RSAConference™2024

San Francisco | May 6 – 9 | Moscone Center

THE ART OF POSSIBLE

SESSION ID: GRC-T09

Techniques to Evolve Risk Governance and Comply with the SEC Cybersecurity Rule

#RSAC

Jim Mirochnik

CEO, Senior Partner
HALOCK Security Labs
www.halock.com

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference™ or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

If applicable, insert your organization’s disclaimer statement here, in black (or delete this line)

In the last year

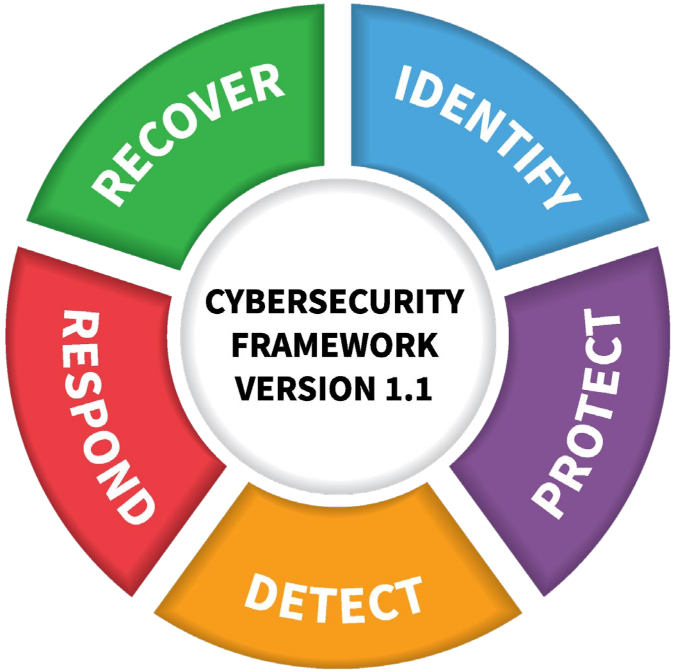
major cybersecurity industry organizations

have increased their requirements

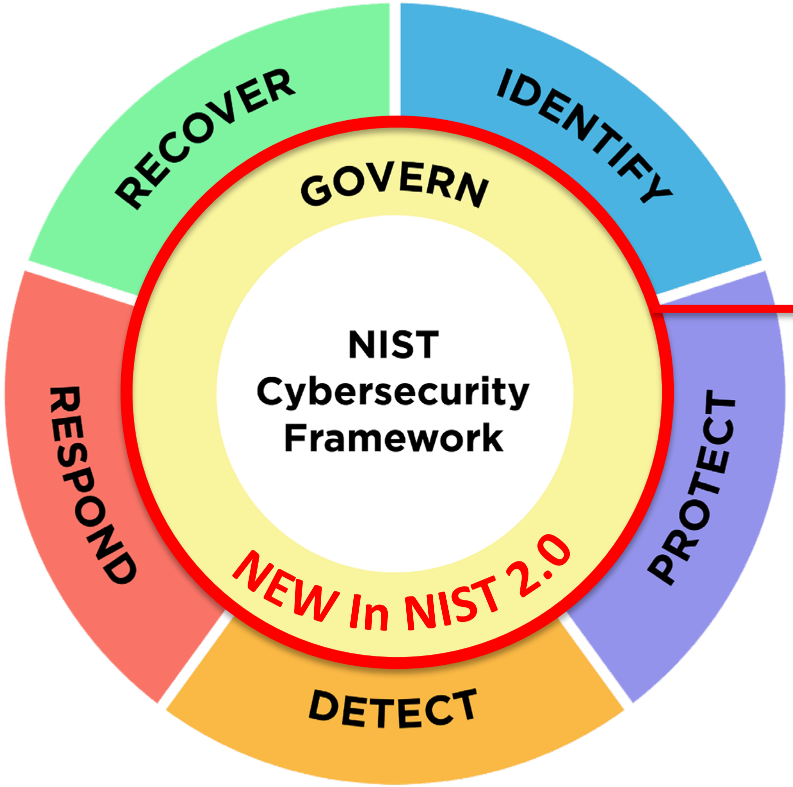
for us in one area…

NIST CSF 2.0 Now Requires Increased Governance

NIST 1.1
(April 16, 2018)



NIST 2.0
(August 8, 2023)



- GV.OC-01: Organization **Mission** is understood.
- GV.RM-02: **Risk appetite** and tolerance are determined and communicated
- GV.RM-06: A standardized method for **calculating and prioritizing cybersecurity risks** is established and communicated

PCI DSS v4.0 – Now Requires Increased Governance

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

- **Periodic Cadence Requirements**
  - Requirements where you can set your cadence (with justification)
  - Must risk analyze how that cadence reduces the risk reasonably
- **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
  - Two independent Appendixes with templates

The SEC Cybersecurity Rule Now Requires Increased Governance

- **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

- Requires accountability, transparency and communication to Management Team ***and*** Board of Directors for public companies regarding their cybersecurity risks and incidents.

What are these authorities requiring of us?

- **Governance is a Rising Requirement.**
  - NIST Cybersecurity Framework 2.0 (released August 2023)
  - PCI DSS 4.0 (effective April 2024)
  - SEC Cybersecurity Rule (effective September 2023)

- **What do they mean by Increased Governance?**
  - Governance is **evolving** and we are being asked to **evolve** our capabilities

The Evolution of Governance – People, Process, Technology

	Governance Topic	Governance 1.0 (Old Way)	Governance 2.0 (New Requirement)
People	Accountability	No individual Accountability	Clear accountability and ownership
	Executive Oversight	Informed in technical terms	Informed in business terms

The Evolution of Governance – People, Process, Technology

	Governance Topic	Governance 1.0 (Old Way)	Governance 2.0 (New Requirement)
People	Accountability	No individual Accountability	Clear accountability and ownership
	Executive Oversight	Informed in technical terms	Informed in business terms
Process	Risk Assessment Method	Maturity scores based on technical impacts (C/I/A)	Risk Analysis scores based on business impacts
	Risk Analysis Scope	Harm to self	Harm to self and others

The Evolution of Governance – People, Process, Technology

	Governance Topic	Governance 1.0 (Old Way)	Governance 2.0 (New Requirement)
People	Accountability	No individual Accountability	Clear accountability and ownership
	Executive Oversight	Informed in technical terms	Informed in business terms
Process	Risk Assessment Method	Maturity scores based on technical impacts (C/I/A)	Risk Analysis scores based on business impacts
	Risk Analysis Scope	Harm to self	Harm to self and others
Technology	Risk Register	Single-user / Spreadsheet	Multi-user / Database Application
	Executive Reporting	Manually created PPT with a lot of technical terms	Real-time Automated Governance reporting in business terms

Question:
What If We Don’t Have Governance 1.0 Fully Implemented Yet?

Answer:

- **This evolution does not need to be sequential.** If you don’t have Governance 1.0 in place, you can go straight to Governance 2.0!
- India and China did not have landline telephones fully implemented (1.0) and they did not sequentially go to installing landlines (1.0). Instead, they leapfrogged and went straight to mobile phones (2.0).
- You can and should do the same and implement Governance 2.0.

How Do We Implement a Governance 2.0 Program?

To implement a **Security Governance Program**:

- Identify the **elements** of a **Security Governance 2.0 Program**
- Then define the **capabilities** that would enable these Elements

Elements of a Governance 2.0 Program		Capabilities to Enable
Protect your organization	→	Legal defensibility
Align with business objectives	→	Clear line of acceptable risk
Risk management	→	Understanding your known risk
Measure performance	→	Roadmap that reduces risk to acceptable level
Management oversight and accountability	→	Executive reporting

How Today's Presentation Helps You Implement a Governance 2.0 Program.

Each of the 5 Sections of today's presentation covers a capability of a Governance 2.0 Program

Examples and free templates are provided at the end of this presentation.

Elements of a Governance 2.0 Program		Capabilities to Enable
Protect your organization	→	1 Legal defensibility
Align with business objectives	→	2 Clear line of acceptable risk
Risk management	→	3 Understanding your known risk
Measure performance	→	4 Roadmap reducing risk to acceptable leve
Management oversight and accountability	→	5 Executive reporting

The 5 Must-Have Capabilities for A Risk Governance Program

1. Ensuring your security program is **legally defensible.**
2. Defining a **clear line of acceptable risk** below which you can accept risks and above which you must remediate.
3. Understanding the **known risk** to your organization.
4. Providing a **roadmap** for your program that reduces risk to an acceptable level.
5. **Executive reporting to demonstrate your program is effective** to those inside and outside your organization.

(Gathered from Interviews of over 100 CISOs)

1

Ensuring your security program is **Legally Defensible**

Legal Defensibility is a Challenge

- **Have You Ever Heard of a Company Suing Themselves?**
  - Companies usually get sued by entities outside the organization (customers, regulators, investors, etc.)
- **Why do companies assess risk in terms of harm *only to themselves*? Why not assess risk of harm to entities *outside their organization*?**
- **Litigators and regulators want to see you assess the "harm to others" *not just yourself*.**
- **If your risk register *only* assesses the harm to *yourself* then you have documented your negligence.**

What does "Legally Defensible" Mean?
How Do You Strive for Legal Defensibility?

If your company enters into a lawsuit or breach, what are interested parties going to ask you?

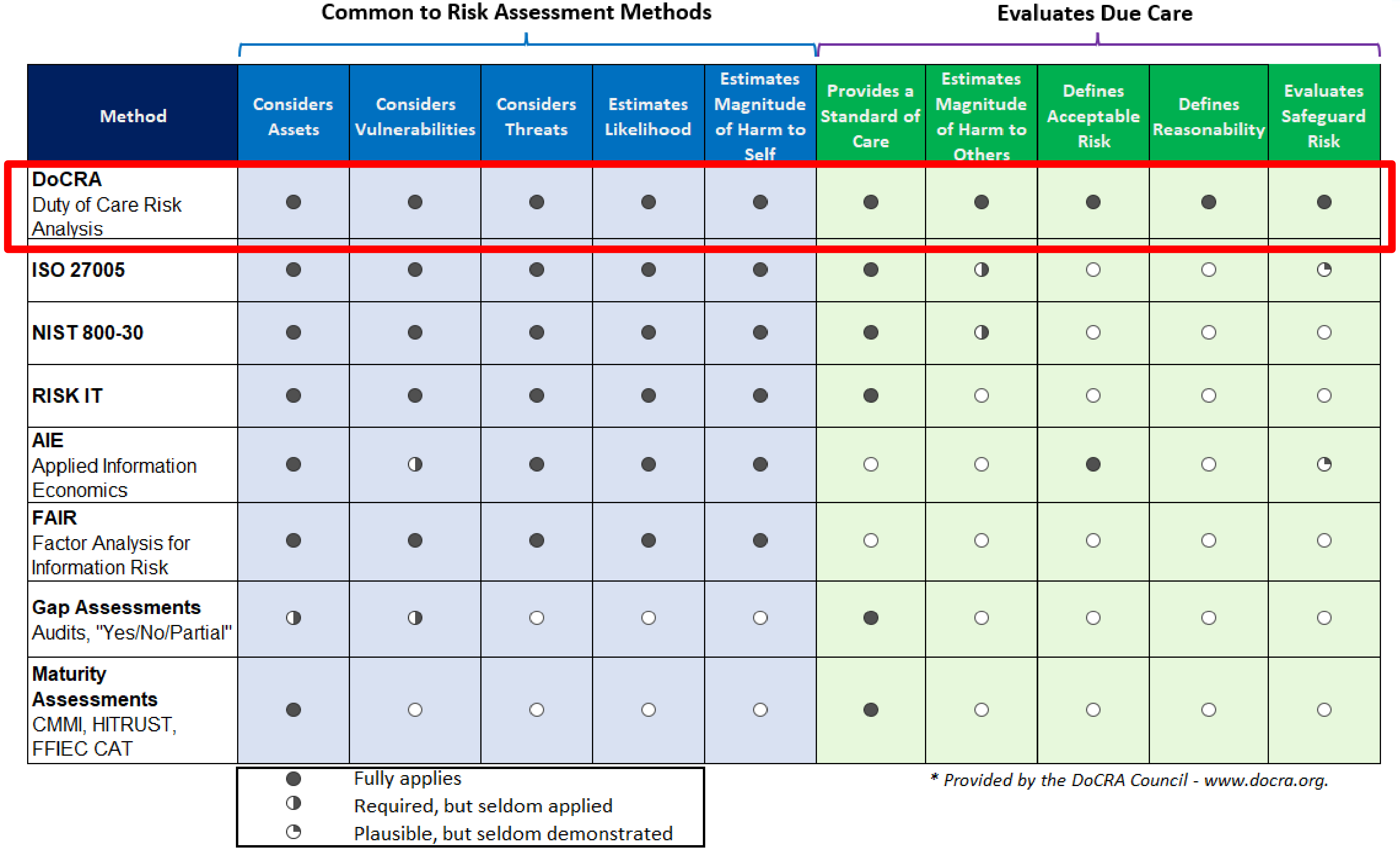
1. **Your Risk Register** – To ensure you are assessing the "risk to others"
   - Did you think through the ***likelihood*** of potential harm to you and others?
   - Did you think about the ***magnitude of that potential harm***?
   - Did you consider ***safeguards to reduce risk*** to an acceptable level? (*acceptable from the perspective of all interested parties*)
   - Do you have a definition of ***acceptable risk***?

2. **Consistent Risk Management** – Evidence that your *"risk register is not just a one-time exercise"*, but that you are performing consistent risk management and reducing your risks to an *"acceptable"* level over time.

Which Risk Assessment Methodologies Assess The Harm To Others?

Only Duty of Care Risk Analysis (**DoCRA)** assesses impacts **inside** *and* **outside** the organization to be treated equally.

This is *necessary for the* balancing test required by law.



	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.*

What is DoCRA?

- **Duty of Care** is foundational for assessing liability in our legal system.
- **Duty of Care Risk Analysis (DoCRA)** is the implementation of Duty of Care for Cybersecurity Risk Assessments.
- **Federal regulators and judges accept DoCRA** as demonstrating ***reasonableness*** even after a breach.
- **DoCRA is used by state Attorneys General** to describe what they mean by reasonable security.
- **The Legal System** values DoCRA.
- **Operating DoCRA demonstrates your program is legally defensible.**

DoCRA History

- 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
- **DoCRA** has had significant adoption (more than 10 states using DoCRA as their definition of reasonable security).
- **Over 140,000 downloads** of the CIS RAM 2.1 (DoCRA-Based Risk Assessment)

Gap Assessment and Maturity Assessments *do not allow you to prioritize your limited spend* in the absence of any risk analysis

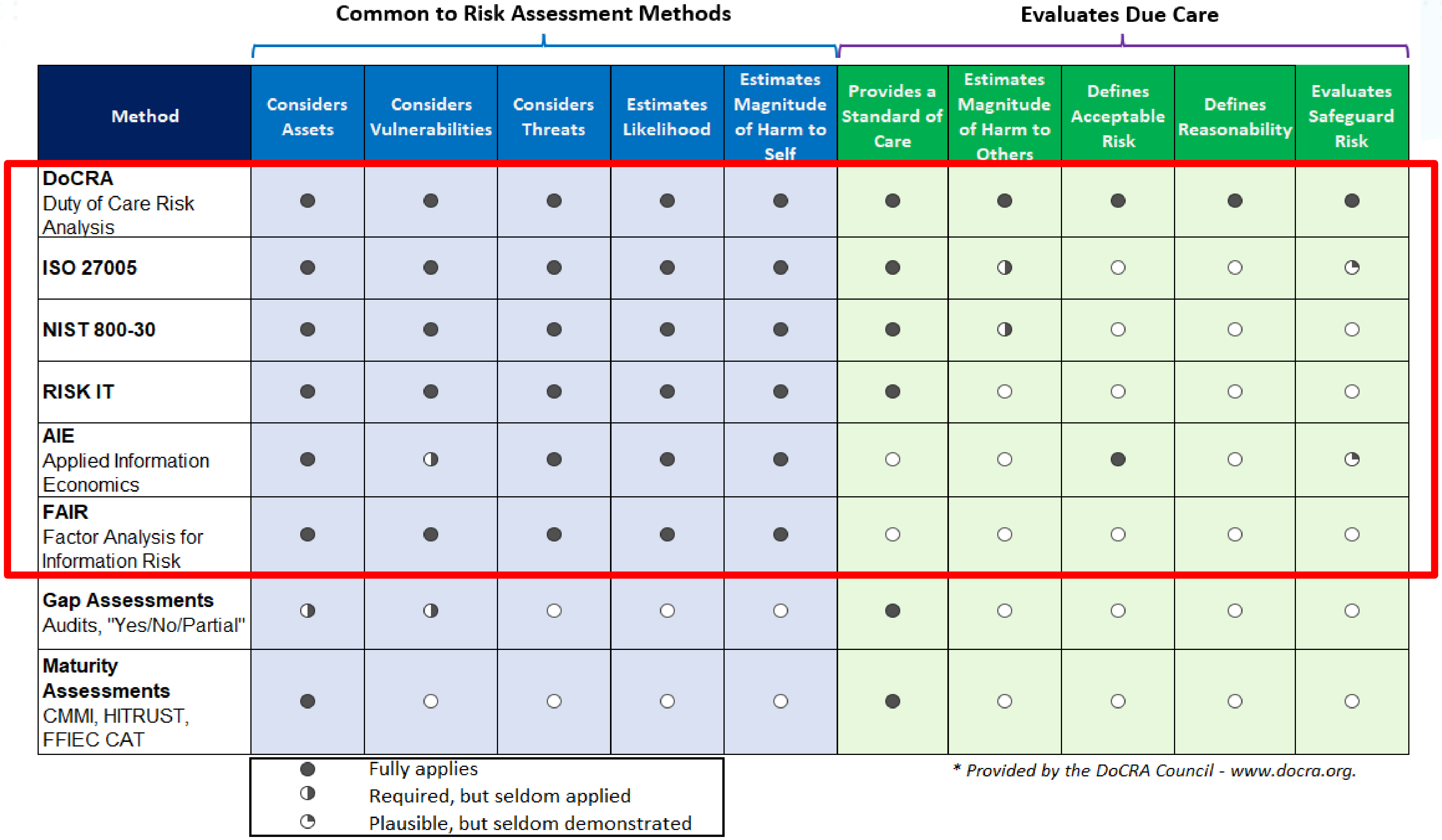
	Common to Risk Assessment Methods					Evaluates Due Care				
Method	**Considers Assets**	**Considers Vulnerabilities**	**Considers Threats**	**Estimates Likelihood**	**Estimates Magnitude of Harm to Self**	**Provides a Standard of Care**	**Estimates Magnitude of Harm to Others**	**Defines Acceptable 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.*

HALOCK®

True risk analysis will help you determine the impacts from lack 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.*

HALOCK®

Only DoCRA covers all the bases and analyzes impacts OUTSIDE the organization, enabling Legal Defensibility.

	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.*

SEC Ruling on Cybersecurity – July 26, 2023

U.S. SECURITIES AND
EXCHANGE COMMISSION

- **Requires accountability, transparency and communication** to management meam and Board of Directors for public companies regarding their cybersecurity risks and incidents.
- 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 of your company as their 3rd party business partner.
- **We will all need to comply with the new SEC Cybersecurity Rule in some shape or form.**

SEC Cybersecurity Rule – 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**.		• DoCRA based Calculated Acceptable Risk Definition (CARD) • halock.com • docra.org

SEC Cybersecurity Rule – 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

SEC Cybersecurity Rule – 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	- Executive Status (Slides 46 - 60) - reasonablerisk.com - docra.org

SEC Cybersecurity Rule – 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	• Executive Status (Slides 46 - 60) • reasonablerisk.com • docra.org
§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	• Executive Status (Slides 46 - 60) • reasonablerisk.com • docra.org

2

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

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

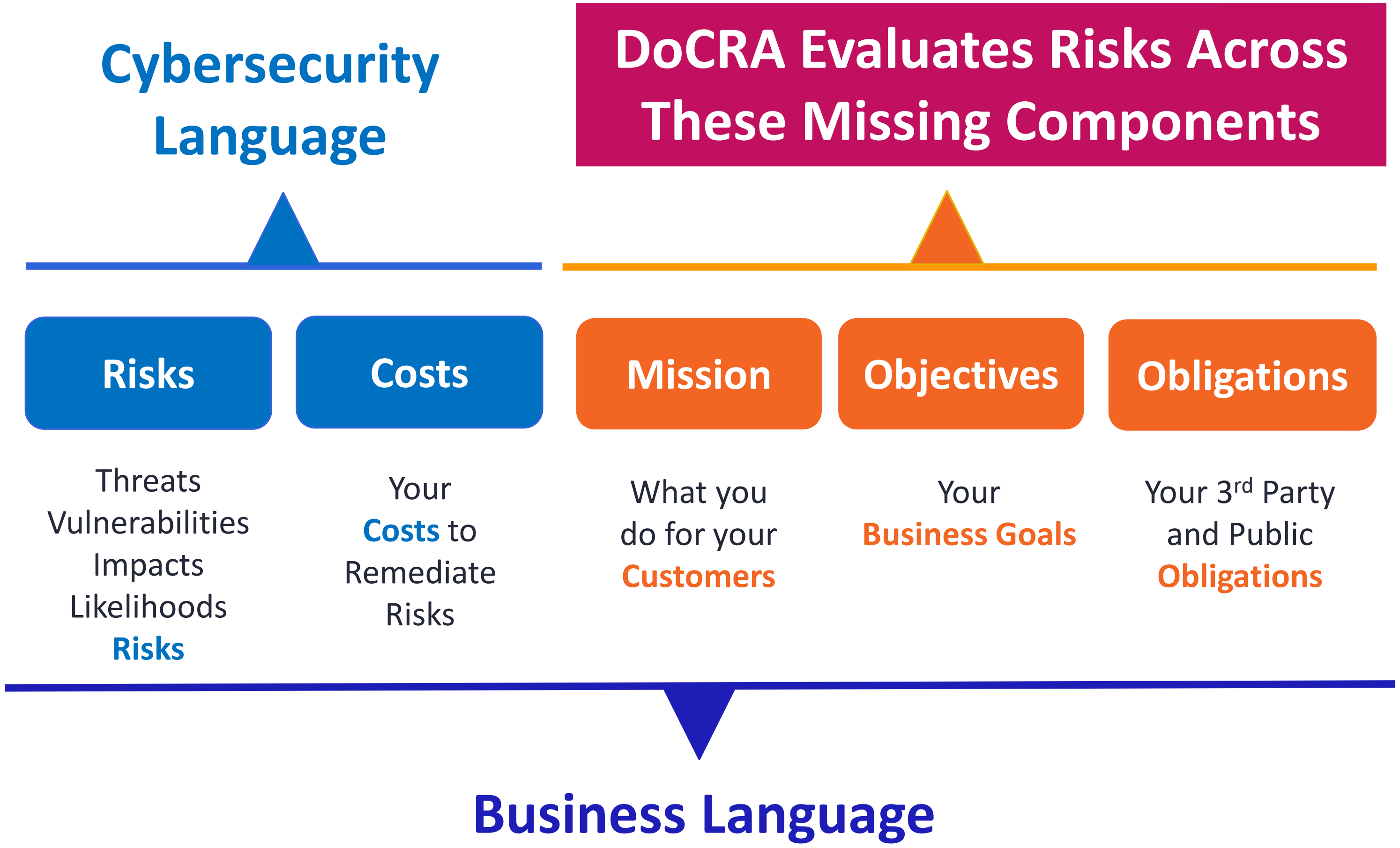
Your 3rd Party
and Public
Obligations

Business Language

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

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

Defining the Line of Acceptable Risk:
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.

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.

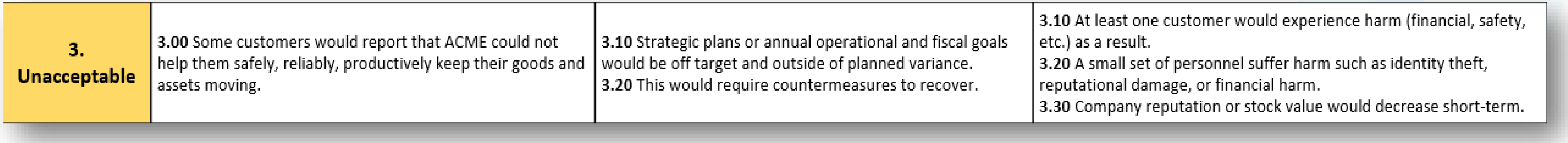
This is when you would disclose an incident.

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.

Defining “The Line” of Acceptable Risk

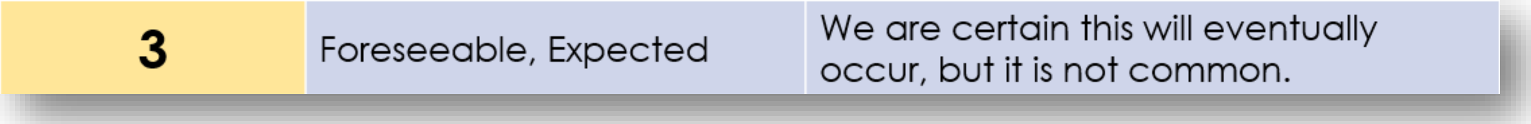
Impact – At this impact level this organization wishes to <u>remediate</u>



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.

IMPACT (3) x LIKELIHOOD (3) = **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**.

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 (3RD 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

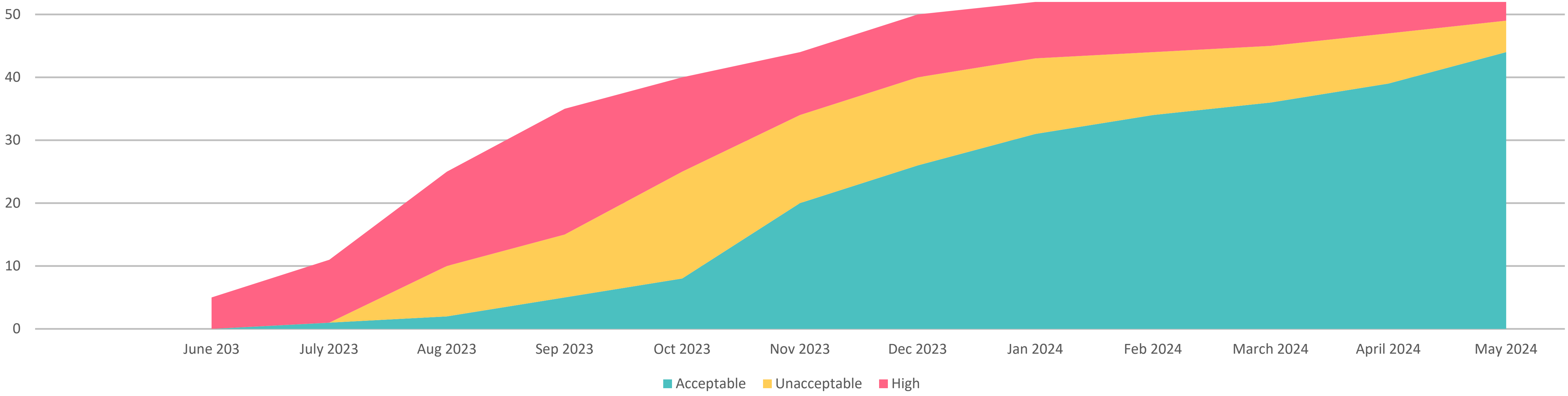
HALOCK®

3

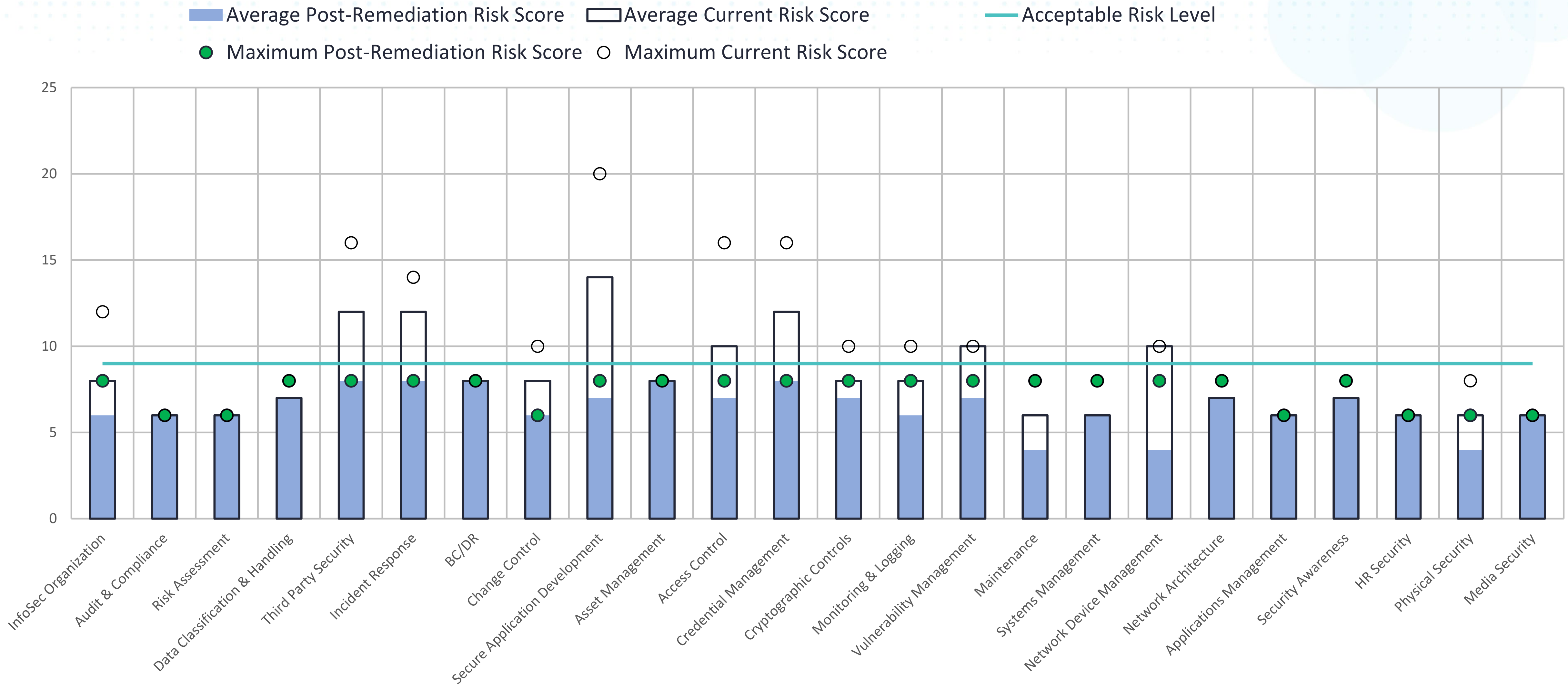
Understanding the known risk to your organization.

Big Picture: Program Progress Over Time

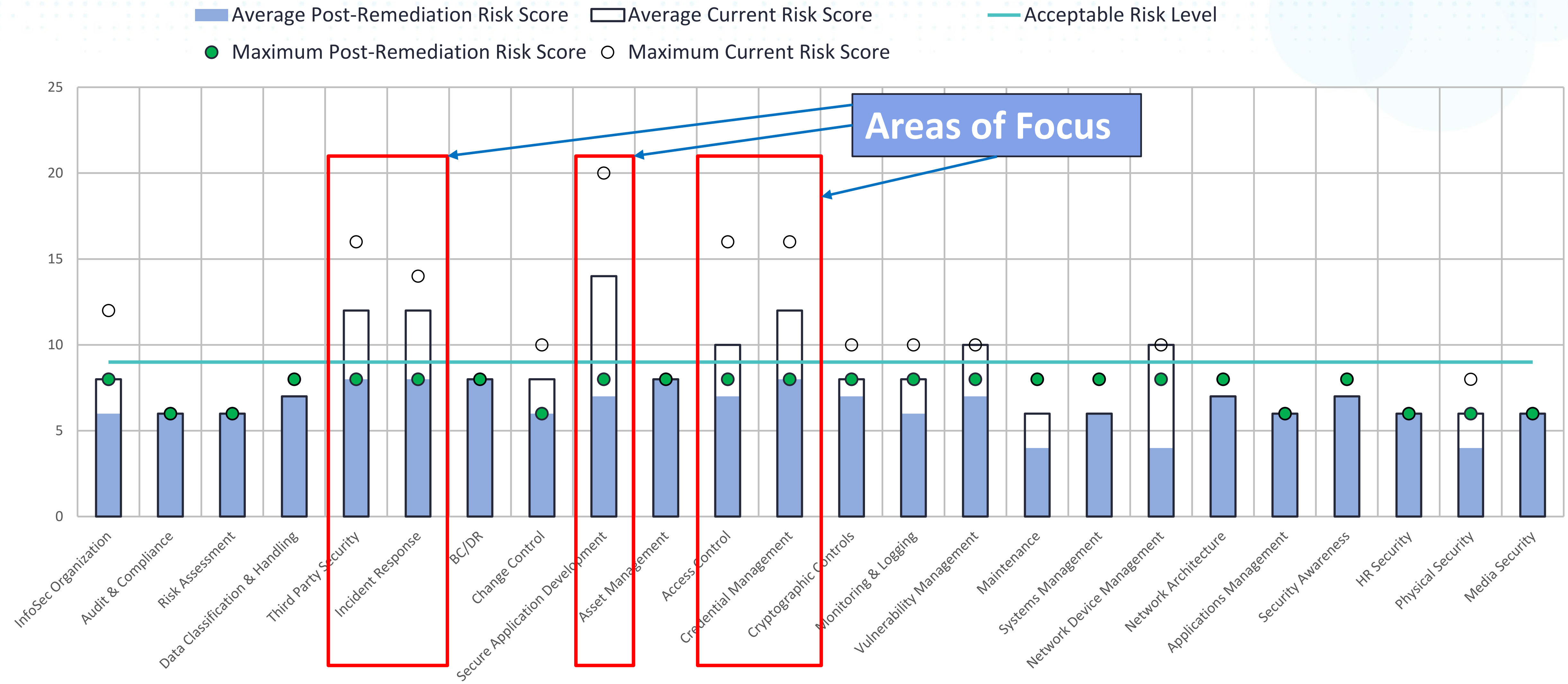
	Jun 2023	July 2023	Aug 2023	Sep 2023	Oct 2023	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	April 2024	May 2024
High	5	10	15	20	15	10	10	9	8	7	5	3
Unacceptable			8	10	17	14	14	12	10	9	8	5
Acceptable		1	2	5	8	20	26	31	34	36	39	44
Total	**5**	**11**	**25**	**35**	**40**	**44**	**50**	**52**	**52**	**52**	**52**	**52**



Risk Score by Security Program



Risk Score by Security Program



HALOCK®

4

Providing a Roadmap for your program that reduces risk to an acceptable level.

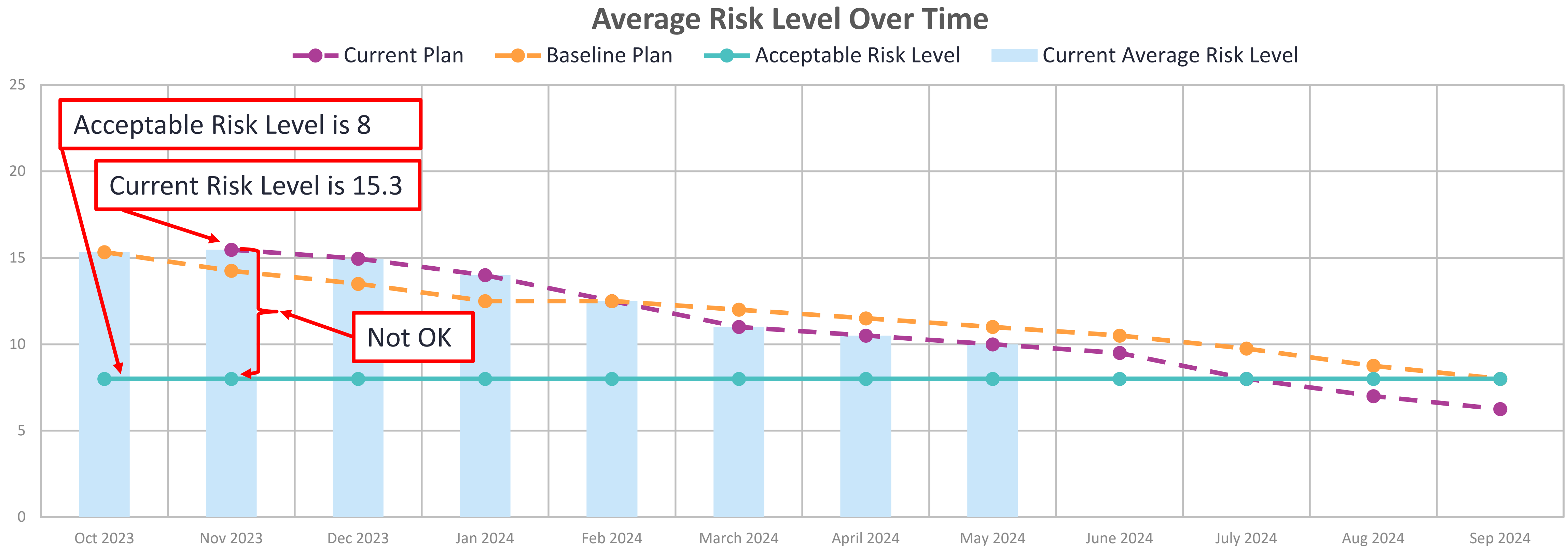
Why is Providing a Roadmap so Difficult?

- 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?"***

Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was 15.3 last November **(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

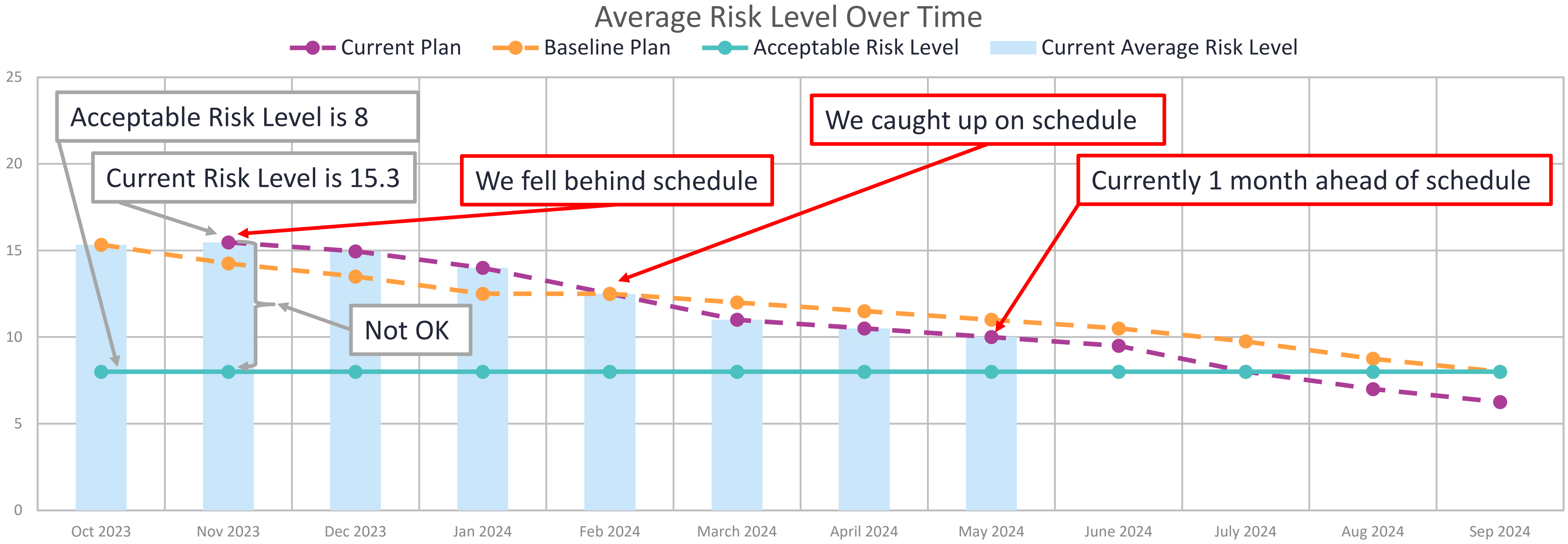
Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was 15.3 last November **(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 November but have caught up in February and we are currently ***1 month ahead of schedule***.



Acceptable Risk Level is 8

Current Risk Level is 15.3

We fell behind schedule

We caught up on schedule

Currently 1 month ahead of schedule

Not OK

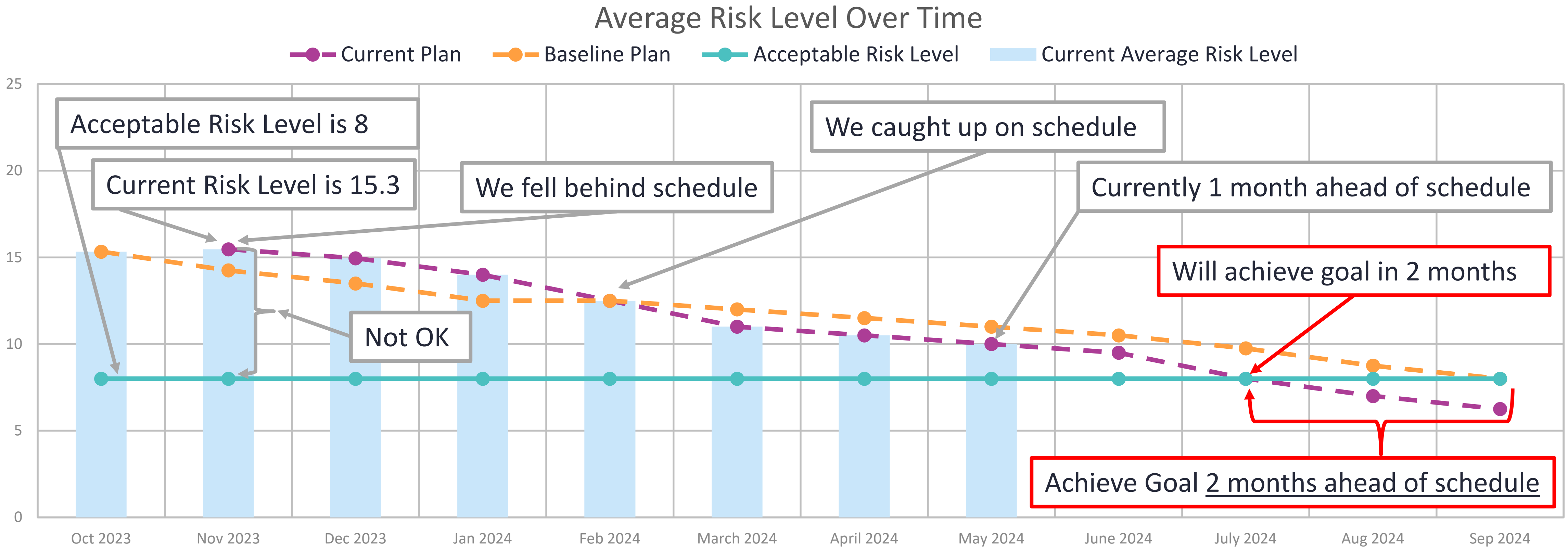
Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was 15.3 last November **(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 November but have caught up in February and we are currently 1 month ahead of schedule.
- We **will achieve our goal in 2 months**, in July, 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.



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

5

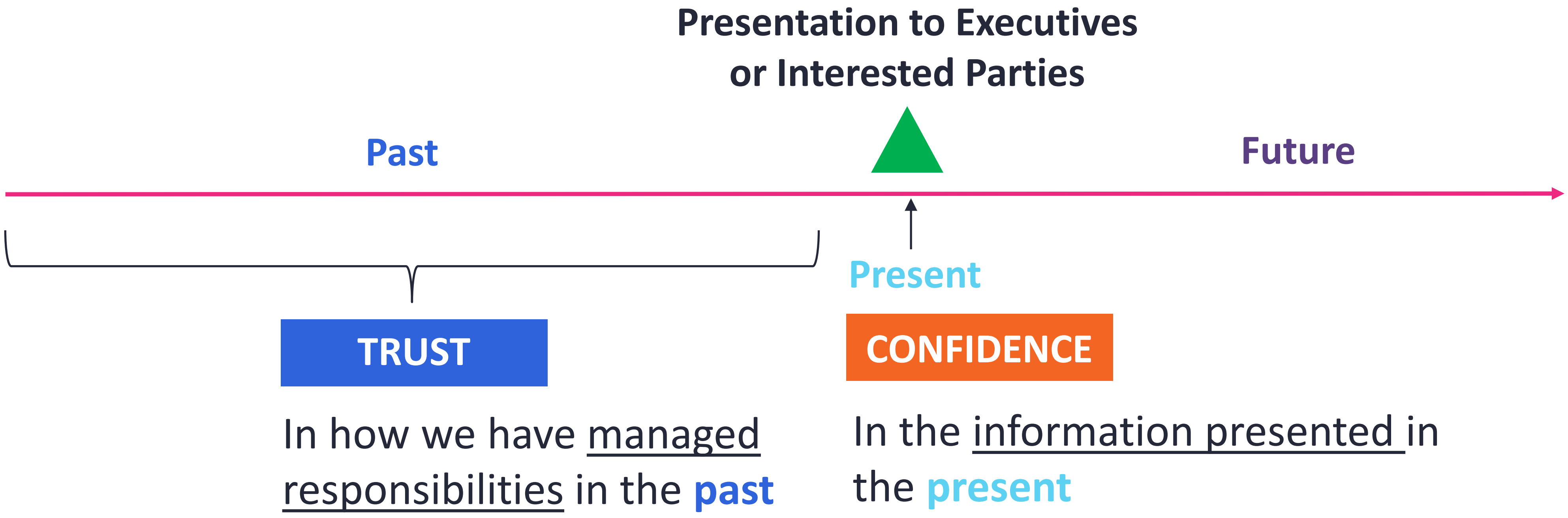
Executive Reporting to Demonstrate Your Program is Effective to those inside and outside your organization.

The Theory Behind Executive Reporting

Two Factors to Consider When Presenting to Executives

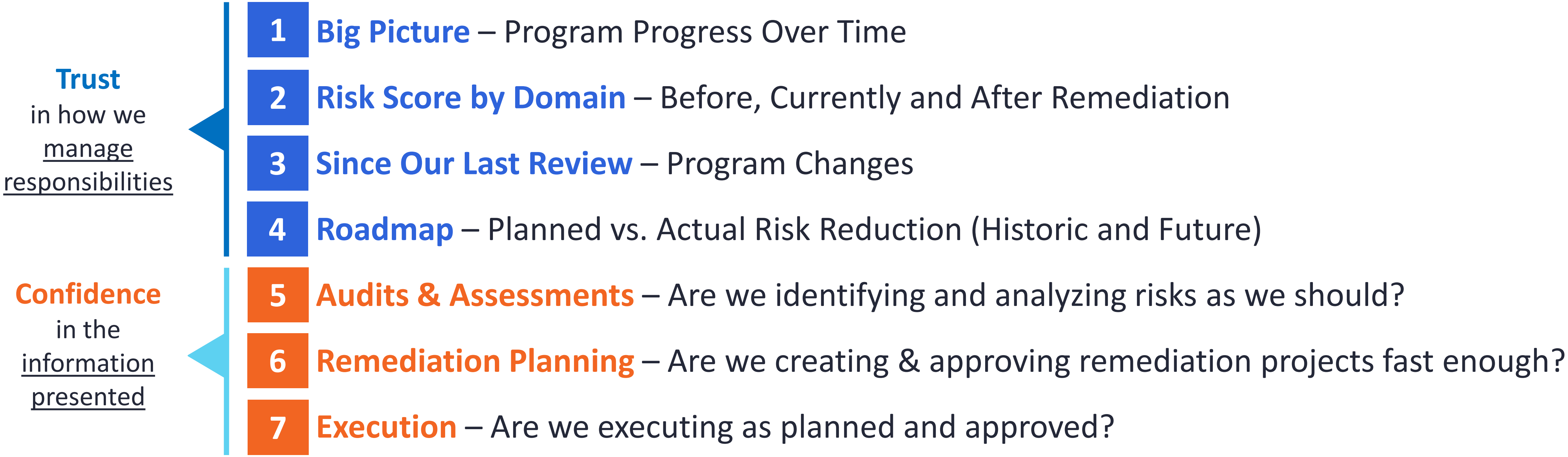
TRUST In how we have managed responsibilities in the **past**

CONFIDENCE In the information presented in the **present**



Presentation to Executives
or Interested Parties
Past
Future
Present
TRUST
In how we have managed responsibilities in the past
CONFIDENCE
In the information presented in the present

Proven Executive Status Approach to Establishing Trust and Enabling Confidence



Trust in how we manage responsibilities

1 **Big Picture** – Program Progress Over Time

2 **Risk Score by Domain** – Before, Currently and After Remediation

3 **Since Our Last Review** – Program Changes

4 **Roadmap** – Planned vs. Actual Risk Reduction (Historic and Future)

Confidence in the information presented

5 **Audits & Assessments** – Are we identifying and analyzing risks as we should?

6 **Remediation Planning** – Are we creating & approving remediation projects fast enough?

7 **Execution** – Are we executing as planned and approved?

Executive Reporting for a Turnkey Governance Program with 5 Must-Have Governance Capabilities

Reasonable Risk

Executive Status

Gauging Your Risk.

Scope: Enterprise

Last Review Meeting: January 2024

Date of Export: April 30, 2024

Agenda

Attendance

Objectives for this Meeting

Program Overview

- **Big Picture:** Program Progress Over Time
- **Risk Score** by Security Program
- **Since Our Last Review:** Program Changes
- **Roadmap:** Planned vs Actual Risk Reduction

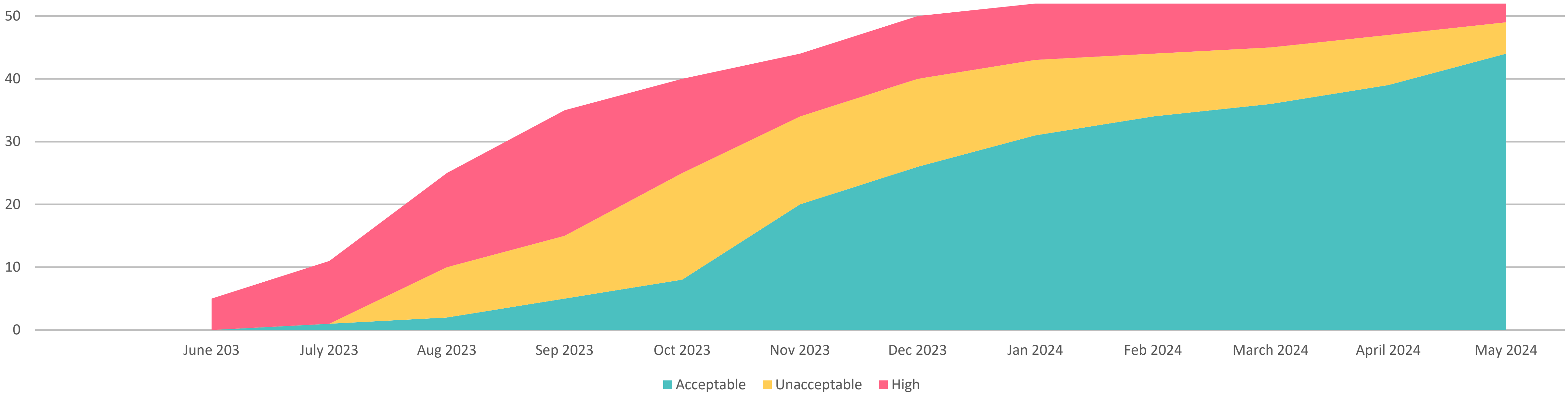
Program Status (PDCA)

- Plan
  - **Assessments & Audit:** Are we identifying and analyzing risks as we should?
  - **Remediation Planning:** Are we creating and approving remediation projects fast enough?
- Do
  - **Execution:** Are we executing as planned and approved?
- Check
  - **Program Status:** Is the risk program effective?
  - **Items Since We Last Met:** Follow up on past action items
- Act
  - **Continuous Improvement:** What other continuous improvement activities should we consider?

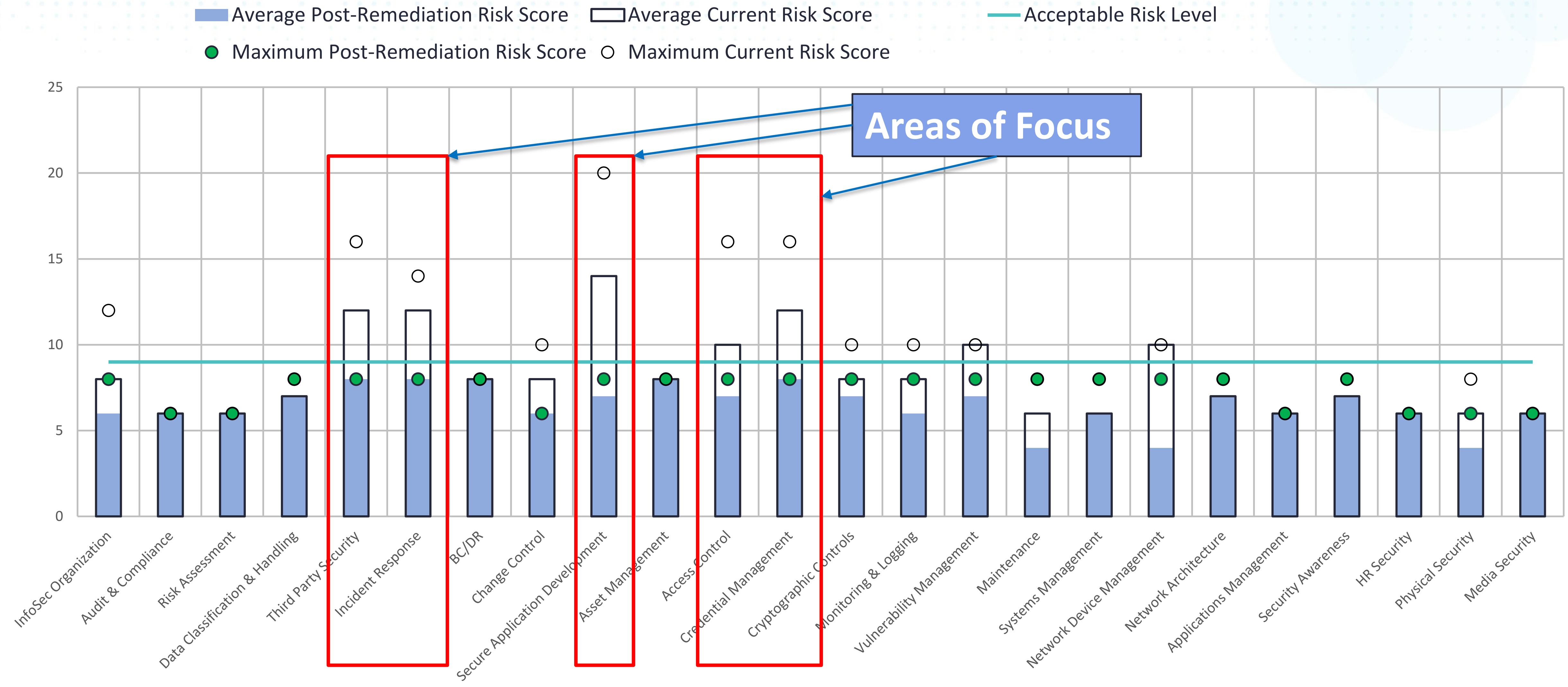
Q&A

Big Picture: Program Progress Over Time

	Jun 2023	July 2023	Aug 2023	Sep 2023	Oct 2023	Nov 2023	Dec 2023	Jan 2024	Feb 2024	Mar 2024	April 2024	May 2024
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**



Risk Score by Security Program



Areas of Focus

Since Our Last Review: Program Changes

Last Time We Met on: 02/07/2024
Information below is as of: 05/07/2024

New Risks Identified	3 new risks identified

Risks	Acceptable	Unacceptable	High
Risk Count | Prior to Last Review	**31**	**12**	**9**
New Risks Identified Since Last Review	**0**	**2**	**1**
Risk Count | Current	48	**5**	**2**

What contributed to risks since last review:

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

Comments	The risks from the upcoming merger with ACME will be included in the next review.

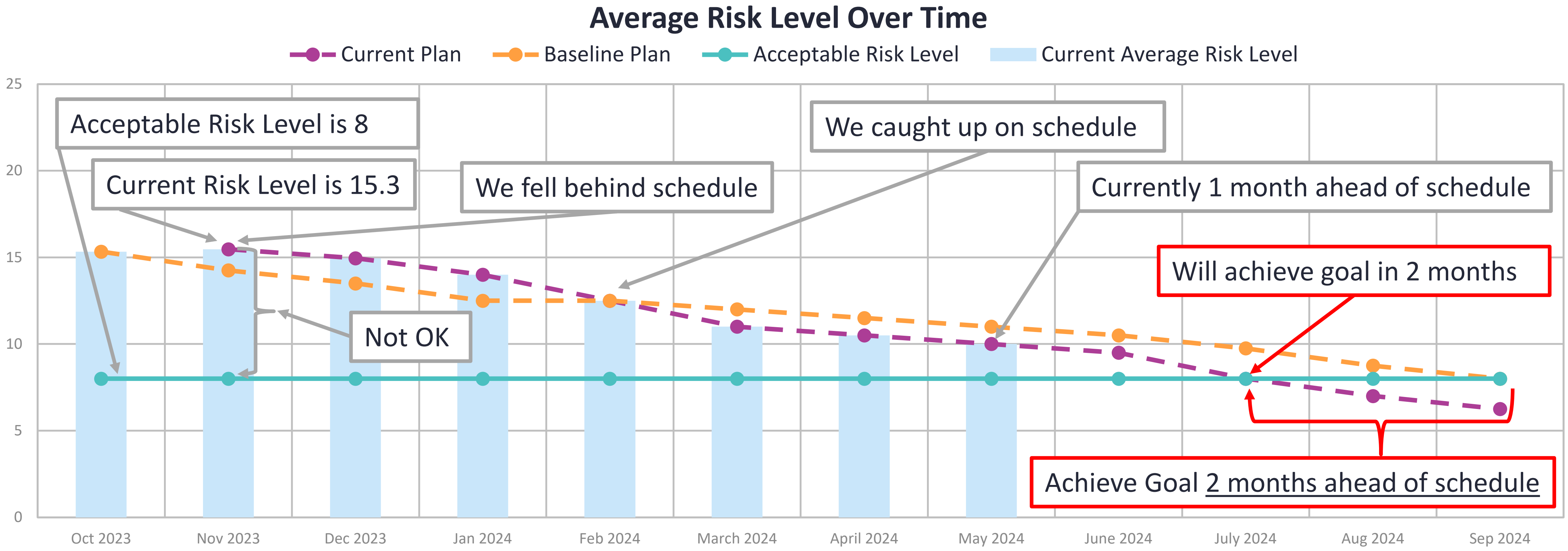
Roadmap: Planned vs. Actual Risk Reduction

Are we OK?

- Our Current Average Risk level was 15.3 last November **(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 November but have caught up in February and we are currently 1 month ahead of schedule.
- We **will achieve our goal in 2 months**, in July, 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.



Acceptable Risk Level is 8

Current Risk 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

Agenda

Attendance

Objectives for this Meeting

Program Overview

- **Big Picture:** Program Progress Over Time
- **Risk Score** by Security Program
- **Since Our Last Review:** Program Changes
- **Roadmap:** Planned vs Actual Risk Reduction

Program Status (PDCA) ✓

- Plan
  - **Assessments & Audit:** Are we identifying and analyzing risks as we should?
  - **Remediation Planning:** Are we creating and approving remediation projects fast enough?
- Do
  - **Execution:** Are we executing as planned and approved?
- Check
  - **Program Status:** Is the risk program effective?
  - **Items Since We Last Met:** Follow up on past action items
- Act
  - **Continuous Improvement:** What other continuous improvement activities should we consider?

Q&A

Audits & Assessments:
Are We Identifying and Analyzing Risk As We Should?

Please fill out the gray columns for each line.

Assessment Type	Assessment Title	Assessment Domain	Planned Completion	+/- Planned Completion	Date of Last Assessment	Status	Reason for Status	Action Plan	Approval Required?
Risk Assessment	Annual 3rd Party Risk Assessment	Enterprise IT	06/07/2024	30 Days Past	05/07/2023	Issue	Late due to contract issues		No
Penetration Test	Quarterly Pen Test	Enterprise	03/07/2024	60 Day Past	04/10/2023	Issue	Late due to unavailability of Infrastructure Team	We are requesting your help to perform an arm-in-arm “friendly escalation” to the Management of Infrastructure Team, to request that they either make this a higher priority or bring on additional personnel to assist	Yes
Vulnerability Scan	Monthly External Vulnerability Scan	Publicly accessible web applications	08/08/2024	91 Days Until		Good	On Schedule		
Audit - External	SOC 2 Audit	Enterprise	09/05/2024	30 Days Past	08/05/2023	Issue	We are starting 4 weeks late due to vendor recently being acquired by another company.	A meeting with Vendor has been scheduled. If we don’t receive commitment that they will adhere to our new schedule, we will escalate within their organization or select another vendor	Yes
Vulnerability Scan	Bi-Annual Panorays Scan	Enterprise	10/05/2024	120 Days Until		Good	On Schedule		No

Remediation Planning:

Are We Creating and Approving Remediation Plans Fast Enough?

Please fill out the gray columns for each line.

Risk Severity & Statistics	Total	Reason for Delay	Action Plan	Approval Required?
High Risks				
Count of risk outside planning horizon	5 of 5	Our infrastructure team has been swamped and understaffed . They were not able to meet with our team at all through Q1 to complete the remediation planning, required for project approval	We are requesting your assistance for a friendly escalation with the Infrastructure Group Management to request that they either make this a higher priority or bring on additional personnel to assist	Yes
Average age of risks beyond planning horizon	99			
Unacceptable Risks				
Count of risk outside planning horizon	1 of 1	NA	NA	NA
Average age of risks beyond planning horizon	20			

Risk Rating	Remediation Planning Horizon
(Time from risk identification to project approval)	
High	45 days
Unacceptable	90 days

Execution:
Are We Executing as Planned and Approved?

Please fill out the gray columns for each line.

Remediation Project	Project Owner	Est. Start Date	Approved Completion Date	Est. Completion Date	+/- Approved Completion	Schedule	Scope	Resources	Count of Unacceptable Risks	Reason for Status	Action Plan	Approval Required?
Third Party Risk Management	John Doe	04/01/2023	4/01/2024	06/03/2024	**62 Days Past**	At Risk	At Risk	Good	4	We have identified several third-party vendors not being assessed	We are creating a list of additional third-party vendors and will provide status by 06/01/2024 if additional resources are needed	No
Data Management Program	Bart Foley	05/01/2023	07/01/2024	10/01/2024	**90 Days Past**	At Risk	Good	Good	7	Infrastructure Team was not available	Addressed in previous slide, request resources through a friendly escalation to their management	Yes
Removable Media Management	John Doe	01/01/2024	07/01/2024	07/01/2024	**On Schedule**	Good	Good	Good	1			
Access Management Program	Sally Smith	01/01/2024	9/30/2024	9/30/2024	**On Schedule**	Good	Good	Issue	1	Several resources out on maternity and paternity leave	We are requesting 2FTE employee resources to be re-assigned to our team or permission to hire 2 FTE resources	Yes
Multifactor Authentication	Barbara Anderson	04/01/2024	12/31/2024	12/31/2024	**On Schedule**	Good	Good	Good	2			No
Incident Response Program	Joe Jones	07/01/2024	11/01/2024	11/01/2024	**On Schedule**	Good	Good	Good	3			No

Applying It

Next Steps…

These Decisions Have Already Been Made

- **NIST** has decided to **require a Governance Program**
- **PCI** has decided to **require a Governance Program**
- **SEC** has decided to **require a Governance Program**
- If you do not implement a Governance Program, you are choosing to ignore the rising requirements for a Governance Program

Why should you move to Governance 2.0?

- Our industry is requiring it (NIST, PCI, SEC, etc.) – Compliance
- You can properly prioritize – Better for your company
- You can be proactive vs. reactive and not get derailed everytime leadership has something else for you – Better for you and your team

Here is the Choice In Front Of You....

The choice in front of you is not whether to move to Governance 2.0,
it has been made clear by authoritative bodies that this is a requirement.

The Choice is HOW do you move to Governance 2.0?

- Do you want to continue with implementing **Governance 1.0**?
- Or jump straight to **Governance 2.0**?

Jumping To Governance 2.0 Now

- **This Week (EDUCATE) – Educate Yourself on Leading Edge Governance Capabilities**
  - **Download a Free Copy of All Tools, Templates and Executive Reporting Samples** in this Presentation
    - www.halock.com/rsa2024
  - **Consider a hiring a consulting organization** to speed up your education

- **3 Months (IMPLEMENT) – Implement a Governance Program**
  - **Complete a Free DoCRA Risk Assessment**:
    - https://www.cisecurity.org/insights/white-papers/cis-ram-risk-assessment-method
  - **Implement and populate** the Executive Status (slides 52 - 61)
  - **Consider engaging a consulting company** to speed up your Implementation
  - **Research Turnkey Governance Software Application(s)** to operationalize your Implementation
    - www.reasonablerisk.com

- **6 months (OPERATE) – Operate a Governance Program**
  - **Populate the Program** Progress Over Time slide to get credit for the work you have completed (slide 54)
  - **Populate the Roadmap** to Demonstrate Actual vs. Planned Risk Reduction (slide 57)
  - **Implement a Turnkey Governance Software Application** to automate and streamline your operations
    - www.reasonablerisk.com

Thank you

Jim Mirochnik

MBA, PMP, ISO 27001 Auditor

CEO, Senior Partner

HALOCK Security Labs

jmirochnik@halock.com

847.221.0205