HALOCK®

Five Deliverables Every Cybersecurity Team Needs to Survive, Thrive and comply with the new SEC Cybersecurity Rule

Terry Kurzynski
Founder, Senior Partner
HALOCK Security Labs
www.halock.com

About the Presenter

- Founding Partner of **HALOCK Security Labs** (1996)
- CISSP since 2002
- ISO 27001 Auditor, CISA, PCI QSA
- *Board Member of the **DoCRA Council***

  ("Duty of Care Risk Analysis")
- Contributing author of the CIS RAM

  Center for Internet Security Risk Assessment Method
- Litigation support for large cyber breaches
- Over 30 years of experience in IT and Security
- University of Wisconsin with a B.S. in Computer Science ('92)

Terry Kurzynski,

Board Member, The DoCRA Council

Senior Partner, HALOCK Security Labs

© 2023 HALOCK Security Labs. All rights reserved.

SEC Ruling on Cybersecurity – July 26, 2023

U.S. SECURITIES AND
EXCHANGE COMMISSION

- This rule is intended to provide investors more consistent information to make decisions
- It applies to public companies registered with the SEC.
- If any of your customers or vendors are publicly traded companies, it’s just a matter of time before they expect some form of this from your company as their 3rd party business partner.
- **We may all need to comply with the new SEC Cybersecurity Rule in some shape or form.**

© 2023 HALOCK Security Labs. All rights reserved.

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies – July 26, 2023

- Think of this as Sarbanes Oxley (SOX) for Cybersecurity.
- The intent is to provide investors transparent information about cyber risk management.
- They apply to public companies registered with the SEC.
- If any of your customers are **publicly traded companies**, expect them to include you in their third-party risk management (TPRM) program.
- This will set expectations for open communication about cyber risk for all businesses.

© 2023 HALOCK Security Labs. All rights reserved.

New SEC Cybersecurity Rules: Think Sarbanes Oxley for Cybersecurity

- Official Version (186 pages)
  - https://www.sec.gov/files/rules/final/2023/33-11216.pdf
- Date Published
  - July 26, 2023
- Official Name
  - "Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure"
  - Filed as 17 CFR Parts 229, 232, 239, 240, and 249
- Applies to SEC Disclosure Reports for Investors
  - 8-K, 10-K, S-K, 20-F forms
- It requires accountability, transparency and communication to Management Team and the Board of Directors for public companies regarding their cybersecurity risks and incidents.

HALOCK®

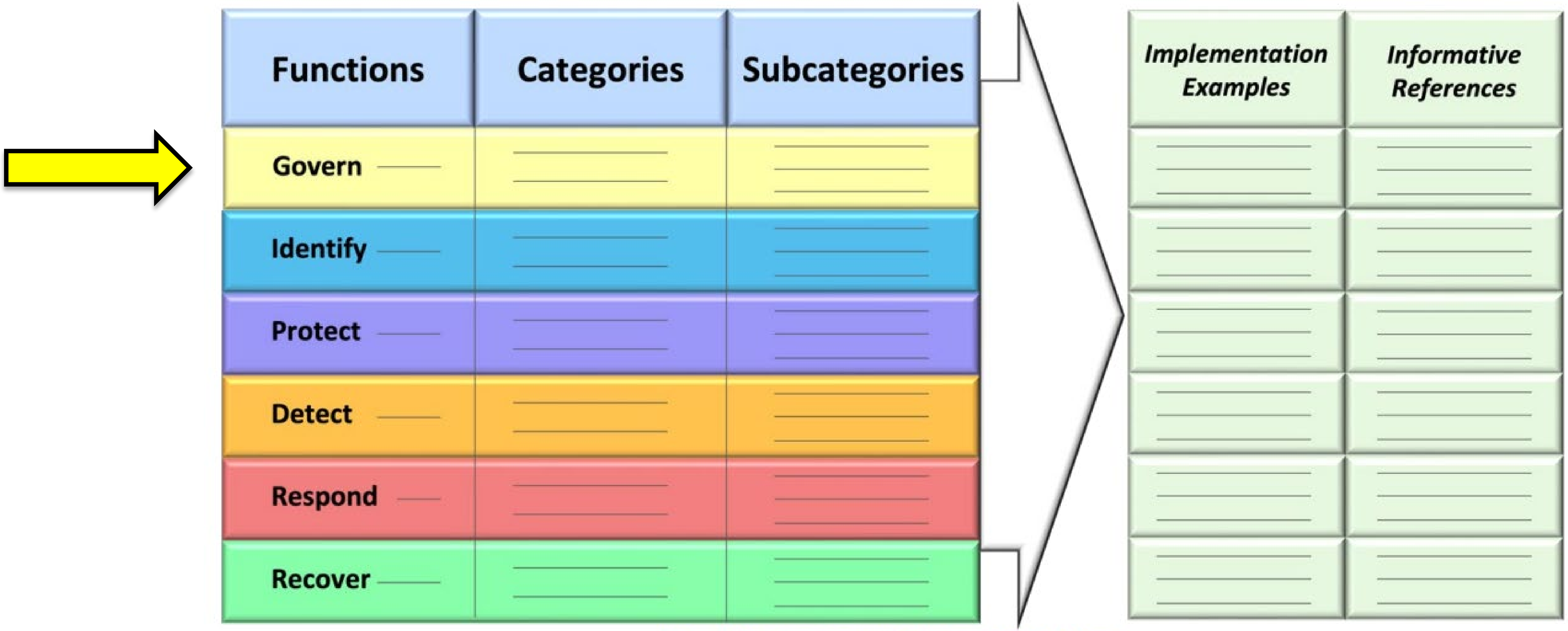
© 2023 HALOCK Security Labs. All rights reserved.

NIST Cybersecurity Framework 2.0 (Governance Function added)

- GOVERN (GV) – Establish and monitor the organization’s cybersecurity risk management strategy, expectations, and policy.
- The GOVERN Function is cross-cutting and provides outcomes to inform how an organization will achieve and prioritize the outcomes of the other five Functions in the context of its mission and stakeholder expectations.

© 2023 HALOCK Security Labs. All rights reserved.

NIST Cybersecurity Framework 2.0 (Governance Function added)



Functions

Categories

Subcategories

Govern

Identify

Protect

Detect

Respond

Recover

Implementation Examples

Informative References

Fig. 1. Cybersecurity Framework Core

© 2023 HALOCK Security Labs. All rights reserved.

PCI DSS v4.0 NEW Targeted Risk Analyses

Enterprise Risk Assessment Replaced with 2 Targeted Risk Analysis (TRA)s

- Periodic Cadence requirements
  - Requirements where you can set your cadence (with justification)
  - Must risk analyze how that cadence reduces the risk reasonably
  - Bullet list of what needs to be included in the requirement (worksheet from SSC being developed)
- Customized Approach
  - PCI DSS Controls that can be validated with this approach include a Control Objective
  - Document how your control meets the objective and reasonably reduces risk
  - Full independent Appendix with templates

© 2023 HALOCK Security Labs. All rights reserved.

PCI DSS v4.0 Targeted Risk Analyses Impact

- Periodic Cadence requirements
  - 9 PCI DSS requirements allow an organization to use a periodic cadence
  - If a cadence requirement is applicable, a TRA to justify the cadence is required by March of 2025
- Customized Approach
  - New option for validating PCI DSS 4.0 requirements
  - Intended for Risk Mature organizations to allow flexibility in meeting the Customized Control Objective
  - Can ONLY be used when validating compliance with an Onsite Assessment and Report on Compliance (no SAQs)

© 2023 HALOCK Security Labs. All rights reserved.

SOC 2 Framework Risk Assessment Criteria

CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

- A formal risk management process must be implemented.

CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

- At least annually, a full risk assessment must be performed, including potential technology/security risks, organizational risks, and other risks that may prevent the Company from meeting service commitments to clients and Company objectives.
- Risk assessment must include risk scoring and conclusion on risks identified (acceptable or action required. For actions required, action plans should be documented and aggregated into a risk register.
- At least quarterly (but recommend monthly), the risk register resulting from the risk assessment should be reviewed and updated.

CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

- As a part of the risk assessment, risks related to fraud/potential fraud need to be considered and documented.

CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

- As a part of the risk assessment, risks stemming from planned changes to the Company and service/IT environment should be considered and documented.

© 2023 HALOCK Security Labs. All rights reserved.

5 Distinct Capabilities to Survive and Thrive

1. Defining a **Clear Line of Acceptable Risk** below which you can accept risks and above which you must remediate (what the new SEC rules call “**materiality**”).
2. Ensuring your security program is **Legally Defensible** and complies with **the new SEC Cybersecurity Rule** (published July 26, 2023).
3. Understanding the **Known Risk** to your organization.
4. Providing the C-Suite with a **Roadmap** for your program that reduces risk to an acceptable level.
5. Communicating Risks and Justifying **Expenditure Requests** in business terms.

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Overview and Resources

Each Of These 5 Capabilities Features:

- A Summary of the Fundamentals
- Sample Templates
- Options to Get Started

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question #1

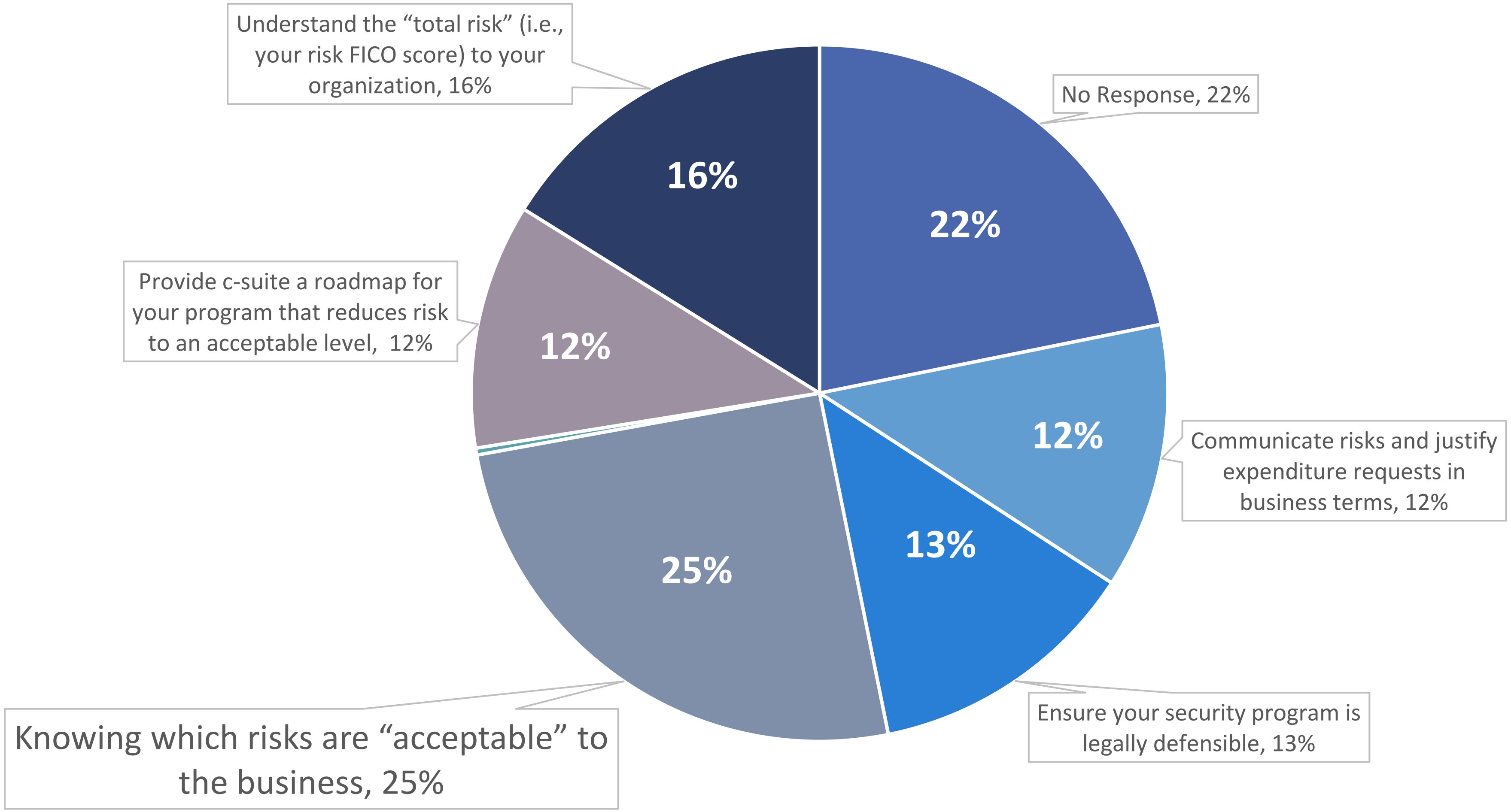
Which of the below 5 poses the biggest challenge for you?

a. Knowing which risks are “acceptable” to the business
b. Understand the “total risk” (i.e., your risk FICO score) to your organization.
c. Communicate risks and justify expenditure requests in business terms.
d. Provide c-suite a roadmap for your program that reduces risk to an acceptable level
a. Ensure your security program is legally defensible.
b. We have no challenges, I’m not even sure why I’m here

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question 1

Poll #1: Which of the below 5 capabilities poses the biggest challenge for you?



HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

1

Defining a **Clear Line of Acceptable Risk** above which you must remediate and below which you can accept

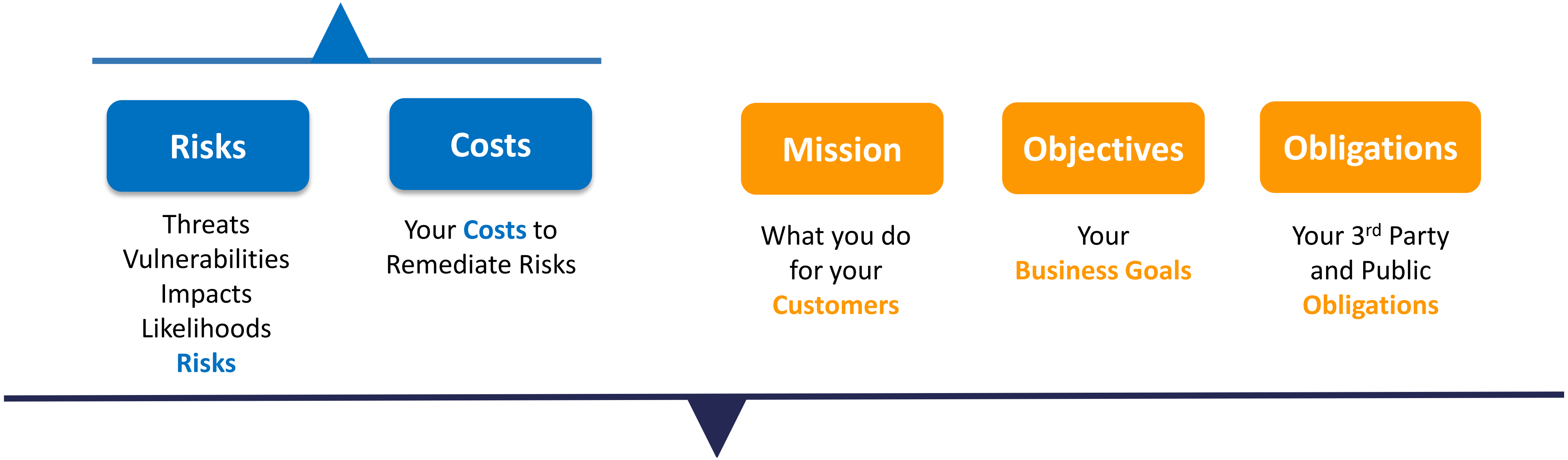
HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

PROBLEM: Cybersecurity & C-Suite Speak Different Languages

Cybersecurity Language

Speaks in Risks and Costs



Risks

Threats
Vulnerabilities
Impacts
Likelihoods
Risks

Costs

Your **Costs** to Remediate Risks

Mission

What you do for your **Customers**

Objectives

Your **Business Goals**

Obligations

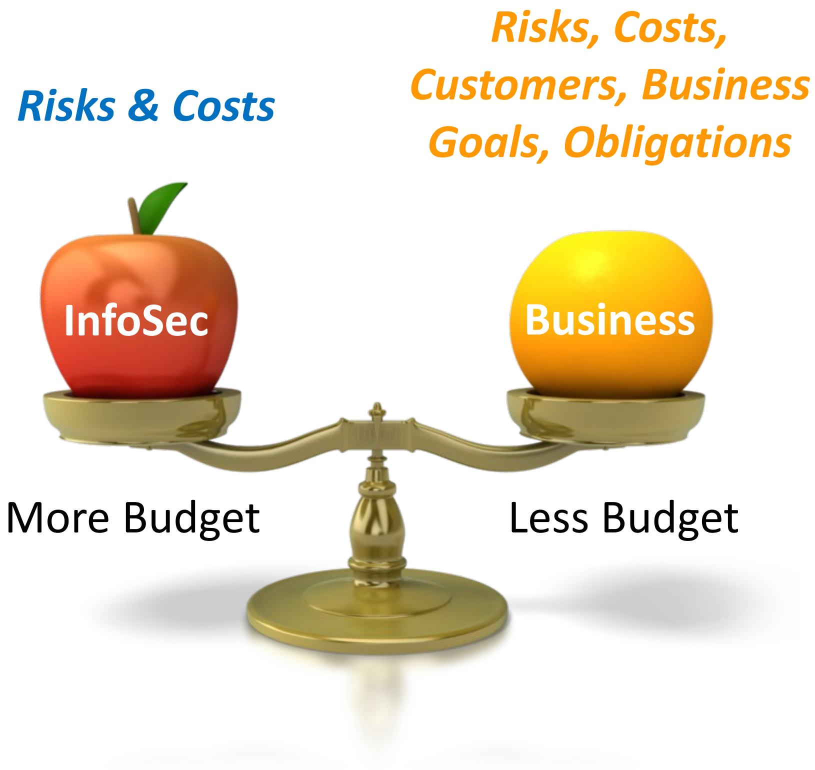
Your 3rd Party and Public **Obligations**

Business Language

Speaks in Terms ***Beyond*** Risks and Costs

© 2023 HALOCK Security Labs. All rights reserved.

When the C-Suite Doesn't Receive the Information They Need, **You Don't Receive the Budget You Need**!



Unless you recently experienced a breach or the project has political clout, the **Business wins the budget debate most of the time!**

© 2023 HALOCK Security Labs. All rights reserved.

SOLUTION: DoCRA

Duty of Care Risk Analysis (DoCRA) is the solution for creating a common language between Cybersecurity and Business!

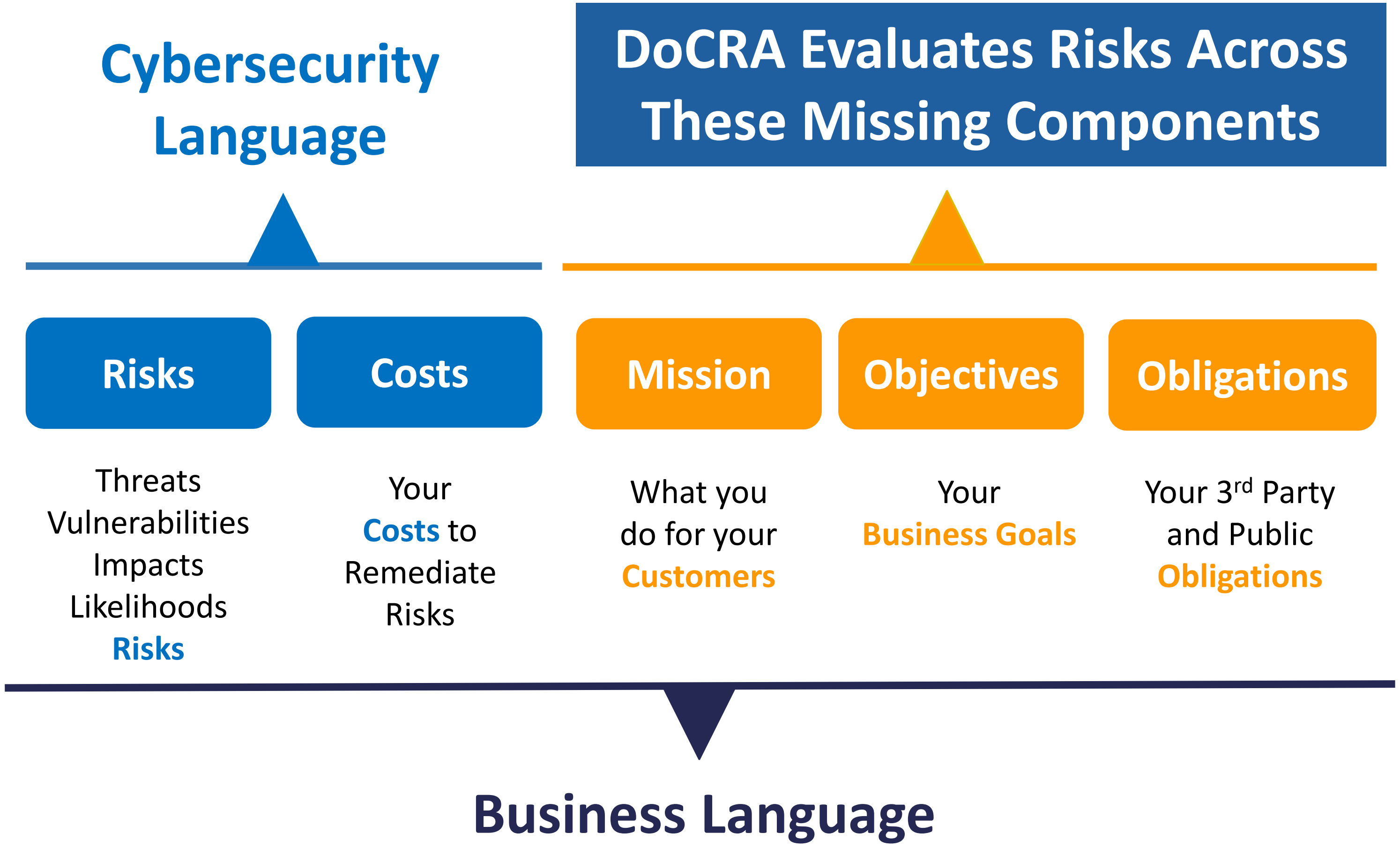
DoCRA is based on the legal concept of "**Due Care**." This means, we must reasonably protect others from the harm we may cause them.

Due Care is the level of care that the legal system expects an organization to perform.

© 2023 HALOCK Security Labs. All rights reserved.

How does DoCRA create a Common Language?

DoCRA fills in the missing components to create a common language as a universal translator.



Cybersecurity Language

DoCRA Evaluates Risks Across These Missing Components

Risks

Threats
Vulnerabilities
Impacts
Likelihoods
Risks

Costs

Your
Costs to
Remediate
Risks

Mission

What you
do for your
Customers

Objectives

Your
Business Goals

Obligations

Your 3rd Party
and Public
Obligations

Business Language

© 2023 HALOCK Security Labs. All rights reserved.

Defining the Line of Acceptable Risk Involves Evaluating Mission, Objectives and Obligations Impacts

Impact	Mission | What Do You Do For Your Customers	Objectives | Your Business Goals	Obligations | Your Public Duty
Definition	**1. 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.**	**1. 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.** **2. To support annual operational and fiscal goals.**	**1. Protect personnel information.** **2. Protect customer information.** **3. Protect investor interests.**
5. Catastrophic	**5.00** ACME would not be able to help customers safely, reliably, productively keep their goods and assets moving.	**5.10** ACME could not operate as a profitable organization.	**5.10** Multiple customers would experience significant harm (financial, safety including loss of life, etc.) as a result. **5.20** Personnel suffering irreparable harm including loss of life. **5.30** Company reputation or stock value would suffer permanent, terminal loss of value.
4. High	**4.00** Many customers would report that ACME could not help them safely, reliably, productively keep their goods and assets moving.	**4.10** Strategic plans or annual operational and fiscal goals would be severely off target and would require material investment or lost opportunity to recover. **4.20** Would result in Business Unit failure.	**4.10** Multiple customers would experience harm (financial, safety, etc.) as a result. **4.20** A material count of personnel suffer harm such as identity theft, reputational damage, or financial harm. **4.30** Company reputation or stock value would decrease long-term.
3. Unacceptable	**3.00** Some customers would report that ACME could not help them safely, reliably, productively keep their goods and assets moving.	**3.10** Strategic plans or annual operational and fiscal goals would be off target and outside of planned variance. **3.20** This would require countermeasures to recover.	**3.10** At least one customer would experience harm (financial, safety, etc.) as a result. **3.20** A small set of personnel suffer harm such as identity theft, reputational damage, or financial harm. **3.30** Company reputation or stock value would decrease short-term.
2. Acceptable	**2.00** We would not expect to see customer satisfaction surveys describe a negative perception.	**2.10** Strategic plans would be off target, but within planned variance. **2.20** Annual operational and fiscal goals would be off target, but within planned variance.	**2.10** Compromise of information assets may cause concern to customers but would not result in harm. **2.20** Compromise of information assets may cause concern to personnel but would not result in harm. **2.30** Compromise of information assets may cause concern to investors but would not result in harm.
1. Negligible	**1.00** No detected impact or impairment of mission.	**1.10** Targets set in strategic plans remain on target. **1.20** Annual operational and fiscal goals remain on target.	**1.10** CUI and customer information remains accessible only to approved parties. **1.20** Personnel information remains accessible only to approved parties. **1.30** Corporate value and stock prices are unaffected.

© 2023 HALOCK Security Labs. All rights reserved.

Above That Line are "Unacceptable" Impacts

Impact	Mission | What Do You Do For Your Customers	Objectives | Your Business Goals	Obligations | Your Public Duty
Definition	1. **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.**	1. **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.** 2. **To support annual operational and fiscal goals.**	1. **Protect personnel information.** 2. **Protect customer information.** 3. **Protect investor interests.**
5. Catastrophic	**5.00** ACME would not be able to help customers safely, reliably, productively keep their goods and assets moving.	**5.10** ACME could not operate as a profitable organization.	**5.10** Multiple customers would experience significant harm (financial, safety including loss of life, etc.) as a result. **5.20** Personnel suffering irreparable harm including loss of life. **5.30** Company reputation or stock value would suffer permanent, terminal loss of value.
4. High	**4.00** Many customers would report that ACME could not help them safely, reliably, productively keep their goods and assets moving.	**4.10** Strategic plans or annual operational and fiscal goals would be severely off target and would require material investment or lost opportunity to recover. **4.20** Would result in Business Unit failure.	**4.10** Multiple customers would experience harm (financial, safety, etc.) as a result. **4.20** A material count of personnel suffer harm such as identity theft, reputational damage, or financial harm. **4.30** Company reputation or stock value would decrease long-term.
3. Unacceptable	**3.00** Some customers would report that ACME could not help them safely, reliably, productively keep their goods and assets moving.	**3.10** Strategic plans or annual operational and fiscal goals would be off target and outside of planned variance. **3.20** This would require countermeasures to recover.	**3.10** At least one customer would experience harm (financial, safety, etc.) as a result. **3.20** A small set of personnel suffer harm such as identity theft, reputational damage, or financial harm. **3.30** Company reputation or stock value would decrease short-term.
2. Acceptable	**2.00** We would not expect to see customer satisfaction surveys describe a negative perception.	**2.10** Strategic plans would be off target, but within planned variance. **2.20** Annual operational and fiscal goals would be off target, but within planned variance.	**2.10** Compromise of information assets may cause concern to customers but would not result in harm. **2.20** Compromise of information assets may cause concern to personnel but would not result in harm. **2.30** Compromise of information assets may cause concern to investors but would not result in harm.
1. Negligible	**1.00** No detected impact or impairment of mission.	**1.10** Targets set in strategic plans remain on target. **1.20** Annual operational and fiscal goals remain on target.	**1.10** CUI and customer information remains accessible only to approved parties. **1.20** Personnel information remains accessible only to approved parties. **1.30** Corporate value and stock prices are unaffected.

Aligned with SEC rule's materiality clauses.

This is when you would disclose an incident.

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Your Likelihood Levels Define What is “Foreseeable”

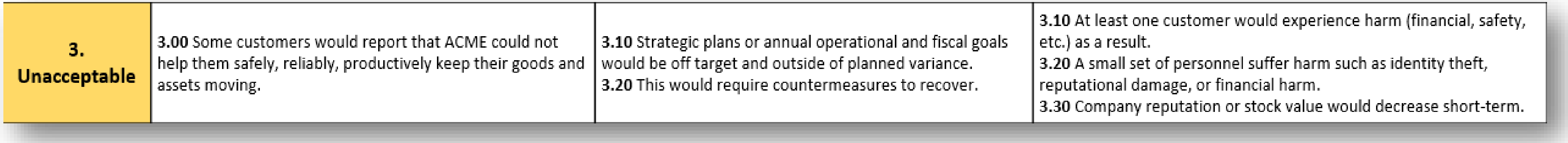
Likelihood Score	Label	Description
5	Continuous	This happens regularly.
4	Common	This happens occasionally.
3	Foreseeable, Expected	We are certain this will eventually occur, but it is not common.
2	Foreseeable, Not Expected	This is plausible, but not expected.
1	Not Foreseeable	This is not plausible in the environment.

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Defining “The Line” of Acceptable Risk

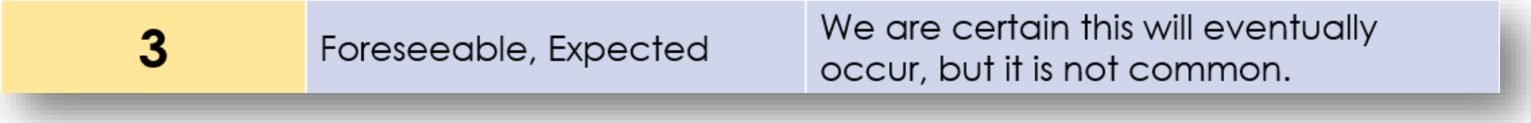
Impact – At this impact level this organization wishes to <u>remediate</u>



3. Unacceptable	**3.00** Some customers would report that ACME could not help them safely, reliably, productively keep their goods and assets moving.	**3.10** Strategic plans or annual operational and fiscal goals would be off target and outside of planned variance. **3.20** This would require countermeasures to recover.	**3.10** At least one customer would experience harm (financial, safety, etc.) as a result. **3.20** A small set of personnel suffer harm such as identity theft, reputational damage, or financial harm. **3.30** Company reputation or stock value would decrease short-term.

X

Likelihood – At this likelihood this organization wishes to <u>remediate</u>



3	Foreseeable, Expected	We are certain this will eventually occur, but it is not common.

=9

<u>Defining “The Line”</u>

This organization decided that when an event likelihood is “**Foreseeable, Expected**” AND the impact is “**Unacceptable**” then this is their “line” at and above which **they always will remediate**.

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

The LINE Identifies those Risks that *Require Treatment* and those Risks we Can **Accept**

The **red line** represents our **Acceptable Risk Level** (a "9"), below which we "**accept**" the risk and at or above which we must do something to "**mitigate**" the risk.

Risk ID	Risk Score	Risk Description	Likelihood	MISSION (For Our Customers)	OBJECTIVES (Business Goals)	OBLIGATIONS (3^{RD} Party & Public)
12	**25**	IT Security conducts informal assessments of all third parties prior to contract completion.	5	4	3	5
8	**15**	Secure application development is conducted by a third party that is non contractually obligated or coding securely.	3	4	4	5
2	**12**	Remote access and remote working policy has not been developed	3	4	3	2
5	**6**	Passwords for privileged accounts not adequately managed	2	2	3	2
9	**6**	Employee onboarding lacks access roles	3	2	1	2

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question #2

Which has the most influence **at your organization** for determining whether risks are "acceptable" or "not acceptable" to the business?

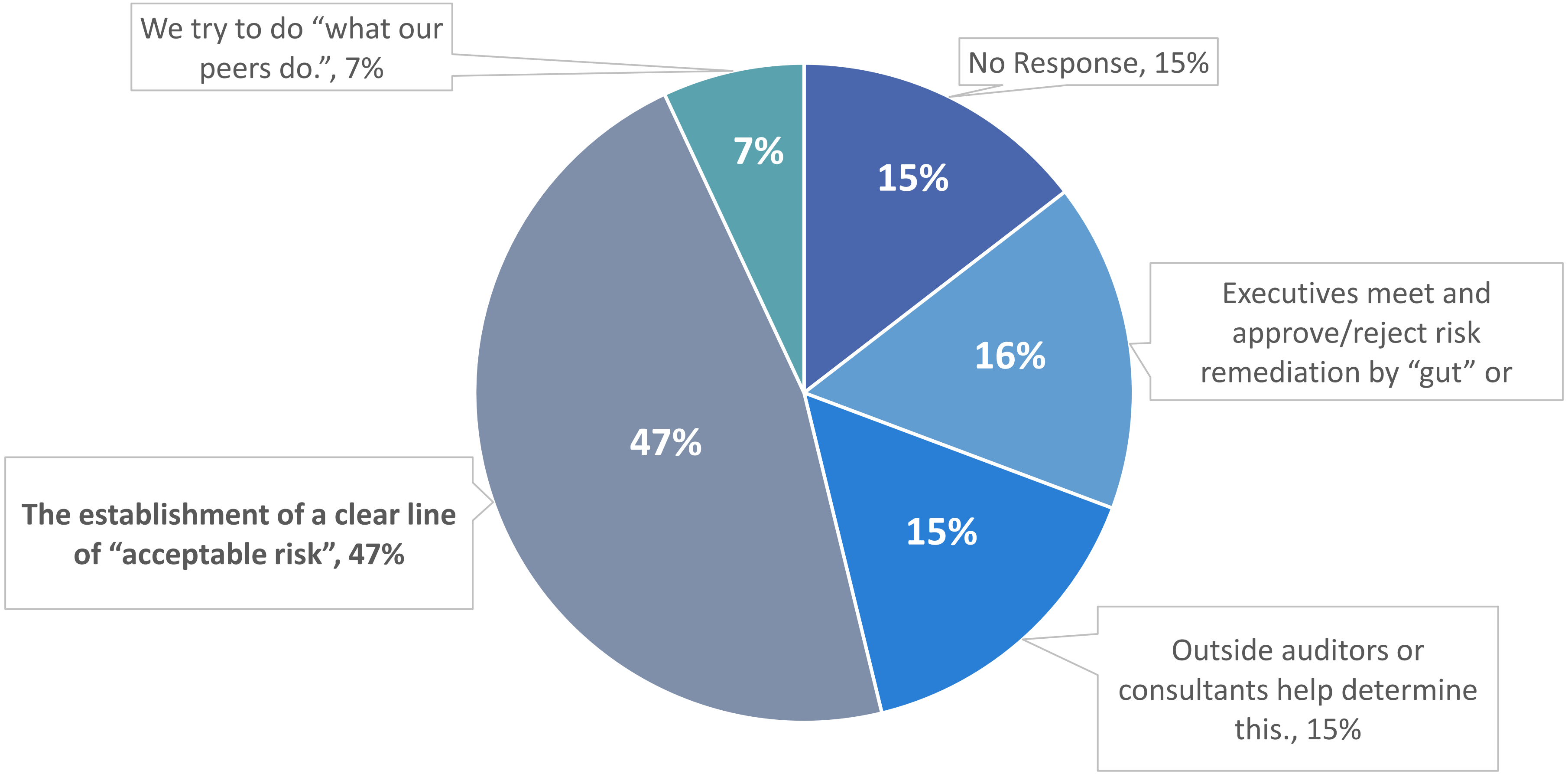
a. **Outside auditors** or **consultants** help determine this.
b. We try to do "what our **peers** do."
c. **Executives** meet and approve/reject risk remediation by "gut" or available budget.
d. The establishment of a **clear line of "acceptable risk"**

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question 2

Poll #2: Which has the most influence for determining whether risks are "acceptable" or "not acceptable" to the business?



© 2023 HALOCK Security Labs. All rights reserved.

2

Ensuring your security program is **Legally Defensible** And complies with **the new SEC Cybersecurity Rules** (published July 26, 2023).

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

What is Duty of Care?

- **Duty of Care** is foundational for assessing liability in our legal system since 1842
- **Duty of Care Risk Analysis (DoCRA)** is the implementation of Duty of Care for Cybersecurity Risk Assessments
- **DoCRA** has had significant adoption
- **Over 120,000 downloads** of the CIS RAM 2.0 (DoCRA-Based Risk Assessment)
- **DoCRA has been recognized and advocated by state Attorneys General** to determine whether **controls were legally “reasonable” during a breach**
- **Utilized by federal regulators** to develop post-breach corrective action plans (injunctive relief)
- Implementing (and operating) DoCRA **demonstrates your program is legally defensible.**

© 2023 HALOCK Security Labs. All rights reserved.

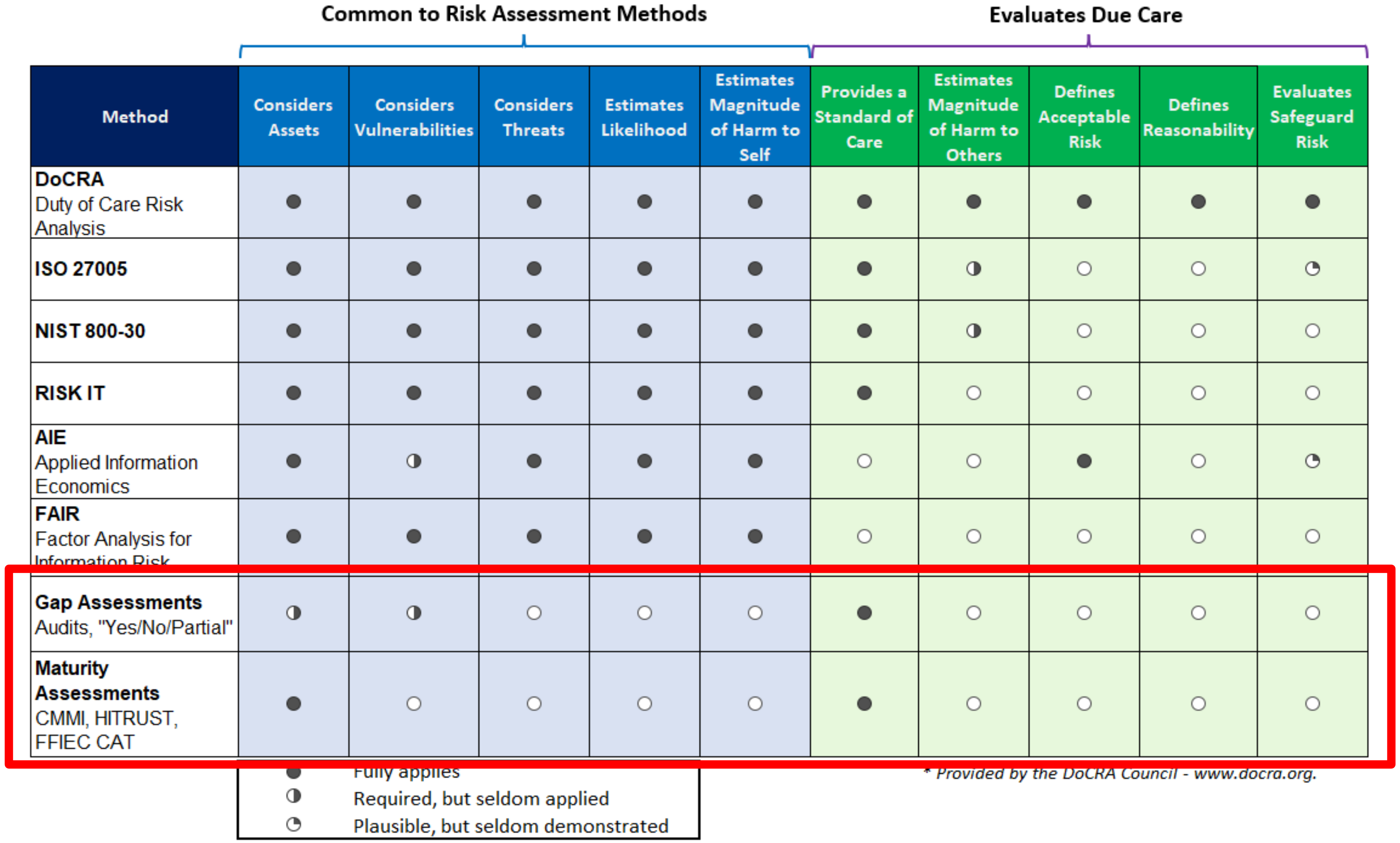
Background on DoCRA

- The **DoCRA Standard** was launched in 2018
- **The DoCRA Council** is a non-profit organization
- **DoCRA** donated a version of its Risk Assessment Methodology to CIS® (Center for Internet Security)
- CIS published the Risk Assessment Methods 1.0 and 2.1 (**CIS RAM**), containing DoCRA, with the CIS Controls Version 8
- **DoCRA** can be utilized with CIS, NIST, ISO or any control set

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

How DoCRA Covers all the Bases for a Legally "Reasonable" Implementation of Controls



	Common to Risk Assessment Methods					Evaluates Due Care				
Method	Considers Assets	Considers Vulnerabilities	Considers Threats	Estimates Likelihood	Estimates Magnitude of Harm to Self	Provides a Standard of Care	Estimates Magnitude of Harm to Others	Defines Acceptable Risk	Defines Reasonability	Evaluates Safeguard Risk
DoCRA Duty of Care Risk Analysis	●	●	●	●	●	●	●	●	●	●
ISO 27005	●	●	●	●	●	●	◑	○	○	◔
NIST 800-30	●	●	●	●	●	●	◑	○	○	○
RISK IT	●	●	●	●	●	●	○	○	○	○
AIE Applied Information Economics	●	◑	●	●	●	○	○	●	○	◔
FAIR Factor Analysis for Information Risk	●	●	●	●	●	○	○	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	◑	◑	○	○	○	●	○	○	○	○
Maturity Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	●	○	○	○	○

●	Fully applies
◑	Required, but seldom applied
◔	Plausible, but seldom demonstrated

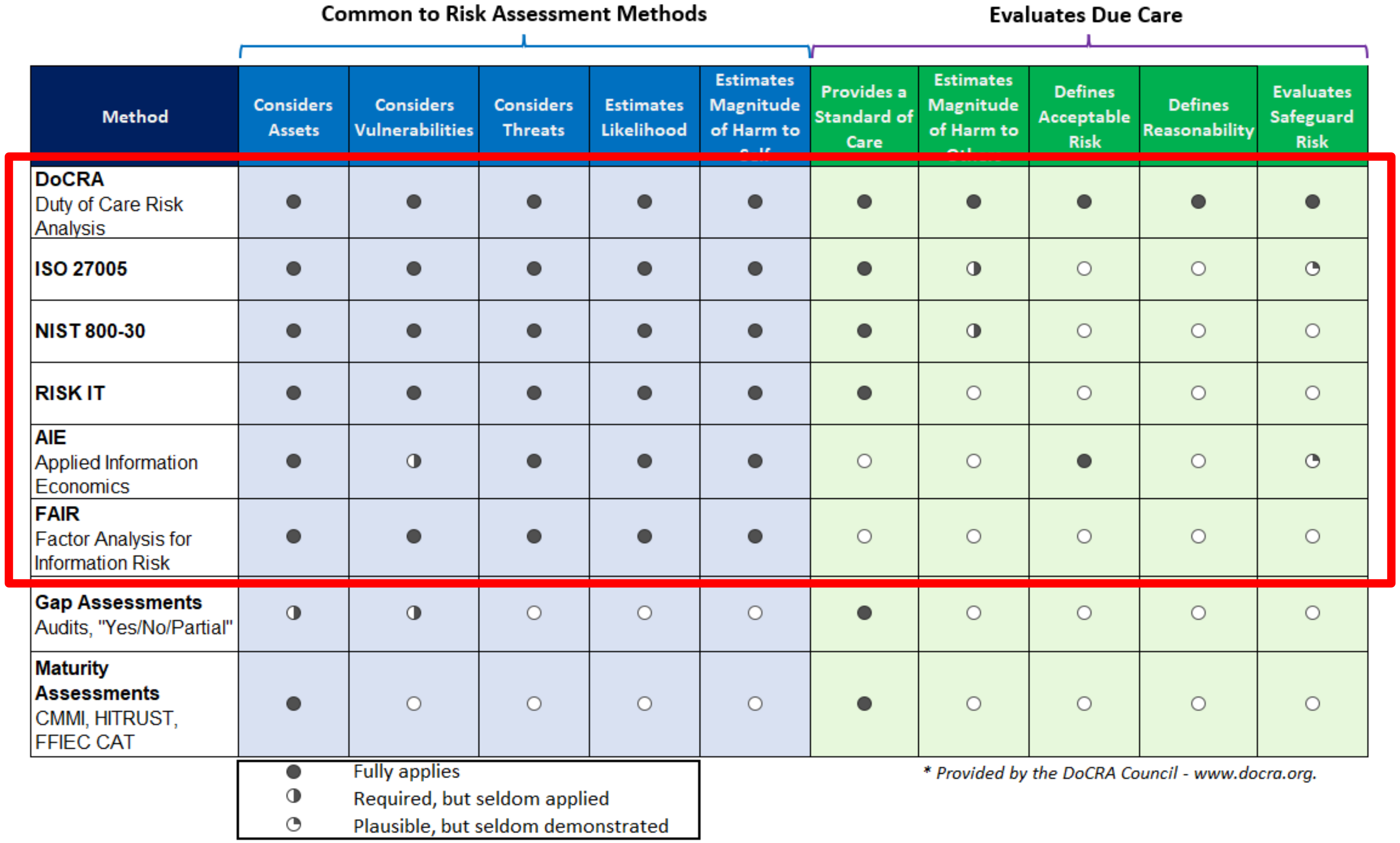
* Provided by the DoCRA Council - www.docra.org.

- Maturity Models and Gap Assessments do not satisfy regulations that require risk analysis to prioritize limited resources.

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

How DoCRA Covers all the Bases for a Legally "Reasonable" Implementation of Controls



Method	Considers Assets	Considers Vulnerabilities	Considers Threats	Estimates Likelihood	Estimates Magnitude of Harm to Self	Provides a Standard of Care	Estimates Magnitude of Harm to Others	Defines Acceptable Risk	Defines Reasonability	Evaluates Safeguard Risk
	Common to Risk Assessment Methods					Evaluates Due Care				
DoCRA Duty of Care Risk Analysis	●	●	●	●	●	●	●	●	●	●
ISO 27005	●	●	●	●	●	●	◑	○	○	◔
NIST 800-30	●	●	●	●	●	●	◑	○	○	○
RISK IT	●	●	●	●	●	●	○	○	○	○
AIE Applied Information Economics	●	◑	●	●	●	○	○	●	○	◔
FAIR Factor Analysis for Information Risk	●	●	●	●	●	○	○	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	◑	◑	○	○	○	●	○	○	○	○
Maturity Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	●	○	○	○	○

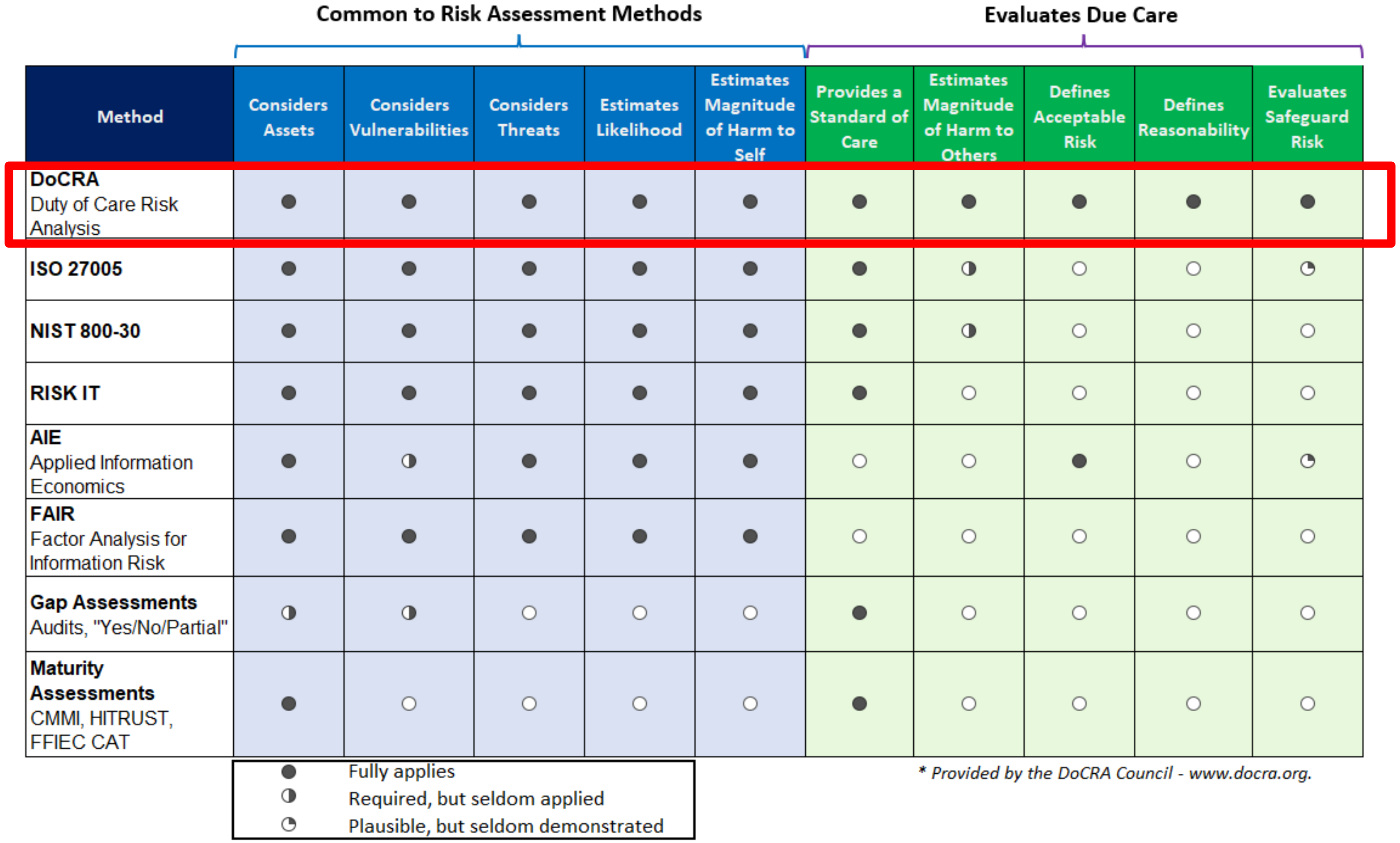
●	Fully applies
◑	Required, but seldom applied
◔	Plausible, but seldom demonstrated

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

- <u>Maturity Models and Gap Assessments do not satisfy regulations that require risk analysis to prioritize limited resources</u>.

© 2023 HALOCK Security Labs. All rights reserved.

How DoCRA Covers all the Bases for a Legally "Reasonable" Implementation of Controls



	Common to Risk Assessment Methods					Evaluates Due Care				
Method	Considers Assets	Considers Vulnerabilities	Considers Threats	Estimates Likelihood	Estimates Magnitude of Harm to Self	Provides a Standard of Care	Estimates Magnitude of Harm to Others	Defines Acceptable Risk	Defines Reasonability	Evaluates Safeguard Risk
DoCRA Duty of Care Risk Analysis	●	●	●	●	●	●	●	●	●	●
ISO 27005	●	●	●	●	●	●	◑	○	○	◔
NIST 800-30	●	●	●	●	●	●	◑	○	○	○
RISK IT	●	●	●	●	●	●	○	○	○	○
AIE Applied Information Economics	●	◑	●	●	●	○	○	●	○	◔
FAIR Factor Analysis for Information Risk	●	●	●	●	●	○	○	○	○	○
Gap Assessments Audits, "Yes/No/Partial"	◑	◑	○	○	○	●	○	○	○	○
Maturity Assessments CMMI, HITRUST, FFIEC CAT	●	○	○	○	○	●	○	○	○	○

●	Fully applies
◑	Required, but seldom applied
◔	Plausible, but seldom demonstrated

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

- Maturity Models and Gap Assessments do not satisfy regulations that require risk analysis to prioritize limited resources.

- Only **DoCRA** requires impacts inside and **outside** the organization to be treated equally.

© 2023 HALOCK Security Labs. All rights reserved.

Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies – July 26, 2023

U.S. SECURITIES AND EXCHANGE COMMISSION ★ MCMXXXIV ★

Clauses and actions

© 2023 HALOCK Security Labs. All rights reserved.

SEC Cybersecurity Risk Management Rules – Highlights

Regulation	Summary of Regulation	What Companies Will Need To Do	Do These 5 Capabilities Enable You to Deliver This?	How Do These 5 Capabilities Enable You to Deliver On This?
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Articulate clearly your cybersecurity strategy “in sufficient detail for a reasonable investor to understand.”	Describe how your **risk management program will inform your investors** about impacts that they would consider **material**.	✓ Delivered	- DoCRA based Calculated Acceptable Risk Definition (CARD) - **halock.com** - **docra.org**

© 2023 HALOCK Security Labs. All rights reserved.

SEC Cybersecurity Risk Management Rules – Highlights

Regulation	Summary of Regulation	What Companies Will Need To Do	Do These 5 Capabilities Enable You to Deliver This?	How Do These 5 Capabilities Enable You to Deliver On This?
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Articulate clearly your cybersecurity strategy "in sufficient detail for a reasonable investor to understand."	Describe how your **risk management program will inform your investors** about impacts that they would consider **material**.	✓ Delivered	- DoCRA based Calculated Acceptable Risk Definition (CARD) - **halock.com** - **docra.org**
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Describe how "any such processes have been integrated into the registrant's overall **risk management system** or processes."	Companies will need to demonstrate a **true risk-based management system (vs. maturity-based management system).** Stating "Our maturity goal is to get to a 3.2" will not be sufficient.	✓ Delivered	- DoCRA covers the bases of Legal Defensibility and SEC Cybersecurity Rule - **halock.com** - **docra.org**

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

SEC Cybersecurity Risk Management Rules – Highlights

Regulation	Summary of Regulation	What Companies Will Need To Do	Do These 5 Capabilities Enable You to Deliver This?	How Do These 5 Capabilities Enable You to Deliver On This?
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Articulate clearly your cybersecurity strategy "in sufficient detail for a reasonable investor to understand."	Describe how your **risk management program will inform your investors** about impacts that they would consider **material**.	✓ Delivered	• DoCRA based Calculated Acceptable Risk Definition (CARD) • **halock.com** • **docra.org**
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Describe how "any such processes have been integrated into the registrant's overall risk management system or processes."	Companies will need to demonstrate a **true risk-based management system (vs. maturity-based management system).** Stating "Our maturity goal is to get to a 3.2" will not be sufficient.	✓ Delivered	• DoCRA covers the bases of Legal Defensibility and SEC Cybersecurity Rule • **halock.com** • **docra.org**
§229.106 (Item 106) Cybersecurity. (b) **Governance**. (2)(ii)	Describe the processes by which **Management is informed** of risks and incidents	Companies will need **Management to be informed in business terms** of risks, incidents and risk reduction progress.	✓ Delivered	• Reasonable Risk SaaS Executive Status **Management** Report • **reasonablerisk.com**

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

SEC Cybersecurity Risk Management Rules – Highlights

Regulation	Summary of Regulation	What Companies Will Need To Do	Do These 5 Capabilities Enable You to Deliver This?	How Do These 5 Capabilities Enable You to Deliver On This?
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Articulate clearly your cybersecurity strategy "in sufficient detail for a reasonable investor to understand."	Describe how your risk management program will inform your investors about impacts that they would consider material.	✓ Delivered	- DoCRA based Calculated Acceptable Risk Definition (CARD) - halock.com - docra.org
§229.106 (Item 106) Cybersecurity. (b) **Risk management and strategy.** (1)	Describe how "any such processes have been integrated into the registrant's overall risk management system or processes."	Companies will need to demonstrate a true risk-based management system (vs. maturity-based management system). Stating "Our maturity goal is to get to a 3.2" will not be sufficient.	✓ Delivered	- DoCRA covers the bases of Legal Defensibility and SEC Cybersecurity Rule - halock.com - docra.org
§229.106 (Item 106) Cybersecurity. (b) **Governance**. (2)(ii)	Describe the processes by which Management is informed of risks and incidents	Companies will need Management to be informed in business terms of risks, incidents and risk reduction progress.	✓ Delivered	- Reasonable Risk SaaS Executive Status Management Report - reasonablerisk.com
§229.106 (Item 106) Cybersecurity. (c) **Governance** (1)	Describe Board of Directors oversight on cybersecurity risks and a description of how Board of Directors are informed.	Companies will need to convey risks and key decisions to Board of Directors in business terms.	✓ Delivered	- Reasonable Risk SaaS Expenditure Approval Board of Directors Report - reasonablerisk.com

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

3

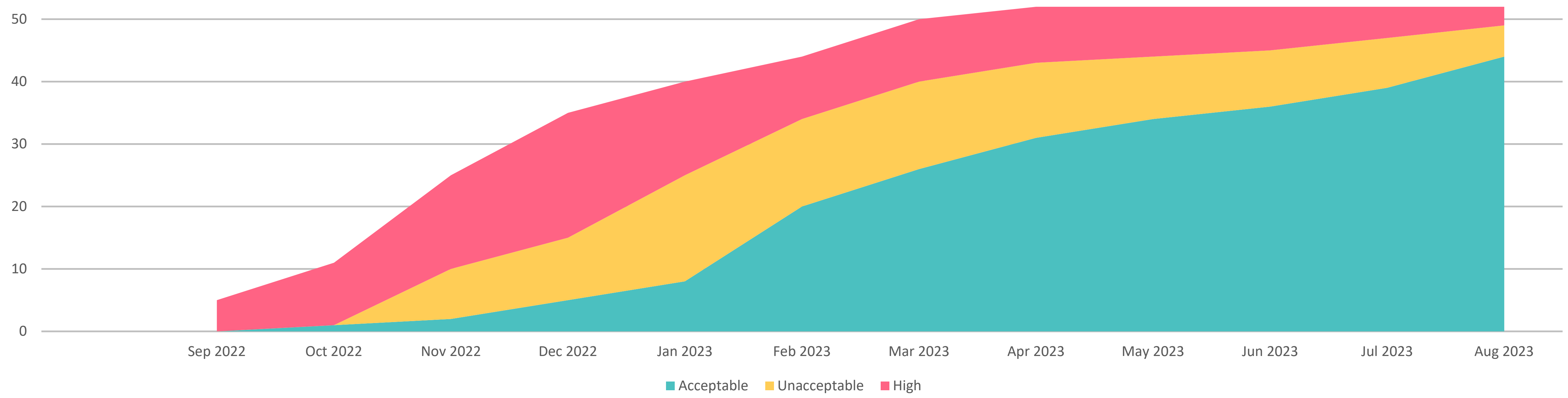
Understanding the Known Risk to your organization.

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

Big Picture: Program Progress Over Time

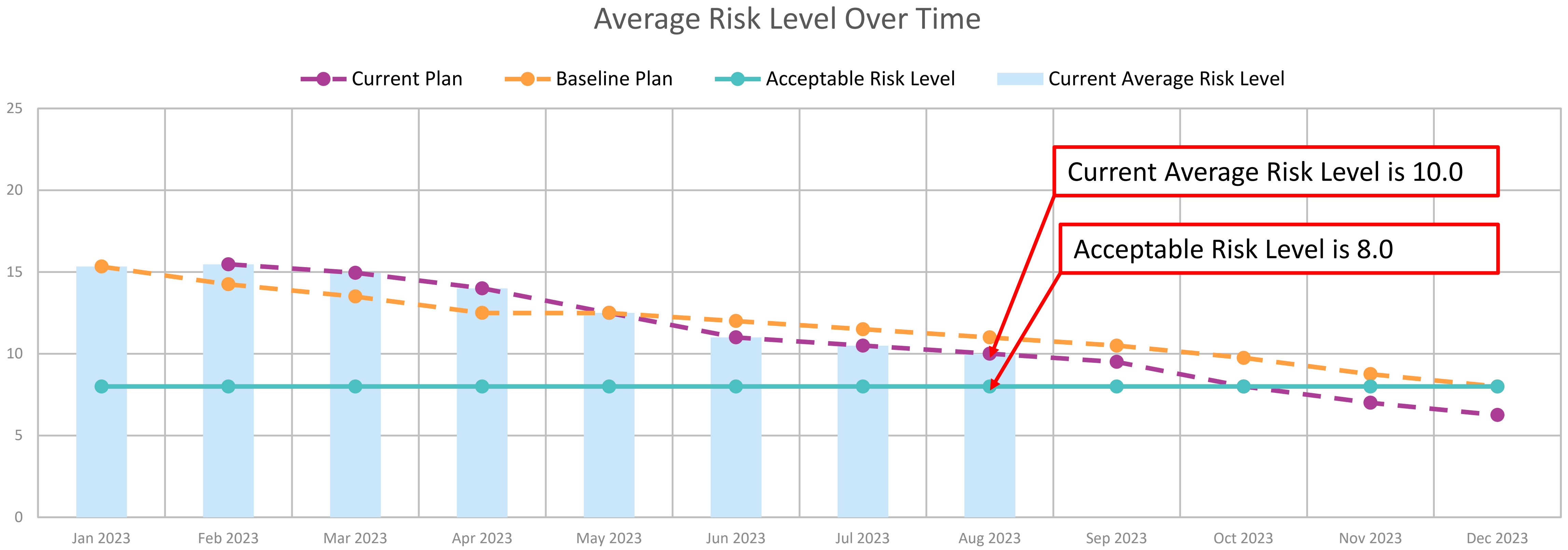
	Sep 2022	Oct 2022	Nov 2022	Dec 2022	Jan 2023	Feb 2023	Mar 2023	Apr 2023	May 2023	Jun 2023	Jul 2023	Aug 2023
High	5	10	15	20	15	10	10	9	8	7	5	3
Unacceptable			8	10	17	14	14	12	10	9	8	5
Acceptable		1	2	5	8	20	26	31	34	36	39	44
Total	**5**	**11**	**25**	**35**	**40**	**44**	**50**	**52**	**52**	**52**	**52**	**52**



© 2023 HALOCK Security Labs. All rights reserved.

How Does Our Average Risk Score Compare to the Acceptable Risk Level?

- Our Current Average Risk Level across the entire Risk Register is 10.0
- Our Acceptable Risk Level is 8.0
- We are not yet where we want to be, but we are trending there



Current Average Risk Level is 10.0

Acceptable Risk Level is 8.0

© 2023 HALOCK Security Labs. All rights reserved.

Given that Averages Can Hide Outliers, List All Unacceptable Risks

24	Centralize Security Event Alerting Status: In Progress	20
52	Establish and Maintain a Data Management Process Status: In Progress	16
49	Establish and Maintain a Data Inventory Status: In Progress	16
50	Securely Dispose of Data Status: In Progress	12
31	Test Data Recovery Status: In Progress	12
12	Train Workforce on Data Handling Best Practices Status: In Progress	10
47	Configure Automatic Session Locking on Enterprise Assets Status: In Progress	9

© 2023 HALOCK Security Labs. All rights reserved.

4

Providing the C-Suite with a Roadmap for your program that reduces risk to an acceptable level.

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

Why is Providing a Roadmap so Difficult?

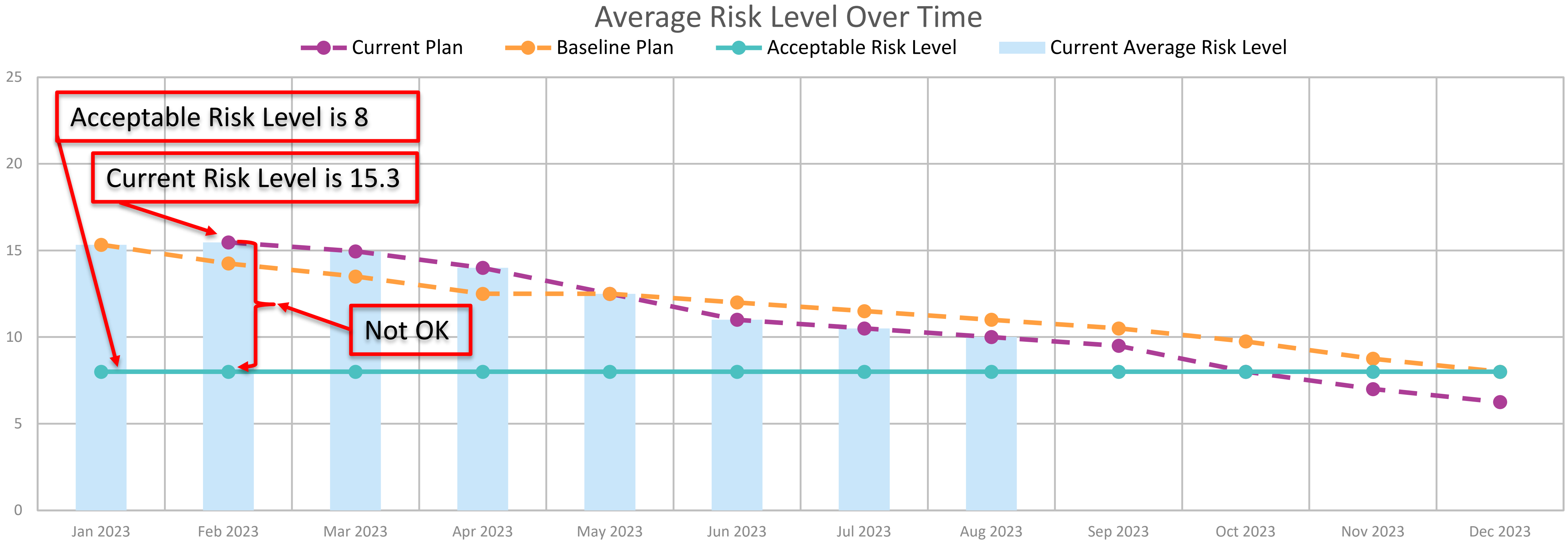
- It is difficult to maintain risk models with changing data over time
- If you do a good job, you’ll be asked to always produce it going forward
- How do you define if the overall Risk Level is “OK” or not?
- And if the Risk Level is “Not OK”, how do you define “how to get to OK?”

© 2023 HALOCK Security Labs. All rights reserved.

Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was over 15 in January **(not OK)**
- We are striving to get to Acceptable Risk Level of 8 or less **(how we define OK)**



Acceptable Risk Level is 8

Current Risk Level is 15.3

Not OK

© 2023 HALOCK Security Labs. All rights reserved.

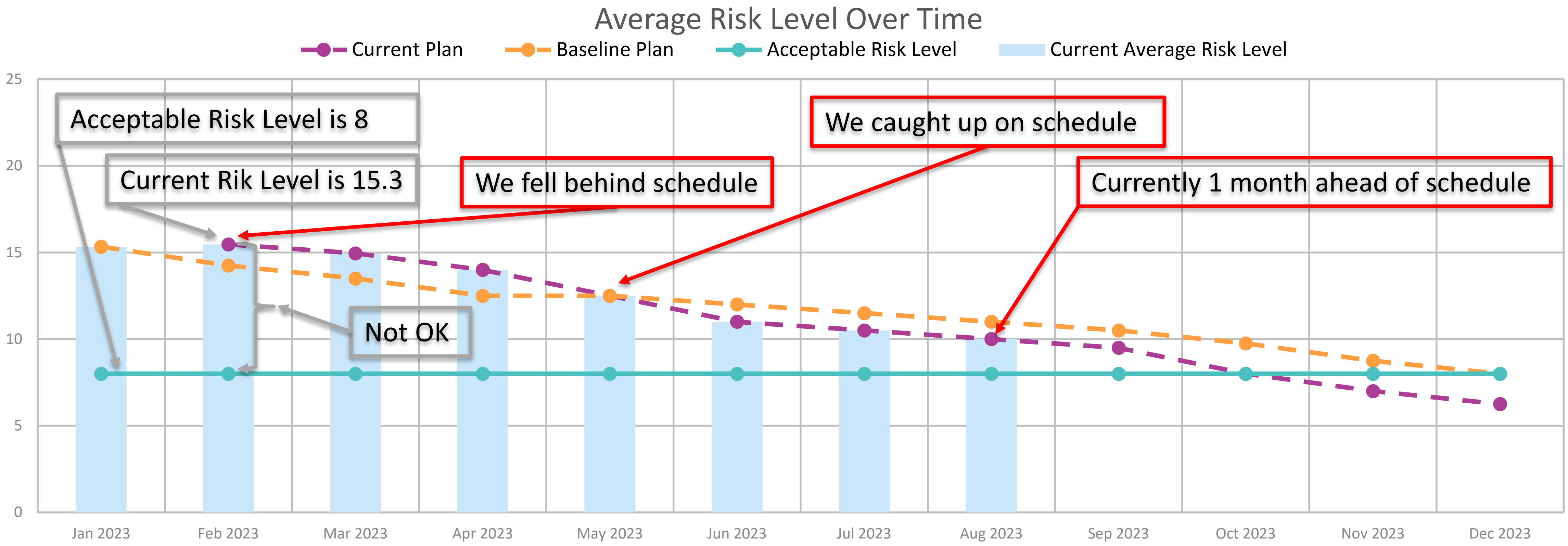
Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was over 15 in January **(not OK)**
- We are striving to get to Acceptable Risk Level of 8 or less **(how we define OK)**

How do we get to OK?

- We fell behind schedule in February of 2023 but have now caught up in May and currently 1 month ahead of schedule.



Acceptable Risk Level is 8

Current Rik Level is 15.3

We fell behind schedule

We caught up on schedule

Currently 1 month ahead of schedule

Not OK

© 2023 HALOCK Security Labs. All rights reserved.

Roadmap: Planned vs. Actual Risk Reduction

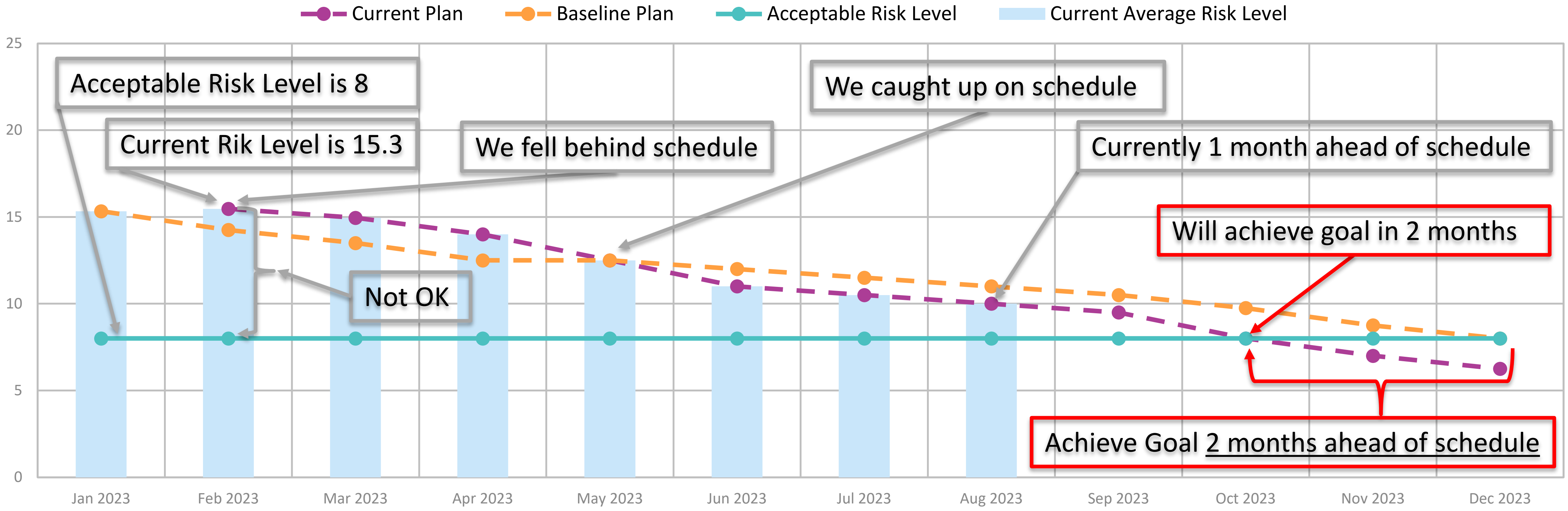
Are we OK?

- Our Current Average Risk level was over 15 in January **(not OK)**
- We are striving to get to Acceptable Risk Level of 8 or less **(how we define OK)**

How do we get to OK?

- We fell behind schedule in February of 2023 but have now caught up in May and currently 1 month ahead of schedule.
- We **will achieve our goal in 2 months**, this October, which will be **2 months ahead of schedule.**
- Our risk reduction will follow the “current plan” line as we implement the remediation projects that you have approved.

Average Risk Level Over Time



Acceptable Risk Level is 8

Current Rik Level is 15.3

We fell behind schedule

We caught up on schedule

Currently 1 month ahead of schedule

Not OK

Will achieve goal in 2 months

Achieve Goal 2 months ahead of schedule

© 2023 HALOCK Security Labs. All rights reserved.

5

Communicating Risks and Justifying Expenditure Requests in business terms.

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.

Can C-Suite and BoD Make Informed Decisions?

If you asked your Leadership Team these four questions,
how would they respond?

1. **Risk Management:** Do we have a "clear line" to definitively know if a Risk is "okay" to accept, or "not okay" to accept and we need to remediate it?
2. **Communication:** When discussing risks, is Cybersecurity and Senior Leadership speaking the same or different languages?
3. **Legal Protection:** Are we in a legally defensible position?
4. **Budgeting:** Are we spending the right amount?

© 2023 HALOCK Security Labs. All rights reserved.

Can C-Suite and BoD Make Informed Decisions?

We surveyed 140 **C-Level Executives**[1]. Of the respondents:

- **65%** DO NOT understand **when** it is "okay" to accept a risk
- **85%** DO NOT understand **what** Cybersecurity is saying
- **96%** DO NOT know if they are in a **legally defensible** position
- **97%** DO NOT know if they are spending the **right amount** on Security

Executives *do not* have the information they need to feel comfortable making decisions!

[1] Cybersecurity Breakfast "How Safe Is Your Data" Webinar - April 22nd, 2021

© 2023 HALOCK Security Labs. All rights reserved.

What Happens if Executives Do Not Have the Information They Need to Make Informed Decisions?

- They approve as little as they feel they must
- That is why the Cybersecurity function is so frequently under-resourced

© 2023 HALOCK Security Labs. All rights reserved.

The Trust & Confidence Meter

-1
0
1
2
3
4
5
6
7
Trust &
Confidence

Trust

In how you Manage Security

Confidence

In the information presented to reach a Quality Decision

© 2023 HALOCK Security Labs. All rights reserved.

Two Expenditure Approval Approaches with Different Outcomes

Example: Data Loss Prevention (DLP) Budget Approval Request

1. **Traditional Approach**

2. **Proven Budget Narrative Approach**

© 2023 HALOCK Security Labs. All rights reserved.

Traditional Expenditure Approval Approach

© 2023 HALOCK Security Labs. All rights reserved.

Traditional Approach – DLP Expenditure Request

CISO: “We need a DLP product to catch personal information for claims data that might be leaving the company through email, FTP, web app file shares, or other means.”

CISO: “I recommend this $280,000 solution that solves this burning issue and gets us everything we need.”

CFO: “That’s a quarter of your budget. Is there a more affordable option or could we implement just a portion of it?”

CISO: “The entry level, bare-bones solution from this vendor is $50,000, but less effective.”

CFO: **“**Let’s start with approving $50,000 this year and re-evaluate next year.”

FAIL

© 2023 HALOCK Security Labs. All rights reserved.

Traditional Approach – DLP Expenditure Request

Does Management Have Information to Feel Comfortable?

1. **Risk Management:** "clear line" to know if a Risk "is okay" to accept? **Don't Know**
2. **Communication:** Speaking the same or different languages? **Don't Understand**
3. **Legal Protection**: Legally protected? **Not Sure**
4. **Budgeting:** Spending the right amount? **Don't Know**

Trust and Confidence

-1
0
1
2
3
4
5
6
7
Trust &
Confidence

What happened?

- The Budget *Approver did not have* the information they needed, so the Budget *Requester did not receive* the budget they needed!
- The *CISO received 20%* of the budget they requested.
- The *company is exposed* and the *CISO is exposed.*

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Approach Utilizing These 5 Capabilities

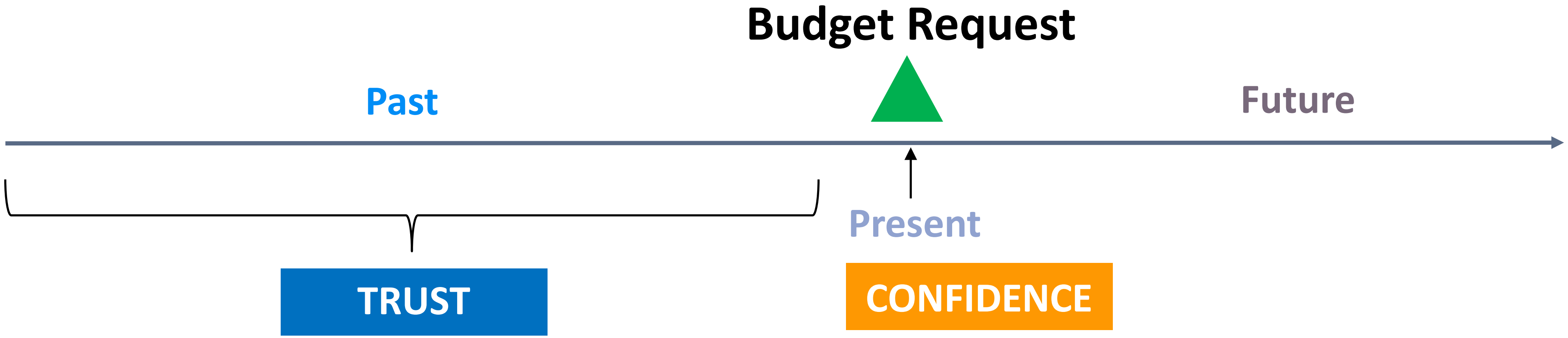
Putting it All Together…

© 2023 HALOCK Security Labs. All rights reserved.

Two Factors to Consider When Approving Expenditures

TRUST In how we have managed responsibilities in the **past**

CONFIDENCE In the information presented in the **present** to reach an informed decision



Budget Request

Past

Future

Present

TRUST

In how we have managed responsibilities in the **past**

CONFIDENCE

In the information presented in the **present** to reach an informed decision

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Approach to Establishing Trust and Enabling Confidence

Trust
in how we <u>manage responsibilities</u>

1. **Big Picture** – Program Progress Over Time
2. **Since Our Last Review** – Program Changes
3. **Roadmap** – Planned vs. Actual Risk Reduction (Historic and Future)

Confidence
in the information presented to reach an <u>informed decision</u>

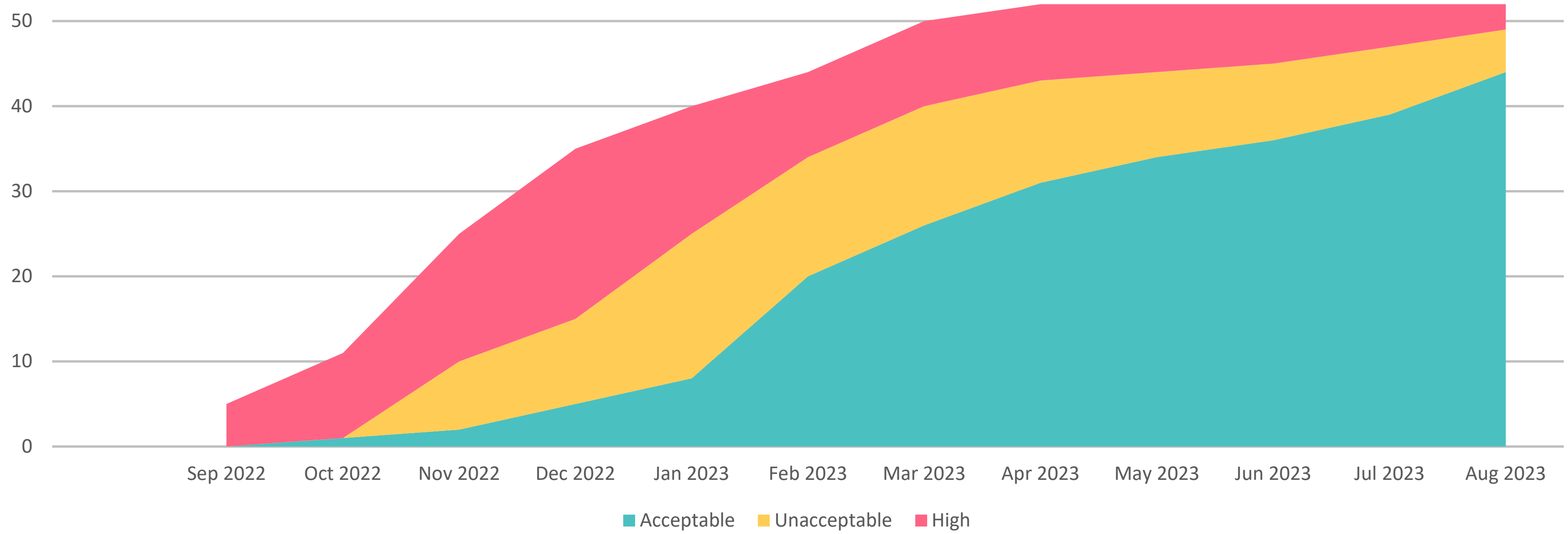
4. **List of Unacceptable Risks**
5. **Budget Request – Level 1**: Budget Level (Projects and Costs)
6. **Budget Request – Level 2**: Project Level (Projects and Business Impacts)
7. **Budget Request – Level 3**: Risk Level (Risks and Business Impacts)

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

1 Big Picture - Program Progress Over Time

	Sep 2022	Oct 2022	Nov 2022	Dec 2022	Jan 2023	Feb 2023	Mar 2023	Apr 2023	May 2023	Jun 2023	Jul 2023	Aug 2023
High	5	10	15	20	15	10	10	9	8	7	5	3
Unacceptable			8	10	17	14	14	12	10	9	8	5
Acceptable		1	2	5	8	20	26	31	34	36	39	44
Total	**5**	**11**	**25**	**35**	**40**	**44**	**50**	**52**	**52**	**52**	**52**	**52**



-1
0
1
2
3
4
5
6
7
Trust &
Confidence

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

2 Since Our Last Review – Program Changes

New Risks Identified	Several new risks identified relating to the Business Email Compromise Incident we experienced last quarter.

Risks	Acceptable	Unacceptable	High
Risk Count | Prior to Last Review	**7**	**2**	**4**
New Risks Identified Since Last Review	**0**	**1**	**1**
Risk Count | Current	**7**	**3**	**5**

What contributed to risks since last review:

- □ Customer Requirements
- ☒ Penetration Test
- □ Zero Day
- ☒ Incident
- □ Regulatory Change
- □ Other (see below)
- □ Mergers & acquisitions
- □ Scope Increase
- □ Threat Landscape
- □ New Technology
- □ Other Assessment

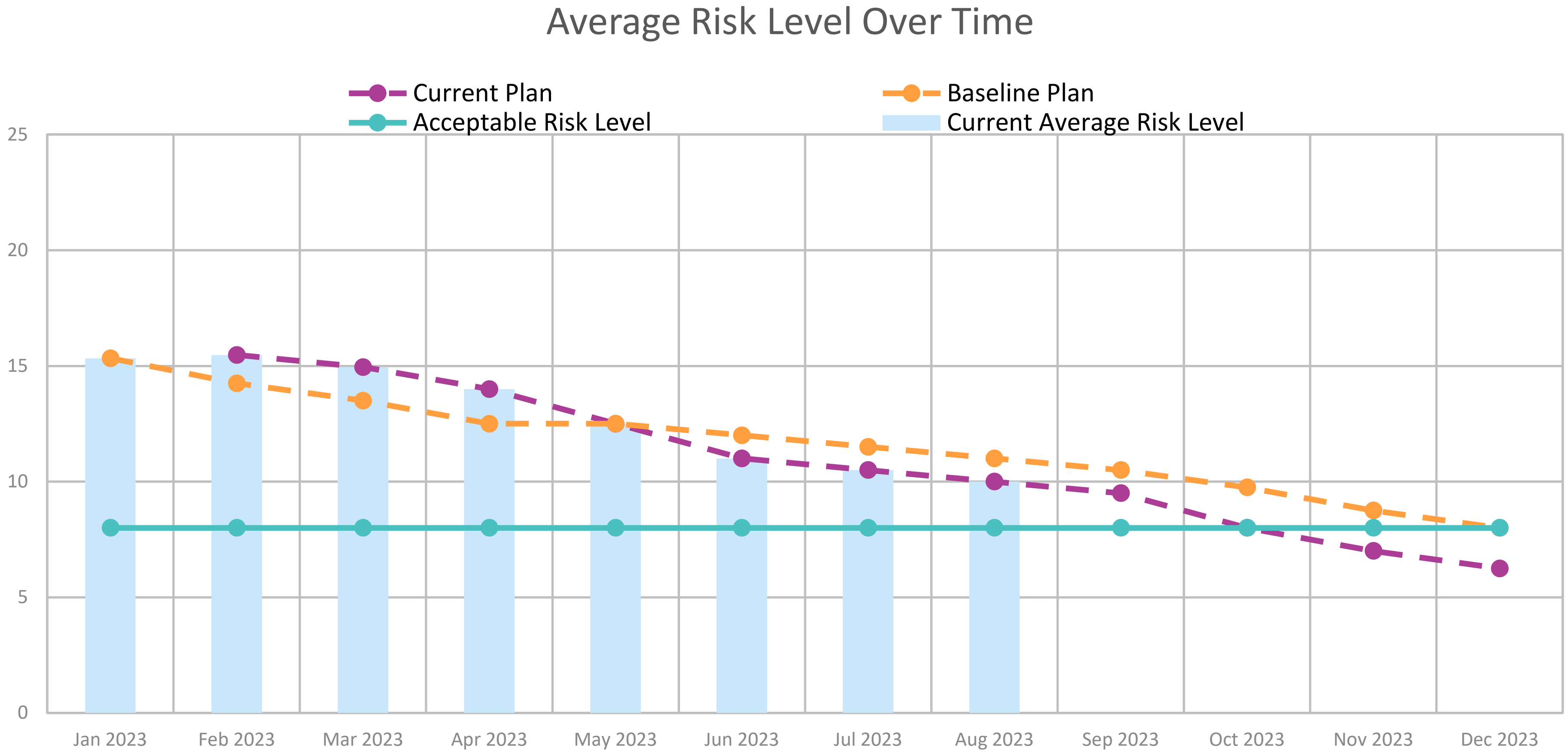
Comments	We completed our yearly Pen Test and also experienced a security incident in the Finance Business Unit relating to Business Email Compromise (BEC)

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

3 Roadmap – Planned vs. Actual Risk Level

- As of May, we are ahead of schedule and currently on track to achieve the target risk level 2 months ahead of schedule.
- The decisions you made when you approved resources in January, ***enabled the organization to achieve these results.***



-1
0
1
2
3
4
5
6
7
Trust & Confidence

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

4 List of Unacceptable Risks

- Personally Identifiable Information (PII) unintentionally leaving the organization is currently the highest risk in the Risk Register

Risk ID	Risk Score	Risk Description	Likelihood	MISSION (For Our Customers)	OBJECTIVES (Business Goals)	OBLIGATIONS (3RD Party & Public)
12	20	PII leaving the perimeter unintentionally	4	4	3	5
8	15	Secure application development is conducted by a third party that is non contractually obligated or coding securely.	3	4	4	5
2	12	All access requests are submitted via ServiceNow and executed by IT.	3	4	3	2
5	6	Passwords for privileged accounts not adequately managed	2	2	3	2
9	6	Employee onboarding lacks access roles	3	2	1	2

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

5 Level 1: Budget Level

Remediation Project	Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
					Hard Costs	Soft Costs	Hard Costs	Soft Costs	
DLP Implementation	12/31/2022	Open	No	12	$250,000	$30,000	$20,000	$10000	**20 to 6**
Total					**$250,000**	**$30,000**	**$20,000**	**$10,000**	

Today's Budget Request Summary

- Total Initial **Implementation Costs**: $280,000 ($250,000 Hard Costs + $30,000 Soft Costs)
- Total Ongoing **Yearly Ongoing Costs**: $30,000 ($20,000 Hard Costs + $10,000 Soft Costs)

Yearly Budget Variance Summary

- Yearly Budget Approved: $1,000,000
- Yearly Budget Already Committed: $800,000
- Budget Variance Requested: $80,000 ($280,000 + $800,000 = $1,080,000. This $80,000 Over Approved Budget)

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Level 1 – Is Budget Level Request Sufficient?

Is the Request **Approved** at ***BUDGET LEVEL*** of detail?

YES

Expenditure is Approved at this level.
Great job!

No

If more detail is required, we can move to the ***PROJECT LEVEL.***

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

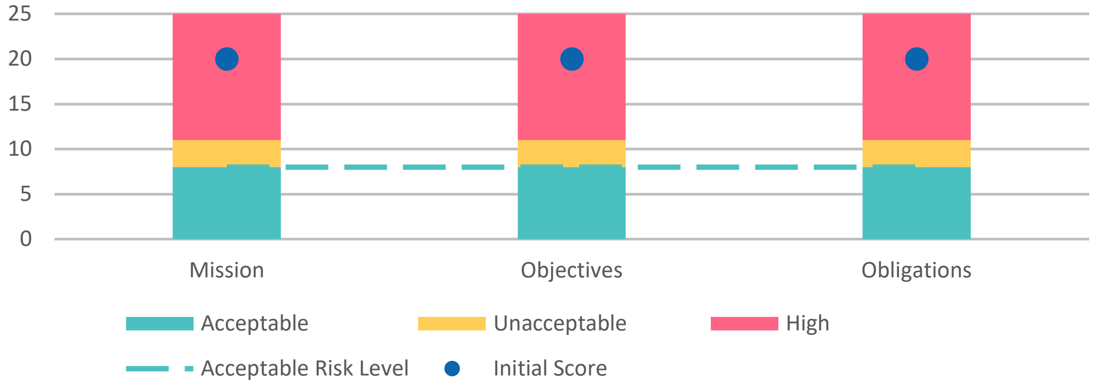
6 Level 2: Project Level

Project Name: ***DLP Implementation Project***

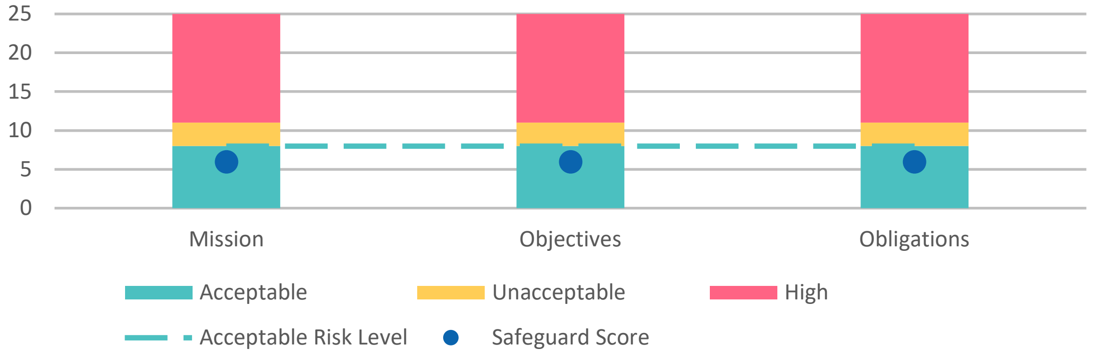
Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
				Hard Costs	Soft Costs	Hard Costs	Soft Costs	
12/31/2021	Open	No	12	$250,000	$30,000	$20,000	$10,000	**20 to 6**

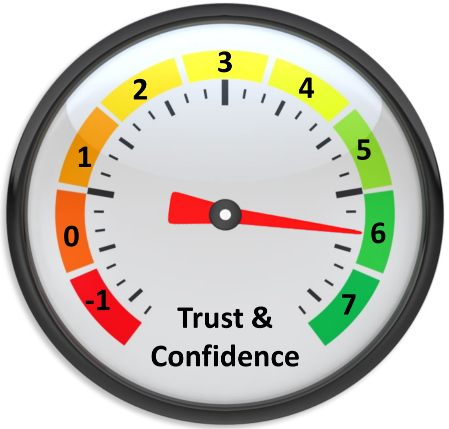
What This Project Accomplishes	PII Leaving Perimeter. Utilizing a $165 cost per lost PII record (2023 IBM Cost of Data Breach Report), we calculate a breach cost of $1,650,000 ($165 x 10,000 customer records) with a potential likelihood of (5) multiple time each year. This risk has a potential financial impact of $1,650,000 multiple times per year
Notes	

Risk ID 12 | **BEFORE** THE SAFEGUARD



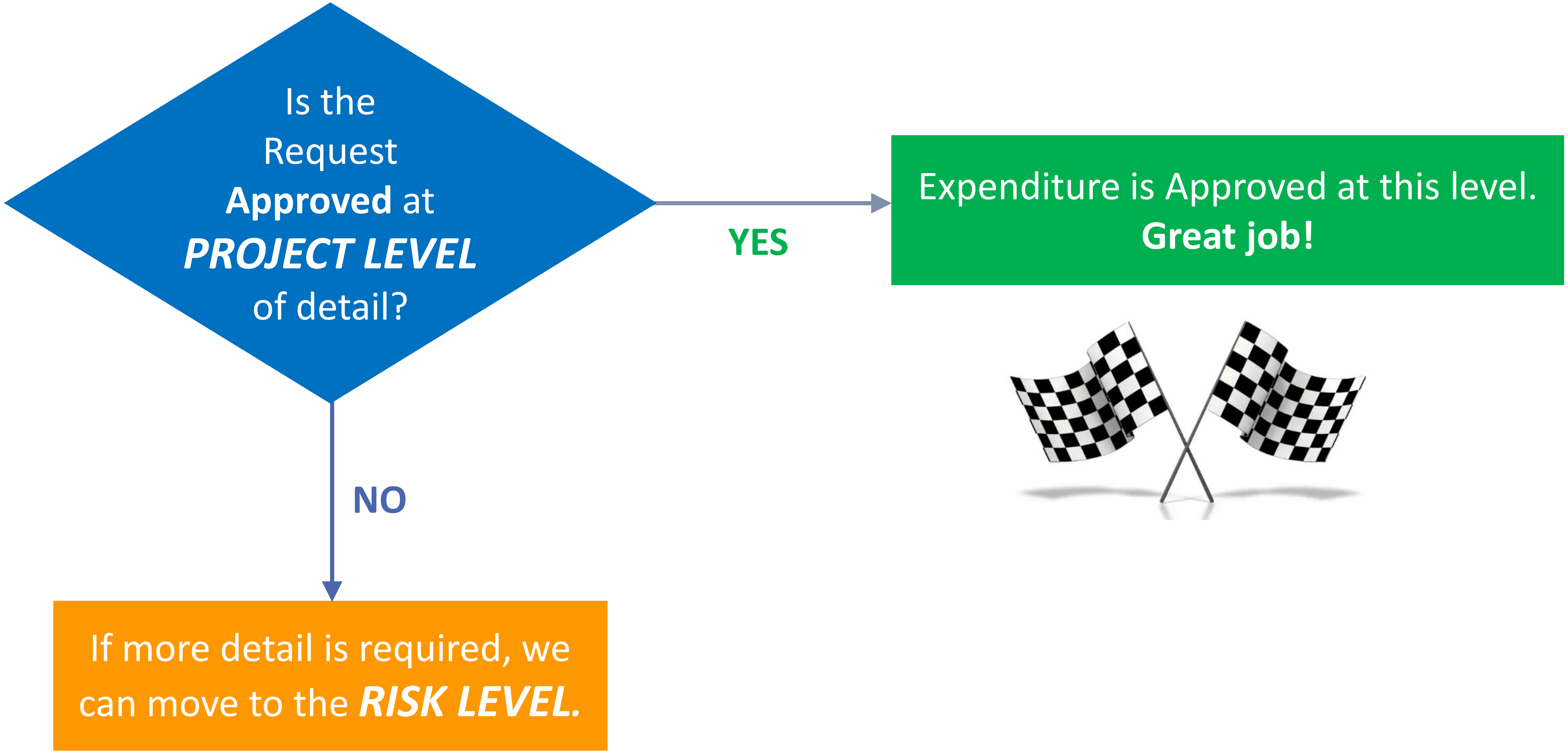
Risk ID 12 | **AFTER** THE SAFEGUARD





© 2023 HALOCK Security Labs. All rights reserved.

Level 2 – Is Project Level Request Sufficient?



Is the Request **Approved** at ***PROJECT LEVEL*** of detail?

YES

Expenditure is Approved at this level. **Great job!**

NO

If more detail is required, we can move to the ***RISK LEVEL.***

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Narrative

7 Level 3: Risk Level

Legend

Risk Score: 25, 20, 15, 10, 5, 0

9 or Greater = Unacceptable

8 or Less = Acceptable

Risk Overview

Risk ID	Risk Description
12	PII Leaving Perimeter. Utilizing a $165 cost per PII lost record (2023 IBM Cost of Data Breach Report), we calculate a breach cost of $1,650,000 ($650 x 10,000 customer records) with a potential likelihood of (5) multiple time each year. This risk has a potential financial impact of $1,6500,000 multiple times per year.

Related Project Overview

Remediation Project	Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
					Hard Costs	Soft Costs	Hard Costs	Soft Costs	
DLP Implementation Project	12/31/2022	Open	No	12	$250,000	$30,000	$20,000	$10,000	**20 to 6**

RISK IF PROJECT IS NOT DONE

Risk Score: 20 out of 25 (Unacceptable)	Mission Score: 16 out of 25	Objectives Score: 16 out of 25	Obligations Score: 20 out of 25
Likelihood = 4 Likelihood (4) x Highest Impact (5) = **Risk of 20**	**4.00** - Many Customers consistently cannot access beneficial information.	**4.00** - Profits may take more than a fiscal year to recover.	**5.00** – 10,000+ records exposed

RISK AFTER DOING THE PROJECT

Risk Score: 6 out of 25 (Acceptable)	Mission Score: 6 out of 25	Objectives Score: 6 out of 25	Obligations Score: 2 out of 25
Likelihood = 2 Likelihood (2) x Highest Impact (3) = **Risk of 6**	**3.00** - Some Customers cannot access the information they need to maintain good health outcomes.	**3.00** - Profits are off planned variance and may take a fiscal year to recover.	**1.00** – 0 to 49 records exposed

HALOCK®

© 2023 HALOCK Security Labs. All rights reserved.

Proven Expenditure Approval Approach

Does Management have information to answer the 4 questions?

1. **Risk Management:** "clear line" to know if a Risk "is okay" to accept? **Yes, must remediate**
2. **Communication:** Speaking the same or different languages? **Yes, impacts in business terms**
3. **Legal Protection**: Legally protected? **Yes, we're performing "due care"**
4. **Budgeting:** Spending the right amount? **Yes, spending $280,000 first year to avoid $1.65M potential impact multiple times each year**

Trust and Confidence

What happened?

- Built Trust using the Proven Expenditure Approval Narrative
- Answered all 4 Questions

Expenditure Approved!

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question #3

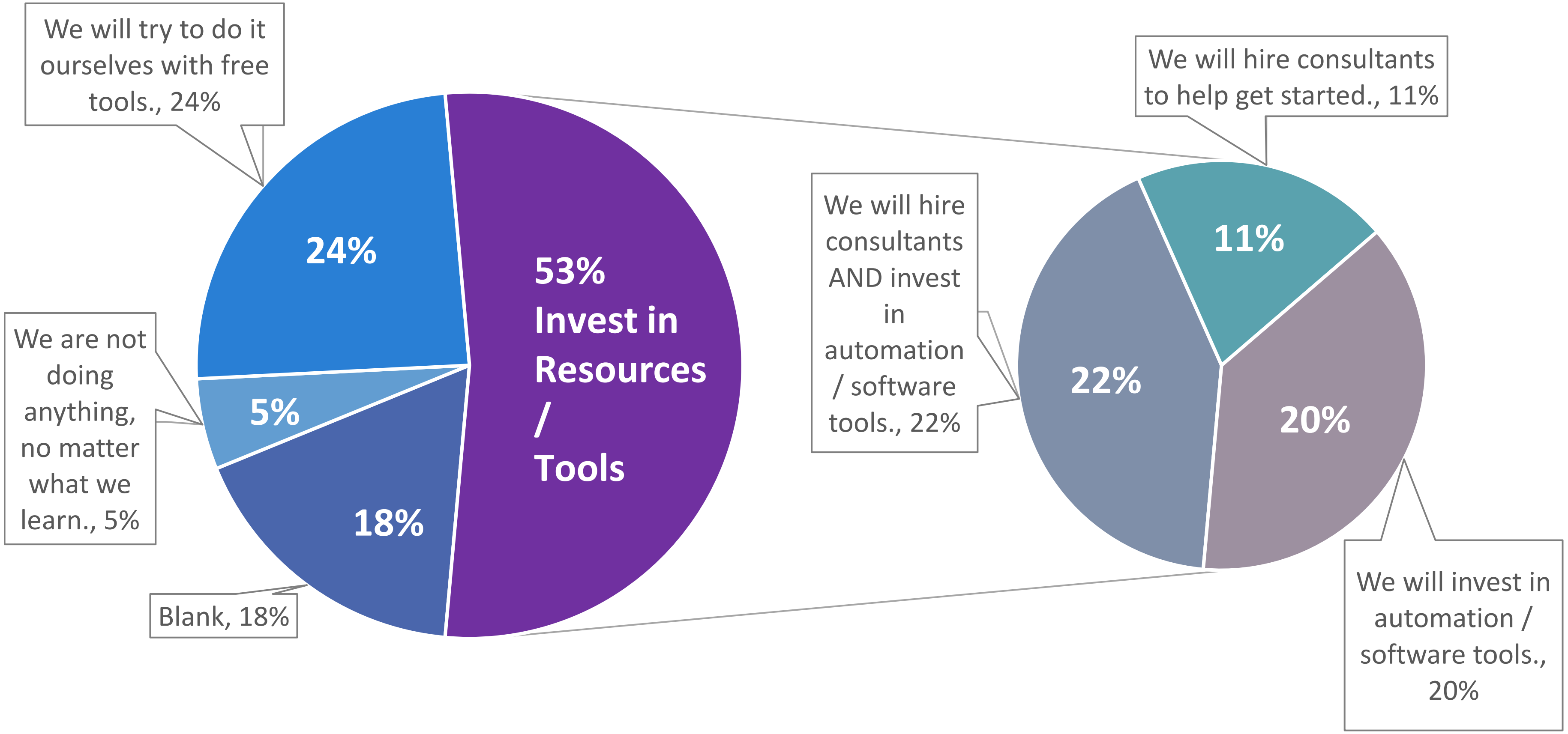
What would be your organization’s approach to enable these 5 Capabilities?

a. We are not doing anything, no matter what we learn.
b. We will try to do it ourselves with free tools.
c. We will hire consultants to help get started.
d. We will invest in automation / software tools.
e. We will hire consultants AND invest in automation / software tools.

© 2023 HALOCK Security Labs. All rights reserved.

Survey Question #3: 53% Will Invest in Consultants, Automation/Software, or Both

Poll #3: What would be your organization's approach to enable these 5 Capabilities?



© 2023 HALOCK Security Labs. All rights reserved.

Helpful Tools

Next Steps…

© 2023 HALOCK Security Labs. All rights reserved.

Templates & Methods - Free

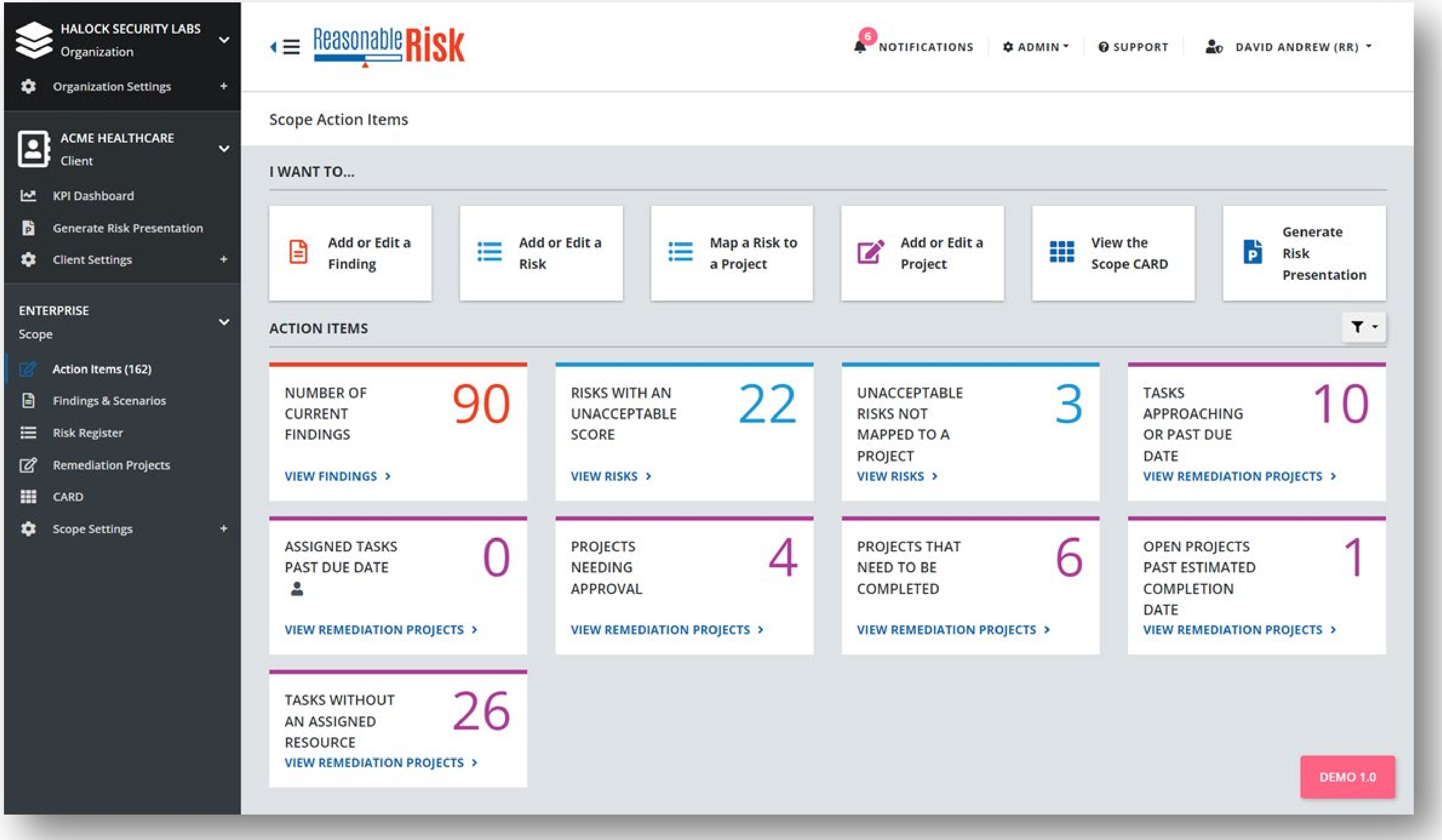
- **CIS RAM** – Risk Assessment Methods, Examples and Templates
  - www.CiSecurity.org

- **This Presentation** – Spreadsheet examples
  - Email me: terryk@halock.com

CIS Controls
CIS Center for Internet Security®
CIS Controls
CIS Risk Assessment Method (RAM)
Version 2.0
Core Document

© 2023 HALOCK Security Labs. All rights reserved.

SaaS Portal – for a Fee



Scope Action Items

I WANT TO...

- Add or Edit a Finding
- Add or Edit a Risk
- Map a Risk to a Project
- Add or Edit a Project
- View the Scope CARD
- Generate Risk Presentation

ACTION ITEMS

NUMBER OF CURRENT FINDINGS 90
VIEW FINDINGS ›

RISKS WITH AN UNACCEPTABLE SCORE 22
VIEW RISKS ›

UNACCEPTABLE RISKS NOT MAPPED TO A PROJECT 3
VIEW RISKS ›

TASKS APPROACHING OR PAST DUE DATE 10
VIEW REMEDIATION PROJECTS ›

ASSIGNED TASKS PAST DUE DATE 0
VIEW REMEDIATION PROJECTS ›

PROJECTS NEEDING APPROVAL 4
VIEW REMEDIATION PROJECTS ›

PROJECTS THAT NEED TO BE COMPLETED 6
VIEW REMEDIATION PROJECTS ›

OPEN PROJECTS PAST ESTIMATED COMPLETION DATE 1
VIEW REMEDIATION PROJECTS ›

TASKS WITHOUT AN ASSIGNED RESOURCE 26
VIEW REMEDIATION PROJECTS ›

© 2023 HALOCK Security Labs. All rights reserved.

Thank you

Terry Kurzynski

CISA, CISSP, PCI QSA, ISO 27001 Auditor

Founder, Senior Partner

HALOCK Security Labs

terryk@halock.com

847.221.0212

Next Steps

Just click and go.

Download this presentation

I have questions (halock.com)

More on the SaaS Portal (reasonablerisk.com)

HALOCK

© 2023 HALOCK Security Labs. All rights reserved.