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

Surviving and Thriving in the Age of Risk

HALOCK®

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 Certification

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

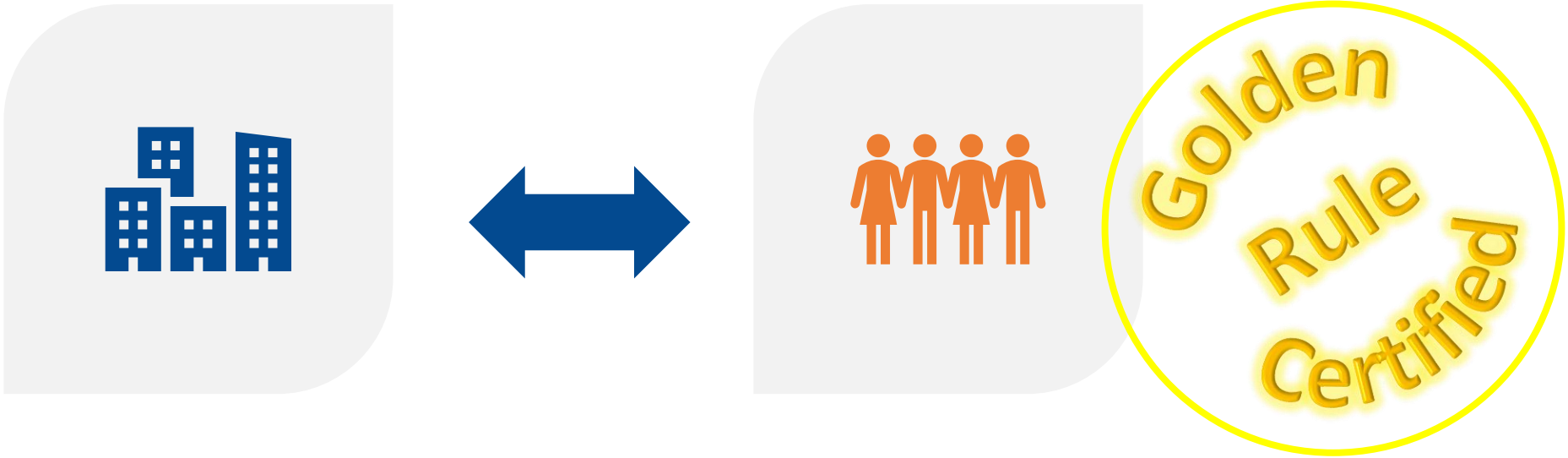
The Age of Compliance

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

Audit!

Anti-malware

Pen Testing!

Hardening

Hardening

Anti-malware

Vulnerability scans

BYOD

VPN!

Anti-malware

Anti-malware

Whitelisting

Secure development

Vulnerability scans

Whitelisting

IoT!

Audit!

IDS / IPS

Secure DNS

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

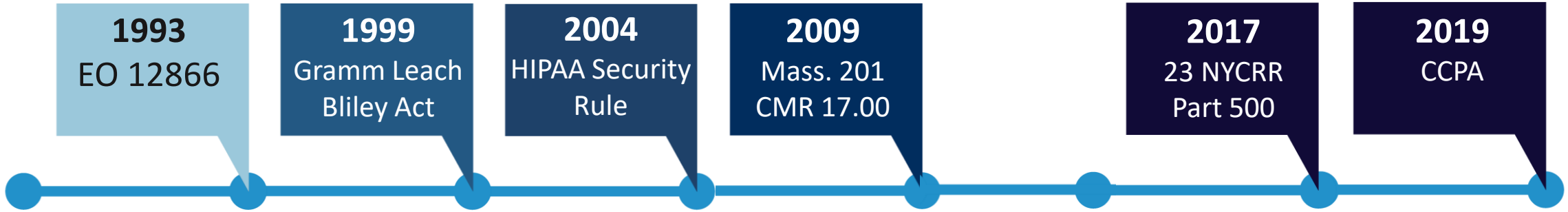
- “These security requisitions don’t make sense to me.”
- “Why are we spending this money?”
- “How do we compare to our peers. Shouldn’t we just do what they do?”
- “Information security is an insurance policy I don’t want to pay for.”
- “I just read an article about breaches on copy machines. Stop everything 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:

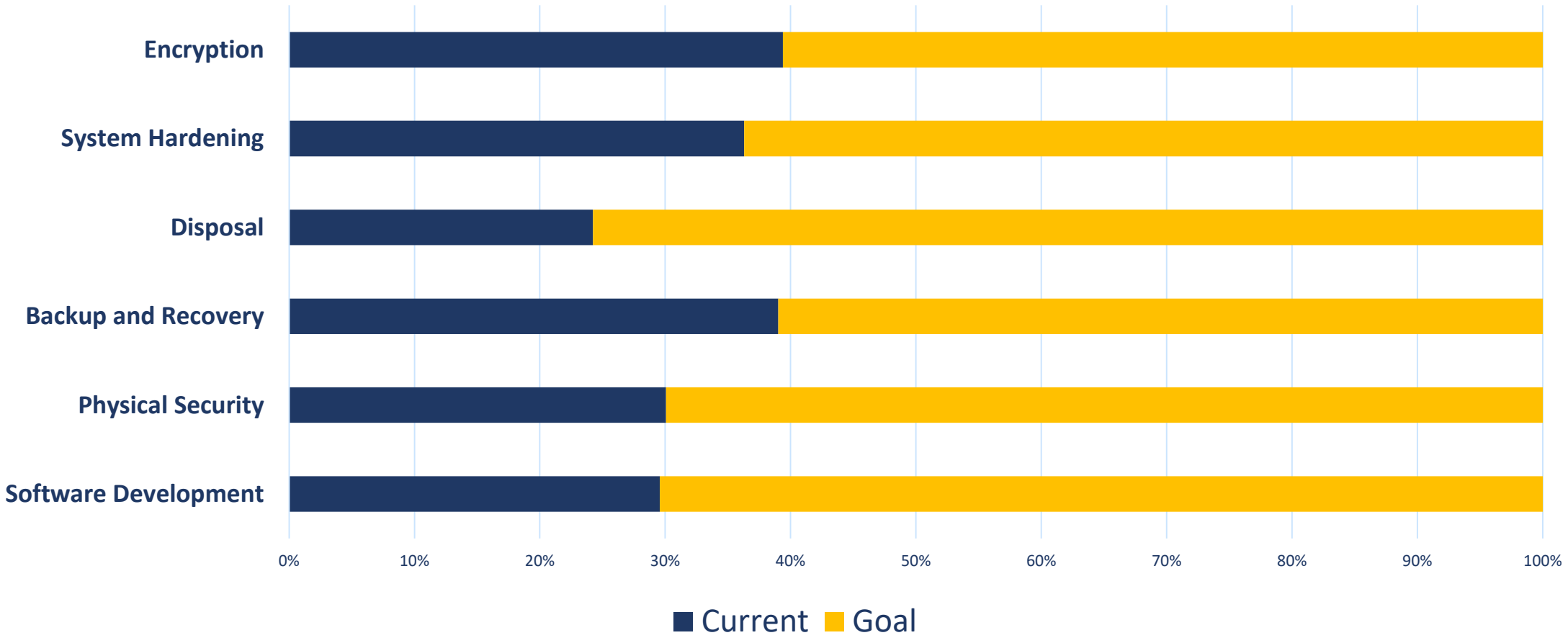
Changed "Compliant" to "Risk" so it became a risk assessment.

Maturity Assessments

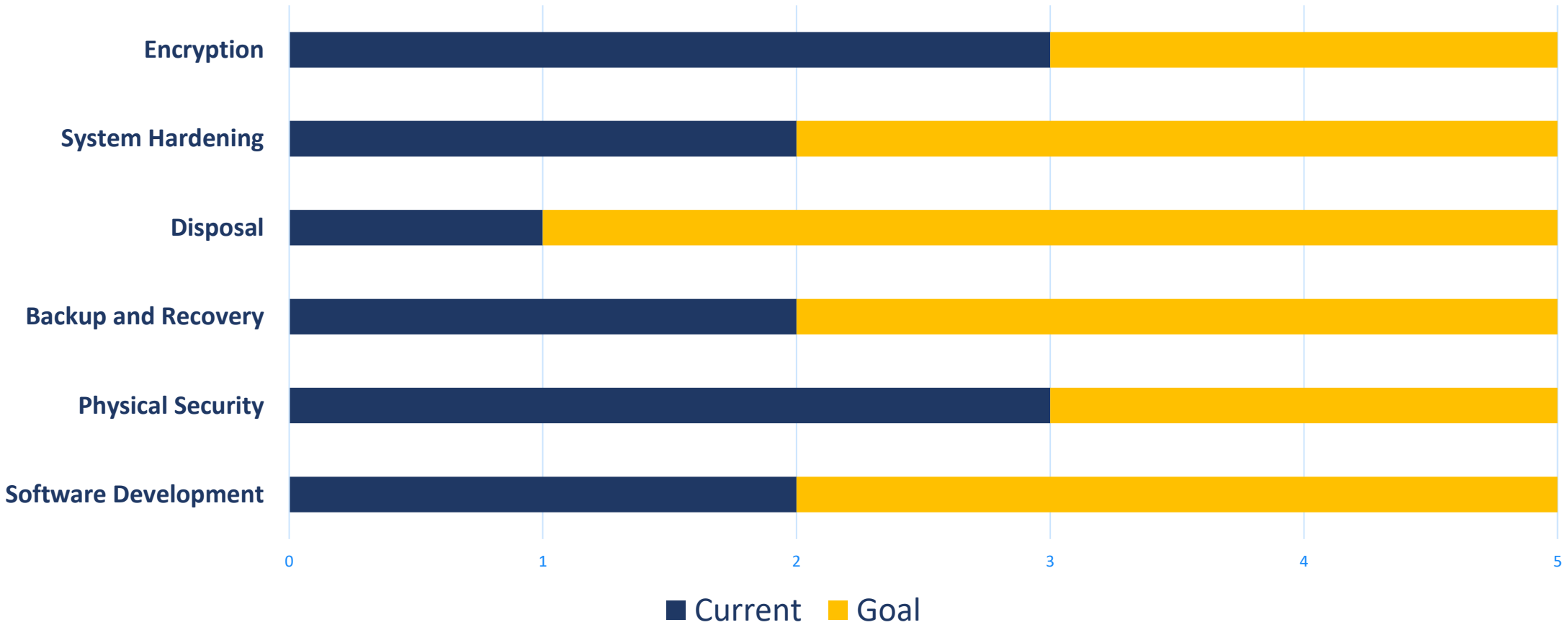
NIST 800-53	Control Title	NIST CSF	Maturity
AC-1	ACCESS CONTROL POLICY AND PROCEDURES		5
AC-2	ACCOUNT MANAGEMENT	PR.AC-4, DE.CM-1	1
AC-3	ACCESS ENFORCEMENT	PR.PT-3	2
AC-4	INFORMATION FLOW ENFORCEMENT	PR.AC-5, PR.DS-5, PR.PT-4	1
AC-5	SEPARATION OF DUTIES	PR.AC-4, PR.DS-5	2
AC-6	LEAST PRIVILEGE	PR.AC-4, 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

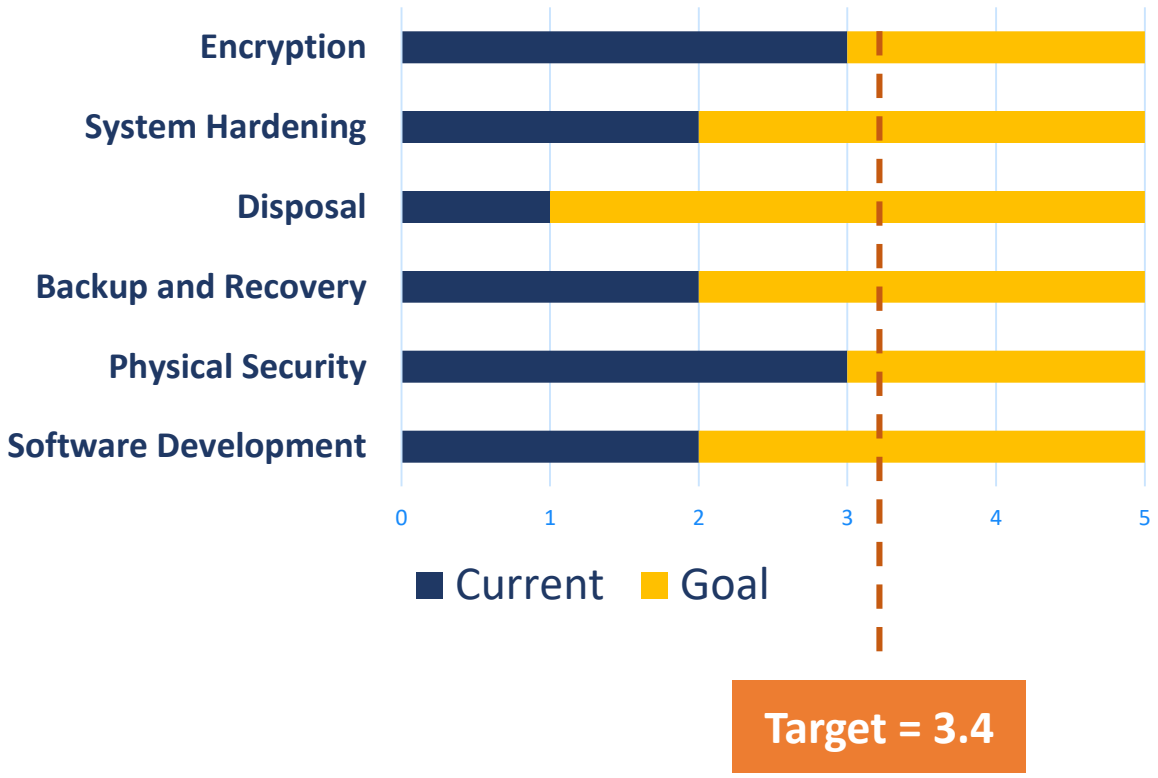
Common recommended target

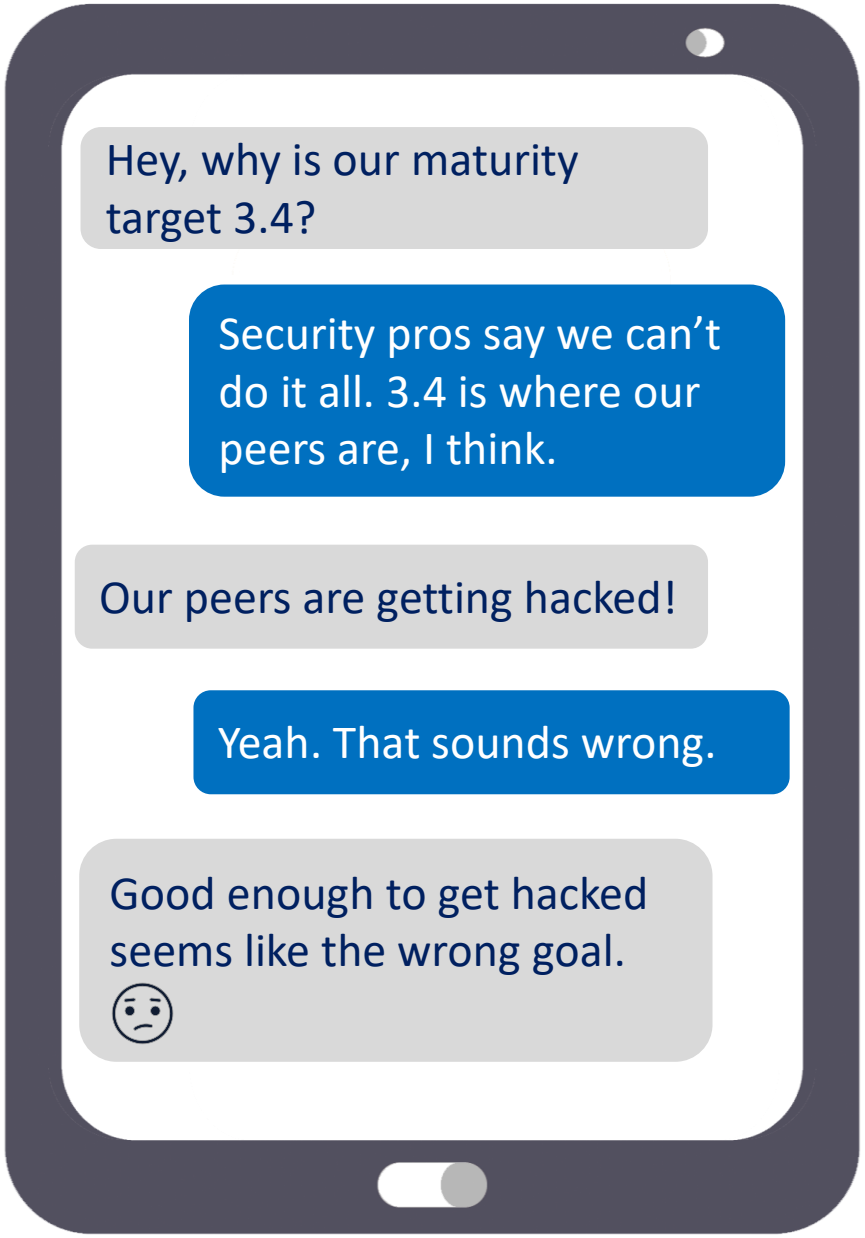
But why not here?

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, Compliant Hospital

- Patient records were everywhere. (Of course! It's a hospital!)
- A hacked server breached thousands of personal records.
- **Regulator:** "How secure was your system?"
- **Hospital:** "We were a 3.1 out of 5."
- **Regulator :** "Come again?"
- **Hospital:** "Three-point-one mature. Out of five."
- **Regulator :** "This makes no sense to me. Would additional controls have been more burdensome than the risk to the plaintiff?"
- **Hospital:** "Ummmm."

The Case of the Hacked, Compliant Hospital

- Finding … **Negligent**, with seven figures in total damages.
- What the regulator would have considered from the hospital.
  - *"The application server was partially hardened, but securing it completely would have prevented people from using it for its purpose."*

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 Hacked, Compliant Hospital

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 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 safeguards that could reduce the likelihood and impact.

Just Add Two More Steps and You Have **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 safeguards 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.***

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	**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	●	○	○	○	○	○	○	○	○

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

A freely available standard for conducting risk assessments.

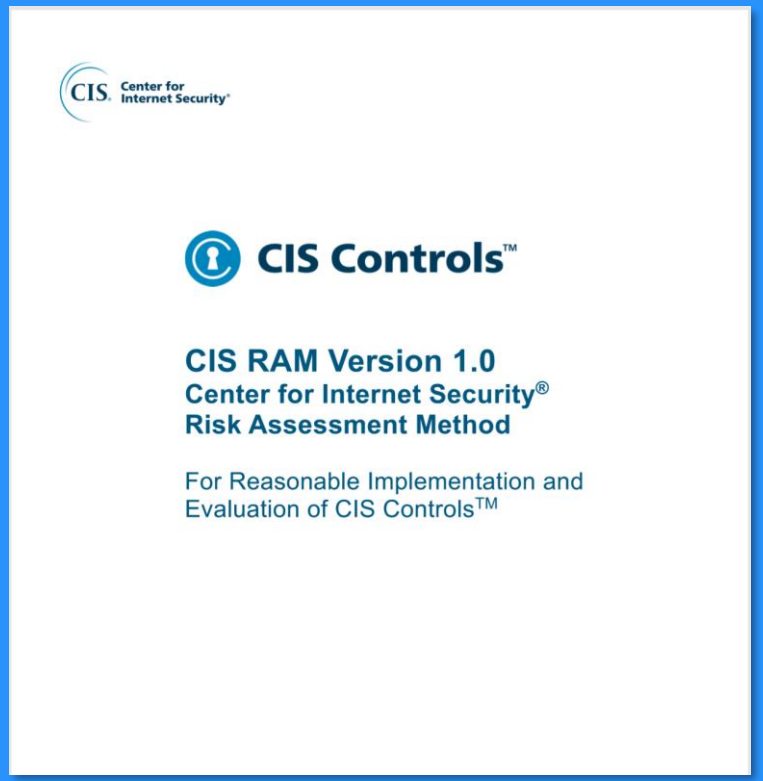
A method for demonstrating reasonableness.

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.

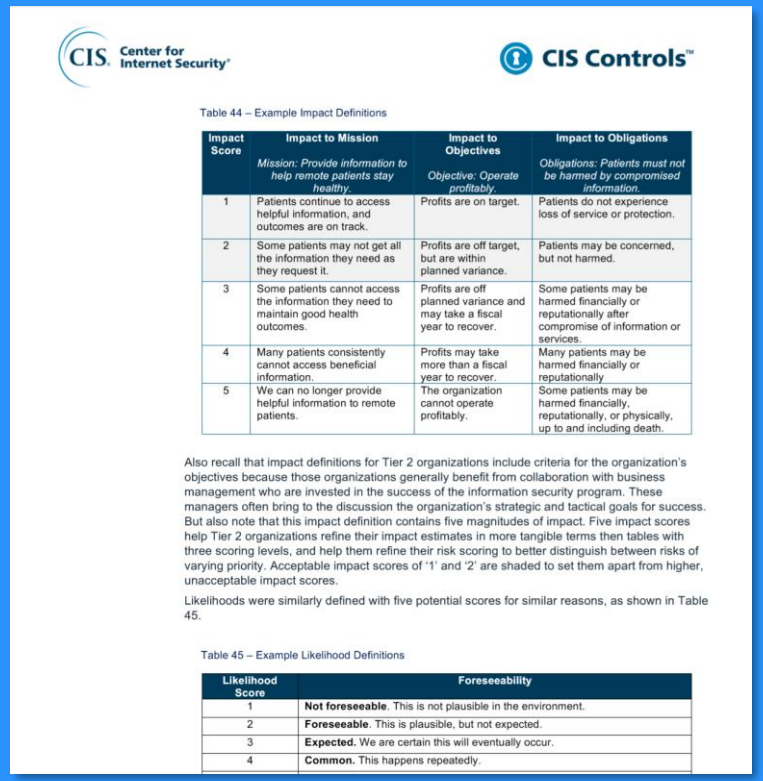


CIS Center for Internet Security

CIS Controls™

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

For Reasonable Implementation and Evaluation of CIS Controls™



CIS Center for Internet Security

CIS Controls™

Table 44 – Example Impact Definitions

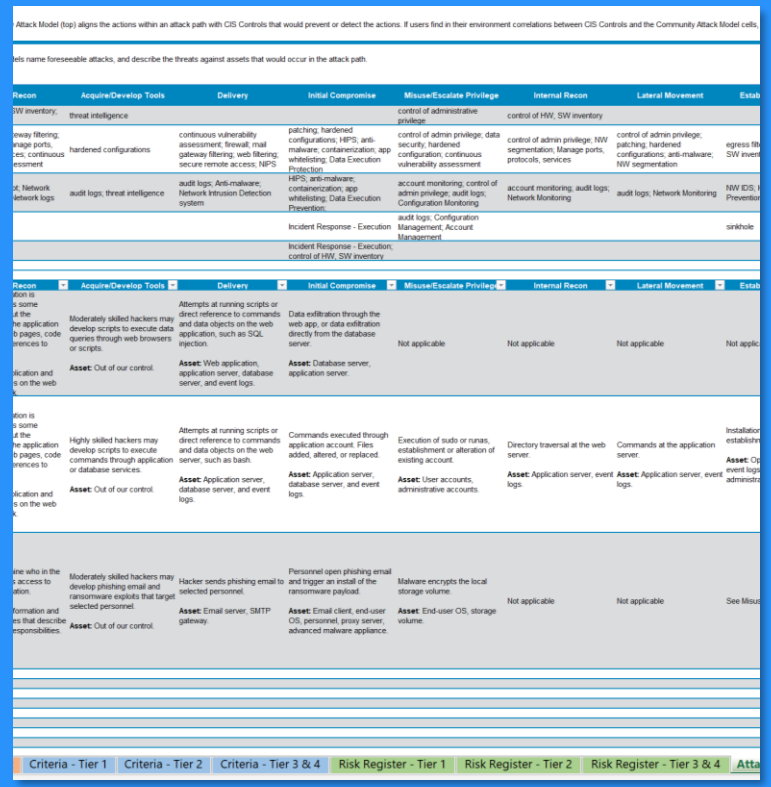
Impact Score	Impact to Mission *Mission: Provide information to help remote patients stay healthy.*	Impact to Objectives *Objective: Operate profitably.*	Impact to Obligations *Obligations: Patients must not be harmed by compromised information.*
1	Patients continue to access helpful information, and 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 then 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	**Not foreseeable**. This is not plausible in the environment.
2	**Foreseeable**. This is plausible, but not expected.
3	**Expected.** We are certain this will eventually occur.
4	**Common.** This happens repeatedly.



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,

dels name foreseeable attacks, and describe the threats against assets that would occur in the attack path.

Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Estab
SW inventory;	threat intelligence			control of administrative privilege	control of HW, SW inventory		
eway filtering; nage ports, es; continuous essment	hardened configurations	continuous vulnerability assessment; firewall; mail gateway filtering; web filtering; secure remote access; NIPS	patching; hardened configurations; HIPS; 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 filt SW invent
k; Network etwork logs	audit logs; threat intelligence	audit logs; Anti-malware; Network Intrusion Detection system	HIPS; 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; I Preventior
			Incident Response - Execution	audit logs; Configuration Management; Account Management			sinkhole
			Incident Response - Execution; control of HW, SW inventory				

Recon	Acquire/Develop Tools	Delivery	Initial Compromise	Misuse/Escalate Privilege	Internal Recon	Lateral Movement	Estab
tion is s some t the he application b pages, code erences to lication and s on the web	Moderately skilled hackers may develop scripts to execute data queries through web browsers or scripts. **Asset:** Out of our control.	Attempts at running scripts or direct reference to commands and data objects on the web application, such as SQL injection. **Asset:** Web application, application server, database server, and event logs.	Data exfiltration through the web app, or data exfiltration directly from the database server. **Asset:** Database server, application server.	Not applicable	Not applicable	Not applicable	Not applic
tion is s some t the he application b pages, code erences to lication and s on the web	Highly skilled hackers may develop scripts to execute commands through application or database services. **Asset:** Out of our control.	Attempts at running scripts or direct reference to commands and data objects on the web server, such as bash. **Asset:** Application server, database server, and event logs.	Commands executed through application account. Files added, altered, or replaced. **Asset:** Application server, database server, and event logs.	Execution of sudo or runas, establishment or alteration of existing account. **Asset:** User accounts, administrative accounts.	Directory traversal at the web server. **Asset:** Application server, event logs.	Commands at the application server. **Asset:** Application server, event logs.	Installation establishe **Asset:** Op event logs administra
ne who in the s access to ation. formation and es that describe esponsibilities.	Moderately skilled hackers may develop phishing email and ransomware exploits that target selected personnel. **Asset:** Out of our control.	Hacker sends phishing email to selected personnel. **Asset:** Email server, SMTP gateway.	Personnel open phishing email and trigger an install of the ransomware payload. **Asset:** Email client, end-user OS, personnel, proxy server, advanced malware appliance.	Malware encrypts the local storage volume. **Asset**: End-user OS, storage volume.	Not applicable	Not applicable	See Misus

Criteria - Tier 1 | Criteria - Tier 2 | Criteria - Tier 3 & 4 | Risk Register - Tier 1 | Risk Register - Tier 2 | Risk Register - Tier 3 & 4 | Atta

DoCRA Practically Applied: CIS RAM

Basic Form

	Our Profit	Patient Privacy
Acceptable	*Profit plan is on track*	*No reputational harm*
Unacceptable	*Not profitable*	*Reputational or financial harm*

Harm to us

Harm to others

More Practical Form

	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.*

Let’s Get Real

To evaluate balance well, define **Your**:

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

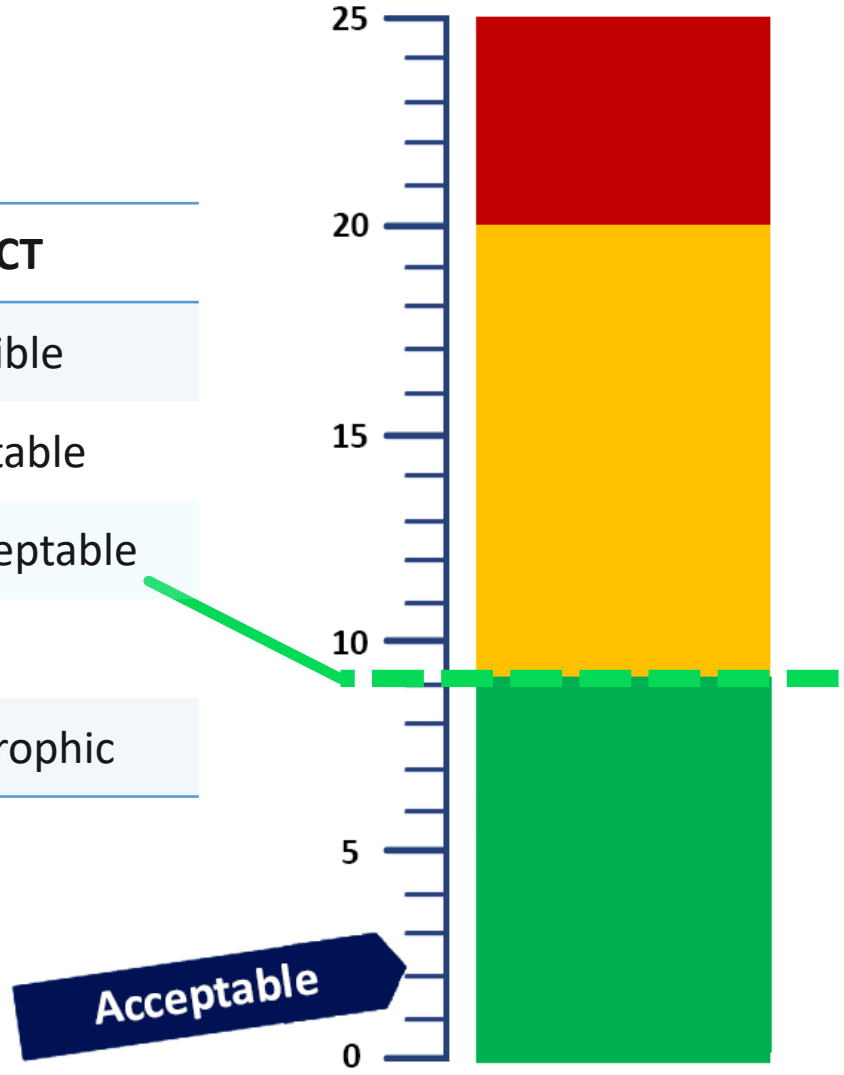
Some Common Impact Criteria

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

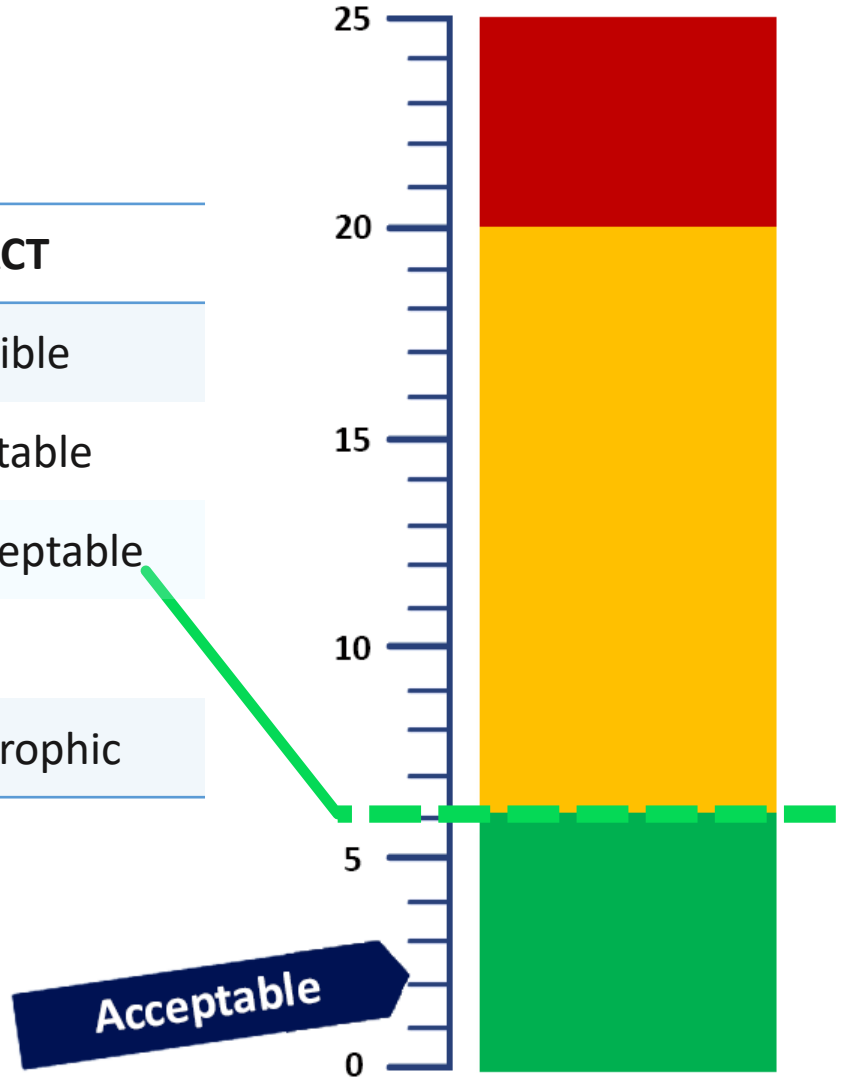
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



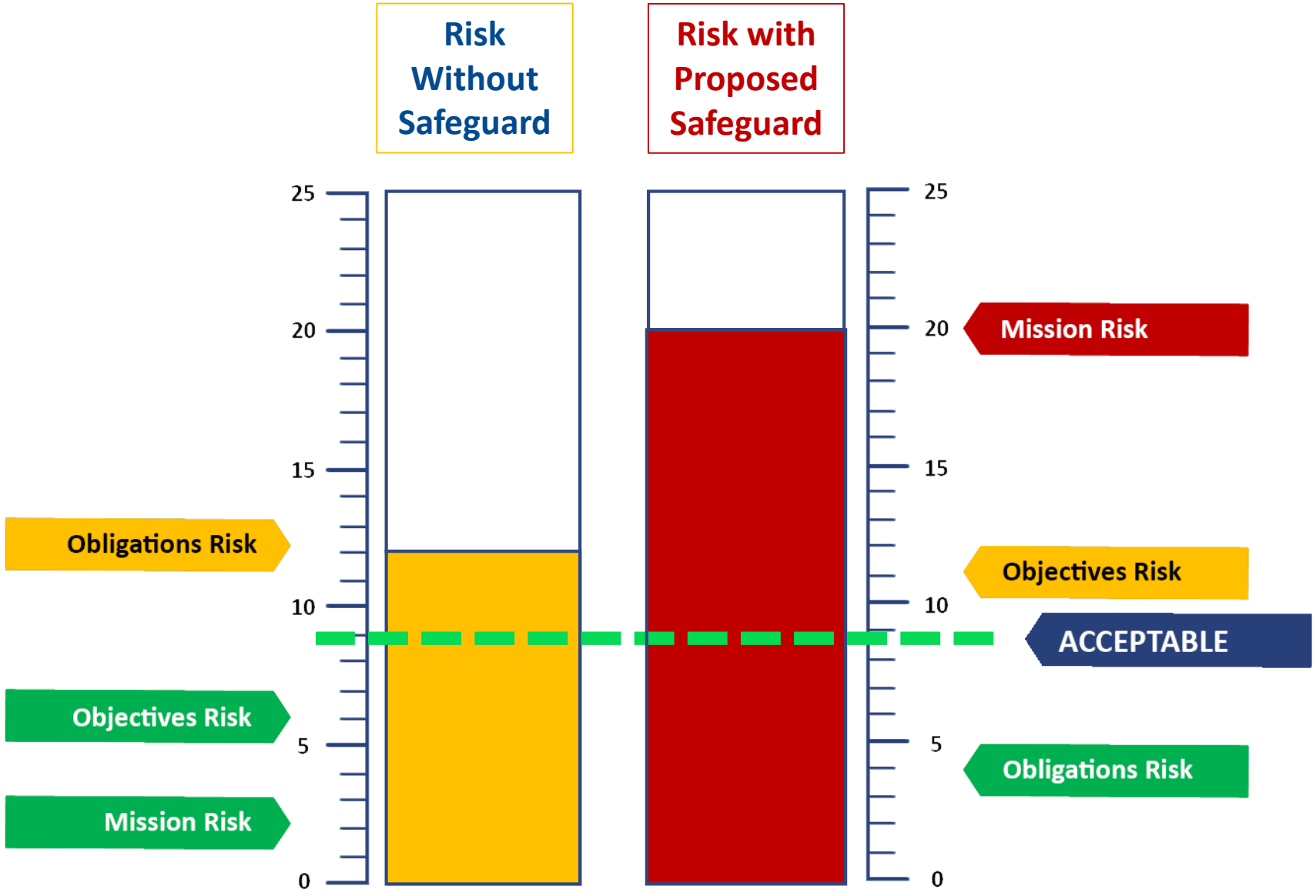
Defining Acceptable Risk

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

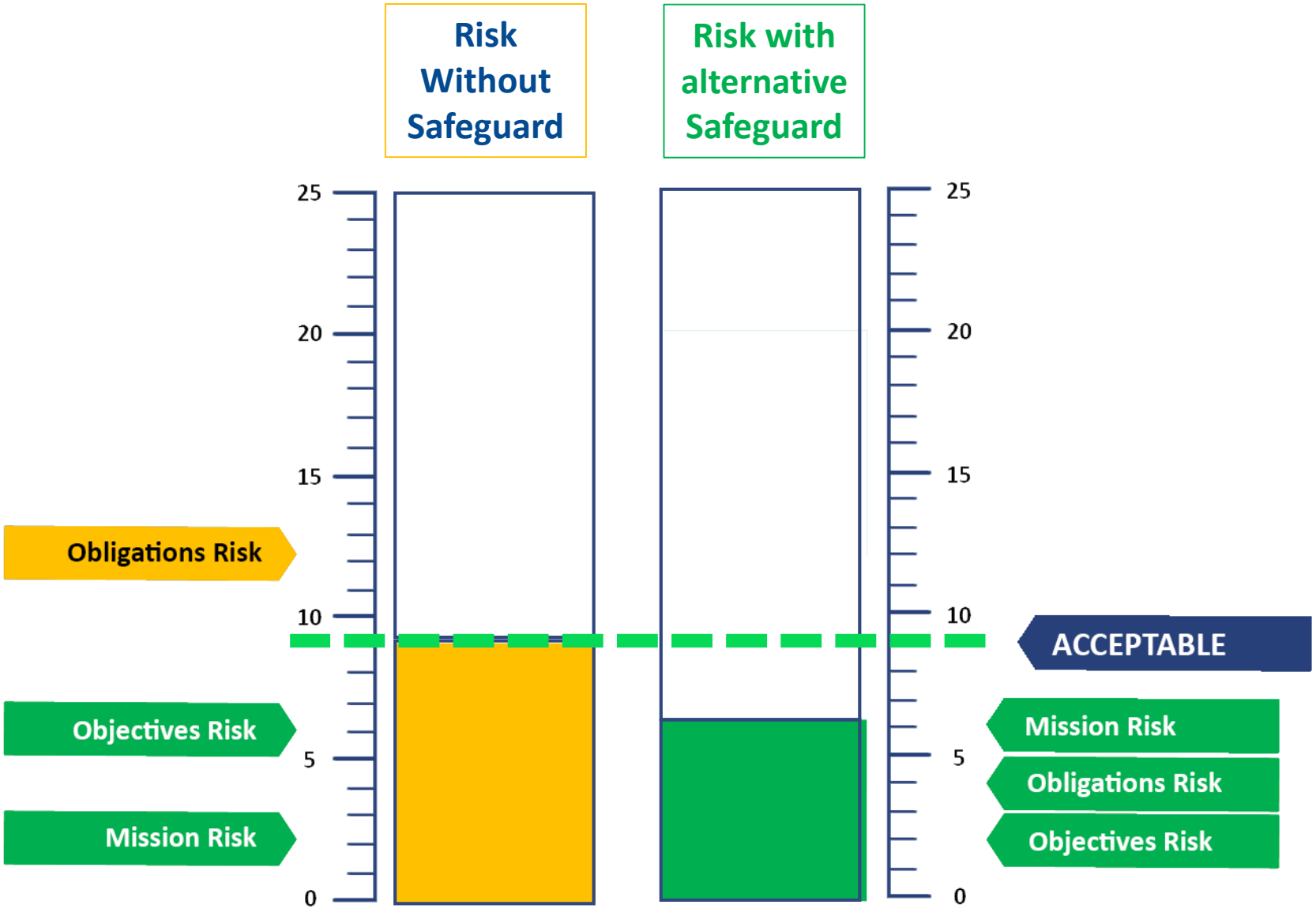
	IMPACT
1	Negligible
2	Acceptable
3	Unacceptable
4	High
5	Catastrophic



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**

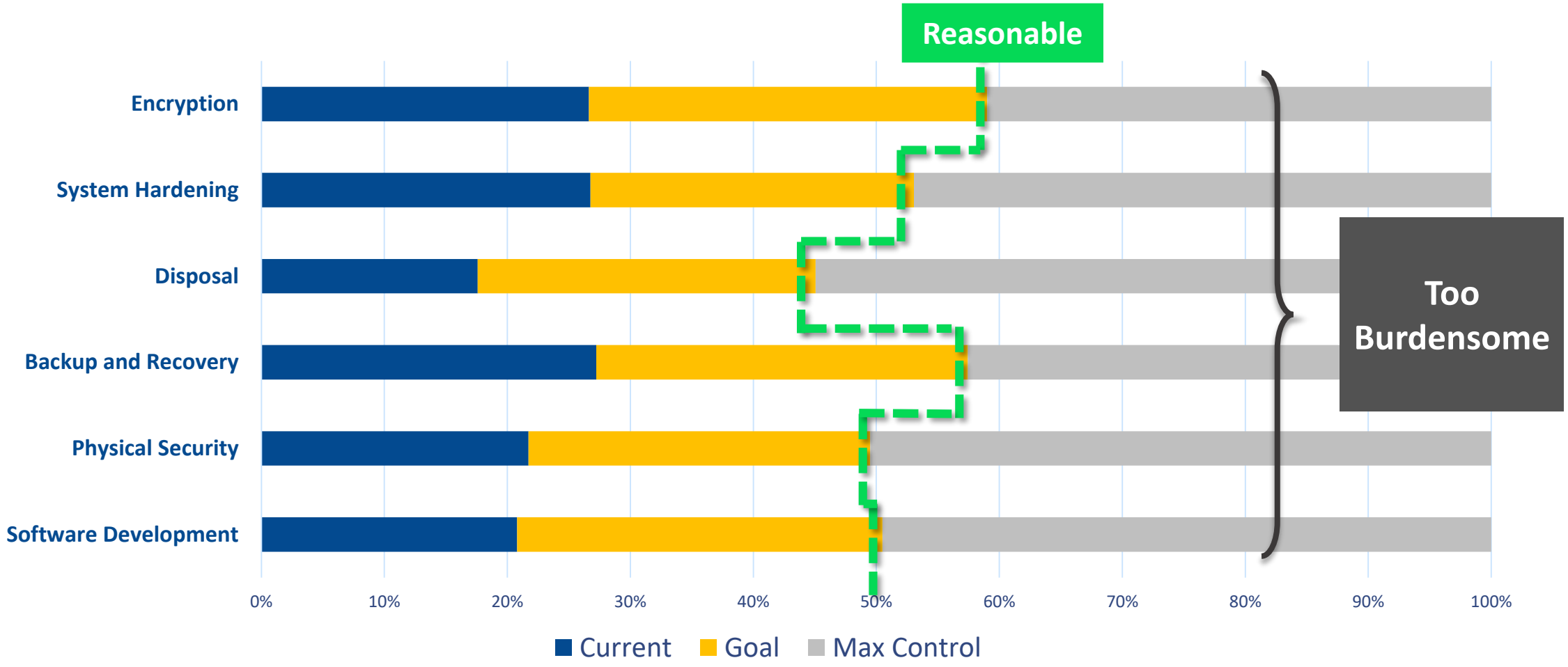
Safeguard	Create a VLAN limited to the application server, database server, IPS sensor.
Safeguard Risk	Promiscuous sniffer would be detected by IPS if on those servers.

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

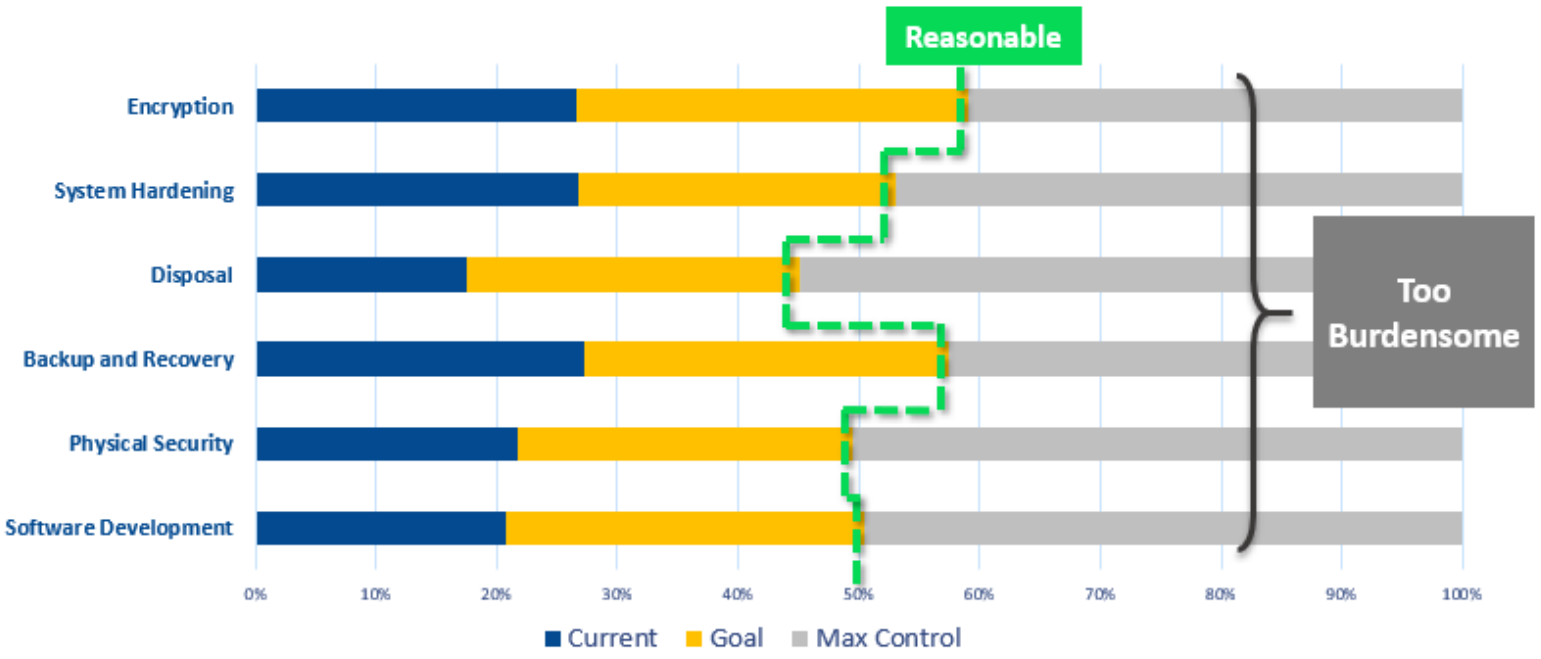
Likelihood	Safeguard Risk Score: Max(Impact) x Likelihood
(4) Expected	**8**

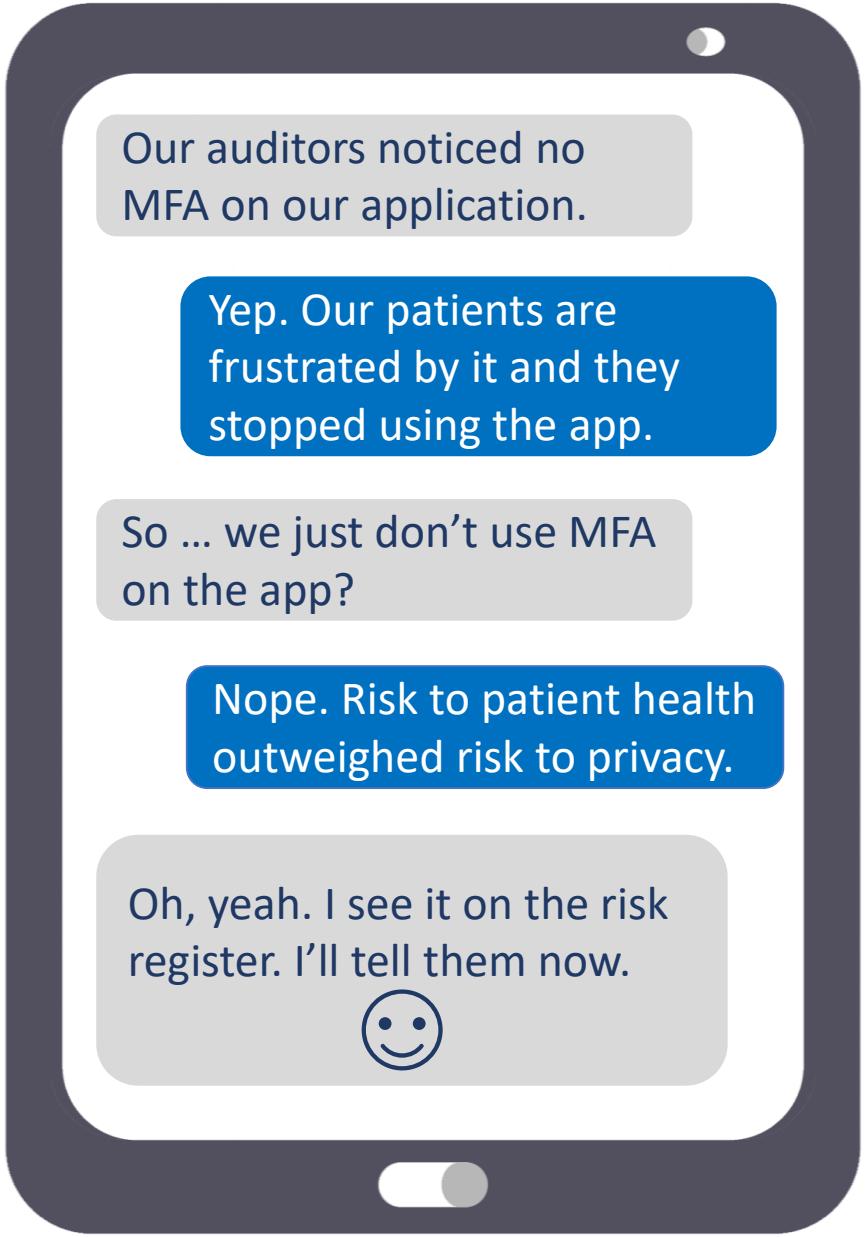
Reasonable Controls
From the Board Room to the Court Room

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



The Value of Risk Management





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.

Thank You

Chris Cronin

HALOCK Security Labs

ccronin@halock.com