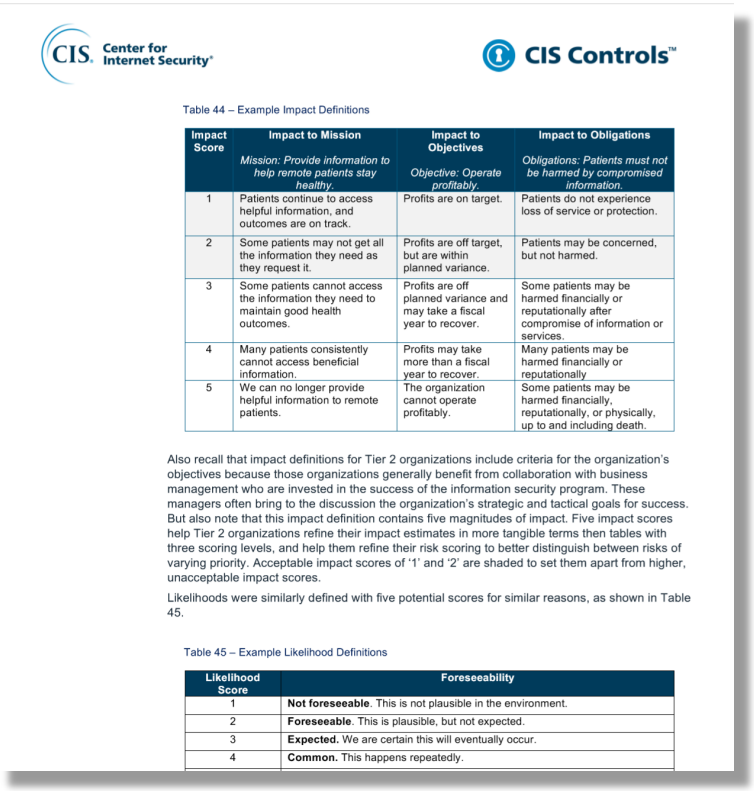
Prevails in litigation and regulation.

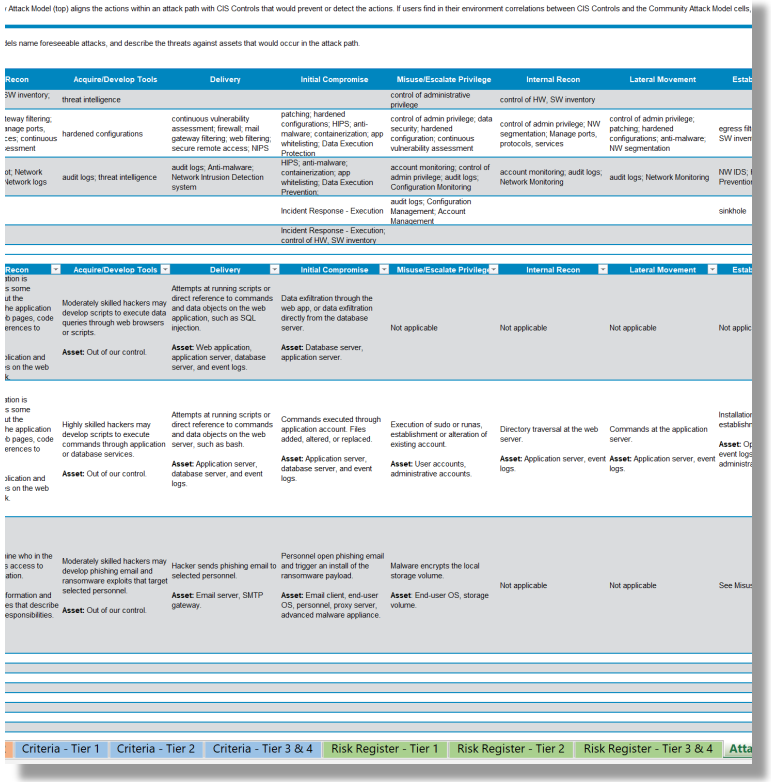
Originally developed by HALOCK Security Labs to help clients establish a goal for “enough” security.

DoCRA 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.







DoCRA Practically Applied: CIS RAM

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

Impact Scores	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	• No detected impact or impairment of mission.	• 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.

Let’s Get Real

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?

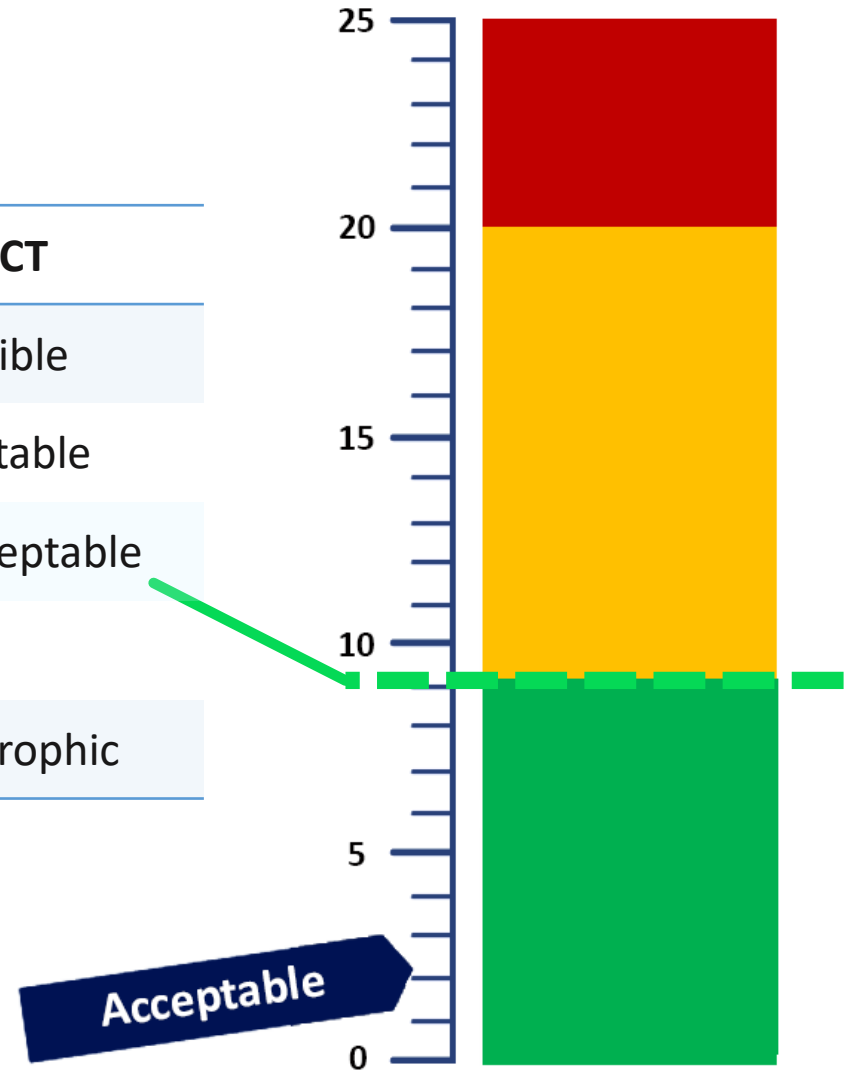
Some Common Impact Criteria

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

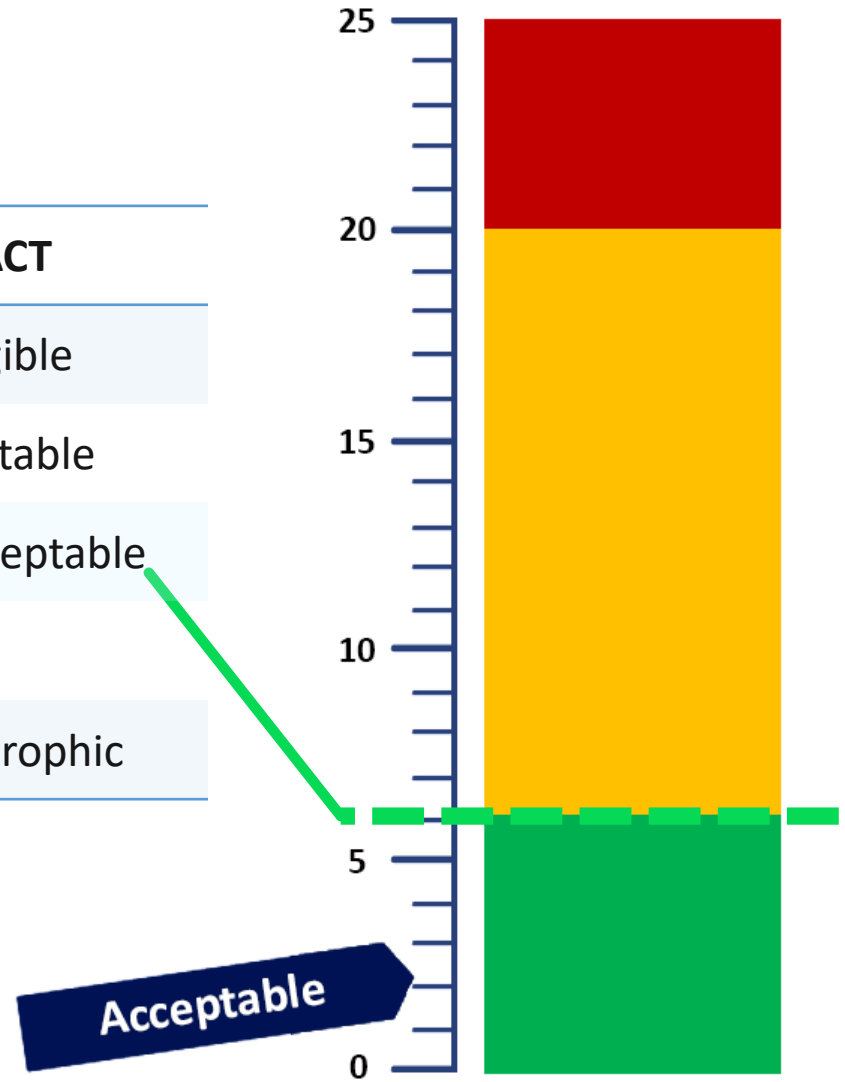
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



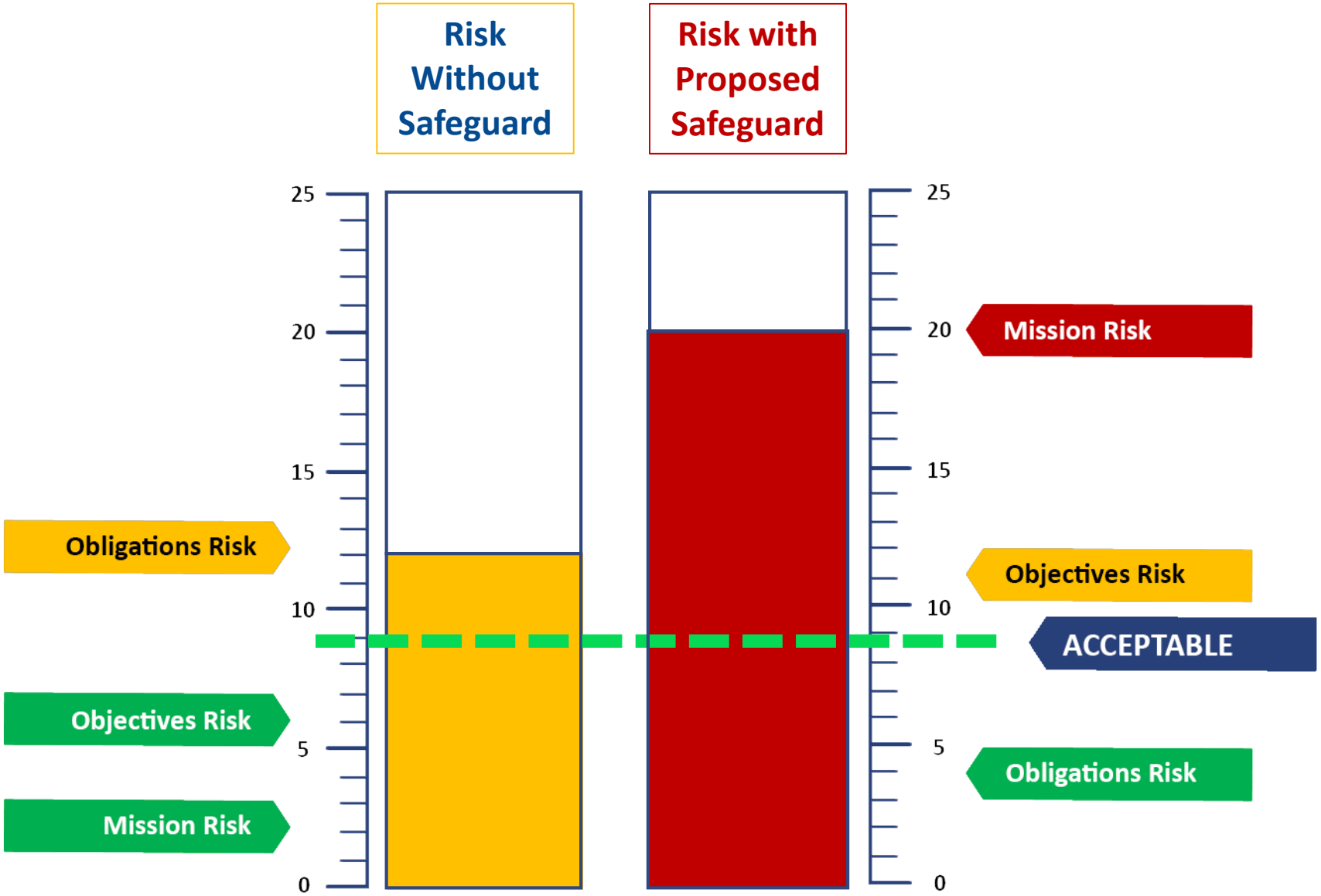
Defining Acceptable Risk

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

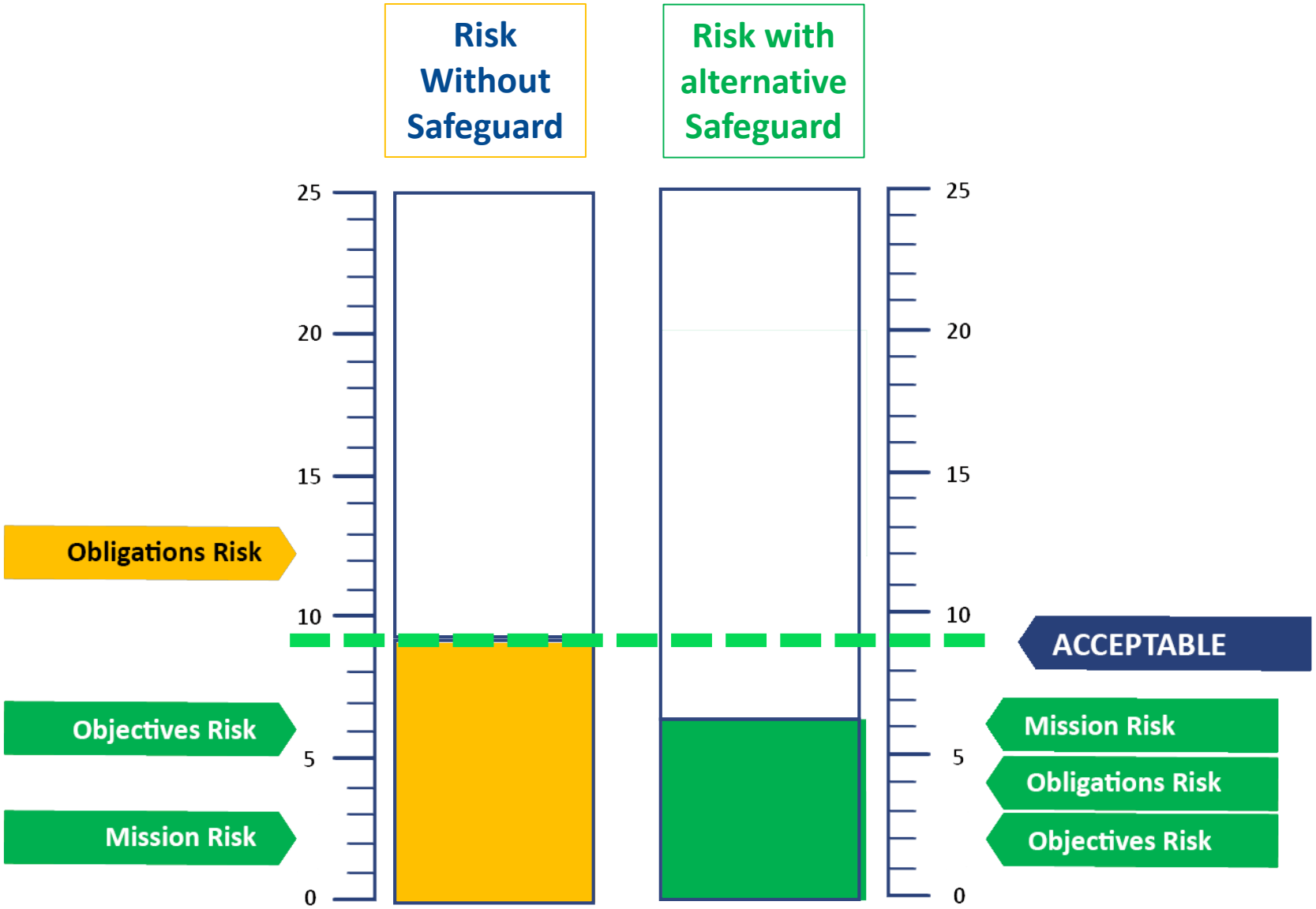
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



Some Safeguards are NOT Reasonable



Demonstrating Reasonable Safeguards



Example Unreasonable Control

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 implement packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Mission Impact	Objectives Impact	Obligations Impact
(3) One product underperforms YoY	(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers

Likelihood	Risk Score: Max(Impact) x Likelihood
(3) Foreseeable	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) One product underperforms YoY	(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers

Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
(4) Expected	16

Example Reasonable Control

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 implement packet sniffers within DMZ, capture plain-text PII, and exfiltrate data.		

Mission Impact	Objectives Impact	Obligations Impact
(3) One product underperforms YoY	(3) Missed RoA targets up to 1%	(4) Recoverable harm to thousands of customers

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

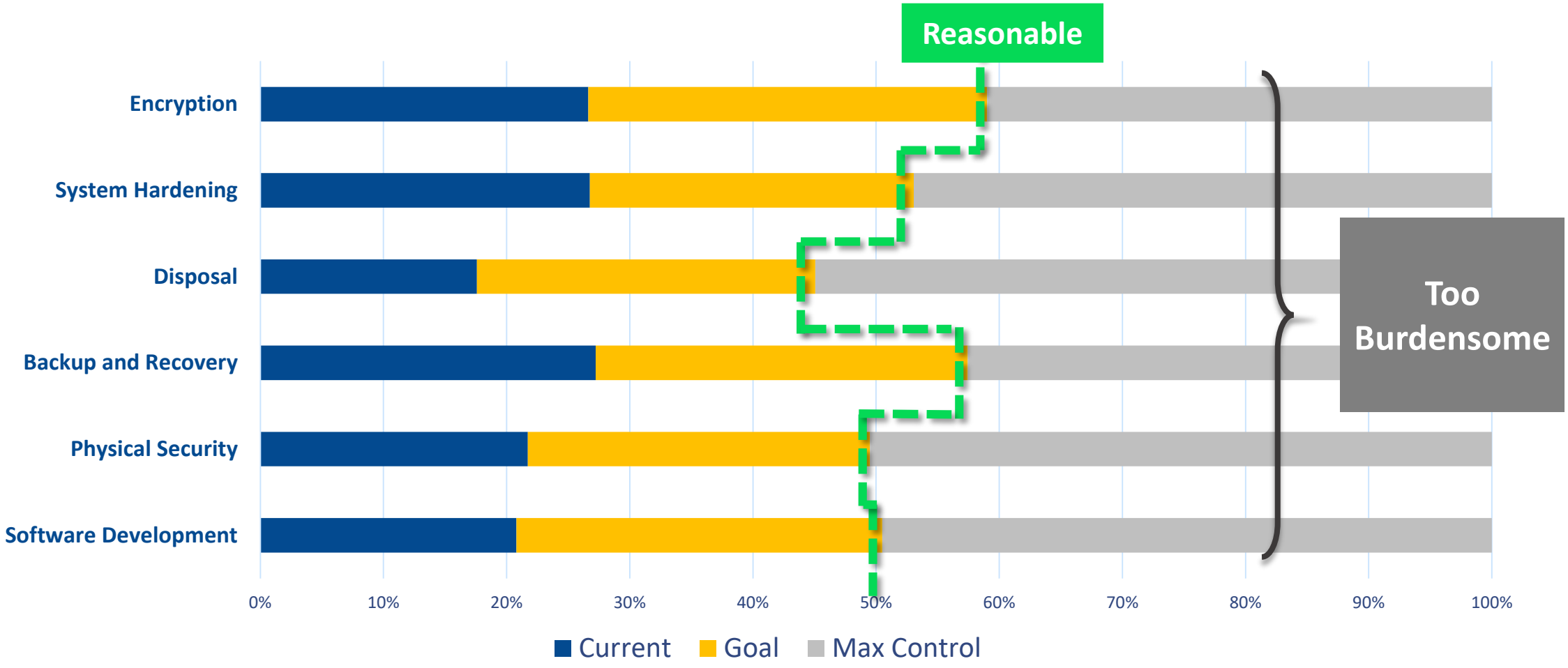
Safeguard	Create a VLAN limited to the application server, database server, IPS sensor.
Safeguard Risk	Promiscuous sniffer would be detected by IPS if on those servers.

Mission Impact	Objectives Impact	Obligations Impact
(1) Customer returns above market	(2) RoA within planned variance	(1) Customer finances not harmed

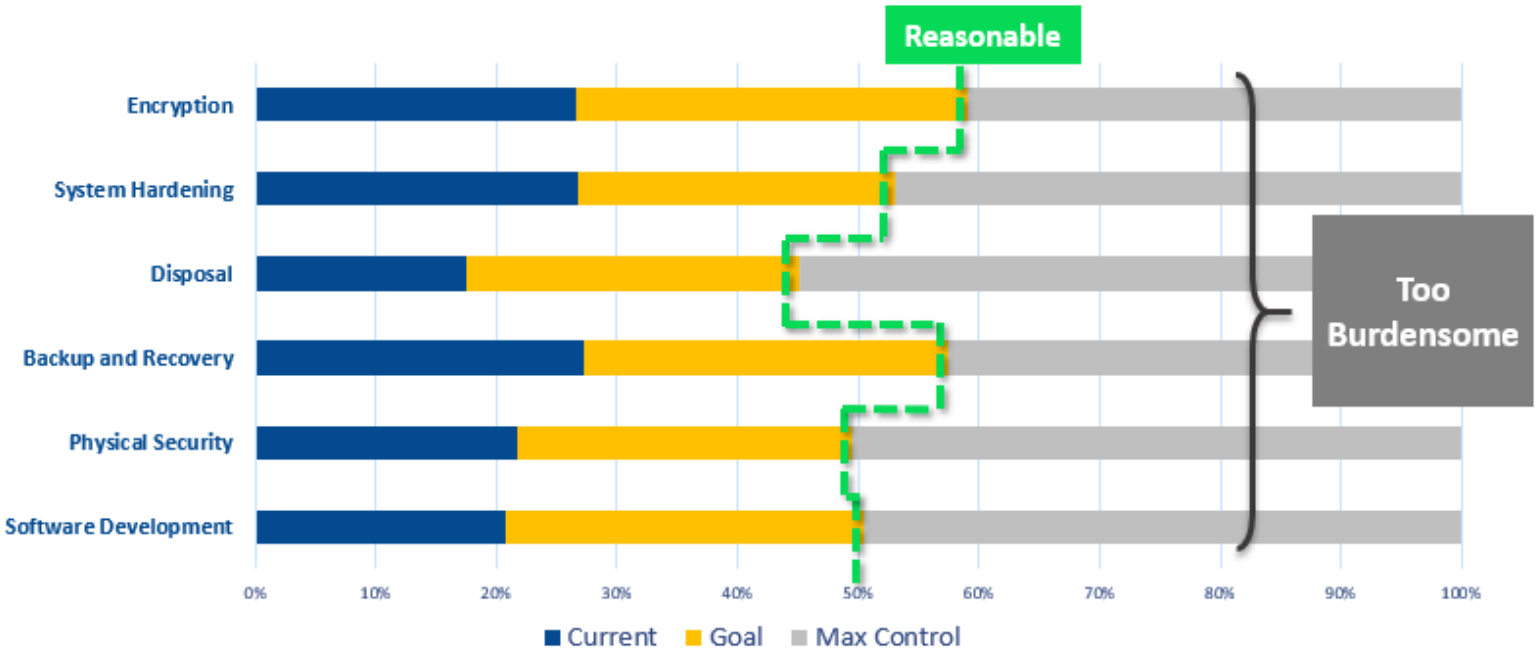
Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
(4) Expected	8

Reasonable Controls
From the Board Room to the Court Room

In the Risk Age We Do Enough to Protect Others, But Not So Much That We Hurt Ourselves



The Value of Risk Management



Our auditors noticed no MFA on our application.

Yep. Our patients are frustrated by it and they stopped using the app.

So … we just don't use MFA on the app?

Nope. Risk to patient health outweighed risk to privacy.

Oh, yeah. I see it on the risk register. I'll tell them now.

The Case of the Hacked, Risk Managed Healthcare Provider: The Lawsuit That Never Happened

- Healthcare provider breached PHI through hacked application accounts.
- State Attorney General reviewed the case to see if they should sue the healthcare provider on behalf of state residents.
- AG did not pursue the case when they saw that additional controls increased risks to patients who would have stopped using the application if it had complicated controls.
- Provider had conducted a Duty of Care Risk Assessment prior to the breach, evaluating risks to themselves and others, and establishing their reasonable plan for resolving the risks.

Lesson of the Case of the Hacked, Risk Managing Healthcare Provider

When your security needs address your business ***and*** risk to others,

they make sense to **judges** and **regulators**.

The Age of Risk: Surviving and Thriving

- Wherever you look, regulations and security frameworks demand risk instead of compliance.
- This is a big favor to you and the public.
- Use **DoCRA** or **CIS RAM** to evaluate risk to others and risk to you.

  You can get this for free at cisecurity.org

- Only use controls that provide balance between you and others.

Problems Solved

- Cyber Security Investments prioritized based on business impact.
- Executive Leadership is easier to obtain as security projects have clear benefits to the business and without…clear impacts to the business.
- Cyber security was now focused on critical business risks, not maturity of controls for maturity sake.
- Cyber security developed Risk Management Program included NIST 171 and NIST 53 controls which nicely integrated with Internal Audit ITG.
- Internal Audit findings could **NOW be verified and prioritized** using Cyber Security's DoCRA-based Risk Management.

Additional Benefits

- **Business Insurance** – since moving to a risk-based model, our business insurance dropped more than 5%.
- **Cyber Insurance** – risk assessments highlighted the need for cyber insurance. Project spearheaded by CIO to investigate and acquire cyber insurance.

Thank You

Terry Kurzynski

TerryK@halock.com

Aaron DeMaster

Aaron.DeMaster@Rexnord.com