HALOCK®

A Proven Methodology to Secure the Budget You Need

Jim Mirochnik
CEO, Senior Partner
HALOCK Security Labs
halock.com

What we are going to cover today

1. **The Problem** – Why Securing Budget is Difficult
2. **The Solution** – Documented Trust & Confidence
3. **Real Life Examples** – How it Works
4. **Applying It** – Immediately, 3 months, 6 months

HALOCK

1. The Problem

Why Securing Budget is Difficult

HALOCK

Your Budget Situation

Raise Your Hand if …

You have 100% of the *budget* you truly need to get your job done right

You have 100% of the *staff* you truly need to get your job done right

Today we will talk about:

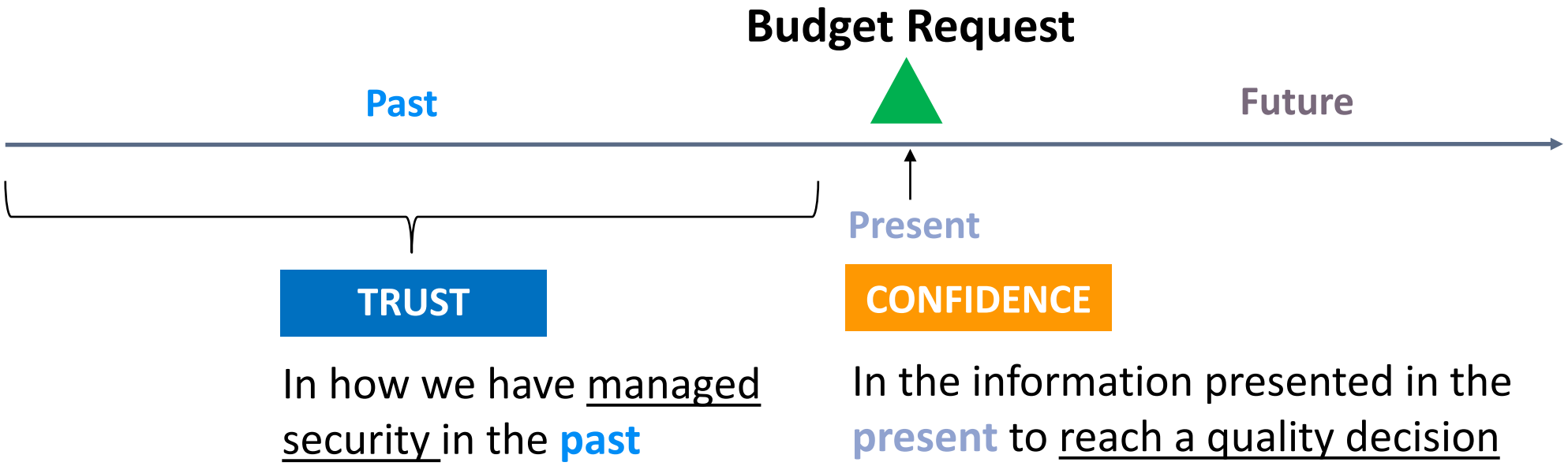
- Why does this problem occur?
- How does this problem manifest itself?
- How ***you can all raise your hand*** *the next time you are asked if* ***you have 100% of the budget or staff you need.***

HALOCK®

Two Parts that Factor into Securing a Budget

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

CONFIDENCE In the information presented in the **present** to reach a quality decision



HALOCK®

Establishing Trust and Confidence

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, are InfoSec 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?

HALOCK®

Establishing Trust and Confidence

We surveyed 140 **CEOs and CFOs**[1]. Of the C-level respondents:

- **65%** DO NOT understand **when** it is "okay" to accept a risk
- **85%** DO NOT understand **what** InfoSec 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

C-Level executives *do not* have the information they need to approve budgets!

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

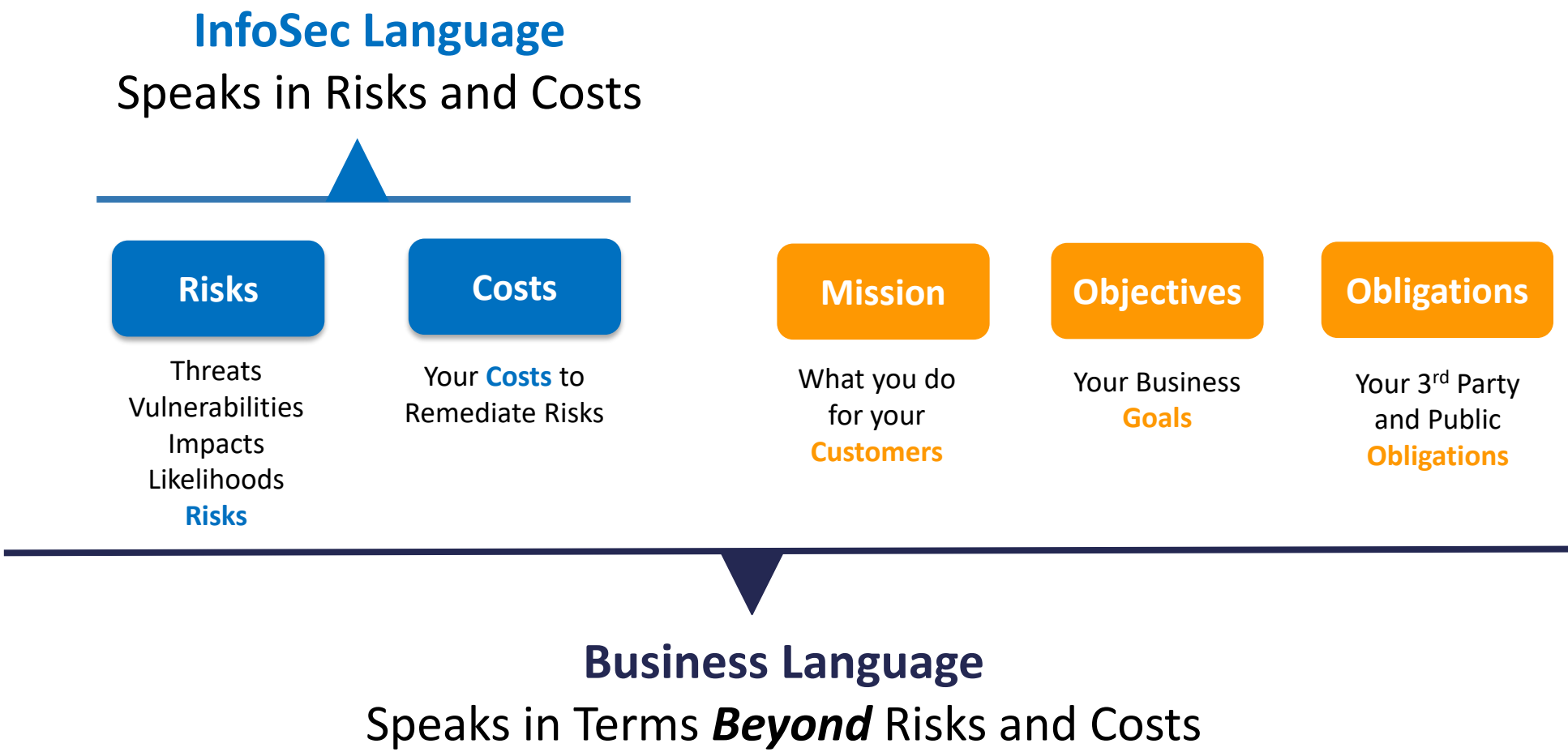
HALOCK®

What Happens When C-Level Does Not Have the Information They Need to Approve?

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

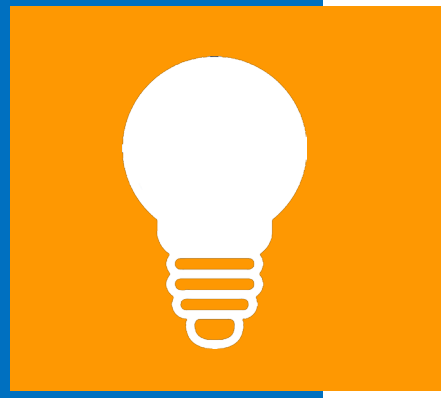
HALOCK®

How Are InfoSec & C-Level Speaking Different Languages?



When Budget Approvers Don'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!**



2. The Solution

Documented Trust & Confidence

HALOCK

SOLUTION: Documented Trust & Confidence

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

DoCRA is based on the legal concept of "**Due Care**." This means, we must protect others from the harm we may cause them by implementing controls that are not more burdensome to us than the risk of the harm to others.

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

HALOCK®

SOLUTION: Documented Trust & Confidence

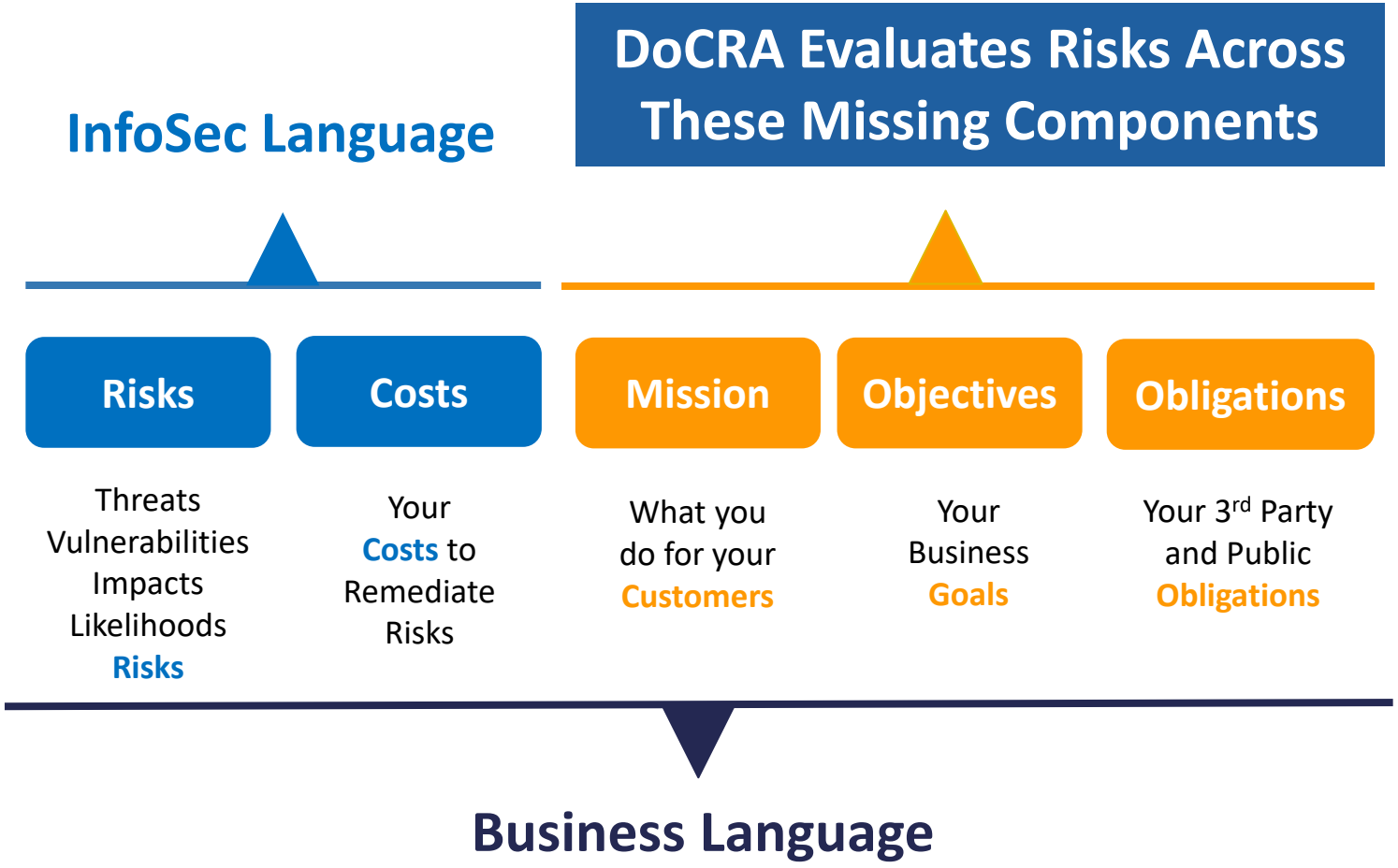
The **DoCRA** Risk Assessment methodology answers the four questions allowing C-Level need to make informed budgeting decisions:

1. **A clear "line" / risk acceptance criteria** to evaluate whether to "accept" the risk or "invest" in mitigation
2. **Common language** between InfoSec and business / regulators / legal system
3. **Legally defensible** position by defining what is legally "reasonable"
4. **Risk Management process** to know you are spending the right amount

HALOCK®

How does DoCRA create a Common Language?

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



About DoCRA

- The **Duty of Care Risk Analysis (DoCRA)** methodology was launched as a standard in early 2018
- **DoCRA** is a non-profit organization
- **DoCRA** donated a version of its Risk Assessment Methodology to CIS® (Center for Internet Security)
- CIS published this Risk Assessment Method 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®

About DoCRA

- **DoCRA** has had **significant adoption**
- Over 50,000 downloads of the CIS RAM 1.0 and over 10,000 downloads of CIS RAM 2.1 Methodology
- Used 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)

HALOCK®

Example: Calculated Acceptable Risk Definition (CARD)

Impact	Mission | What Do You Do For Your Customers	Objectives | Your Business Goals	Obligations | Your Public Duty
Definition	Provide information to help customers achieve greatness.	Operate profitably.	Customers must not be harmed by compromised information.
1. Negligible	**1.00** - Customers continue to access helpful information, and outcomes are on track.	**1.00** - Profits are on target.	**1.00** - Customers do not experience loss of service or protection.
2. Low	**2.00** - Some Customers may not get all the information they need as they request it.	**2.00** - Profits are off target but are within planned variance.	**2.00** - Customers may be concerned, but not harmed.
3. Medium	**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.	**3.00** - Some Customers may be harmed financially or reputationally after compromise of information or services.
4. High	**4.00** - Many Customers consistently cannot access beneficial information.	**4.00** - Profits are off planned variance and may take more than a fiscal year to recover.	**4.00** - Many Customers may be harmed financially or reputationally.
5. Catastrophic	**5.00** - We can no longer provide helpful information to Customers.	**5.00** - The organization cannot operate profitably.	**5.00** - Some Customers may be harmed financially, reputationally, or physically.

HALOCK®

Does the Narrative and How We Provide Information to Budget Approvers Really Matter?

- Do you know what the movies Rocky, Star Wars, The Matrix, Spider Man, The Lion King, Lord of the Rings, Harry Potter, and countless other hits have in common?

- **These Blockbuster Movies** follow a **proven narrative** called "**The Hero's Journey**"
- **Your Budget Requests** should also follow a **proven narrative,** that provides decision makers the information they need to make a quality decision.

HALOCK®

Proven Budget Request Narrative Documenting Trust and Enabling Confidence

Trust in how we manage security

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

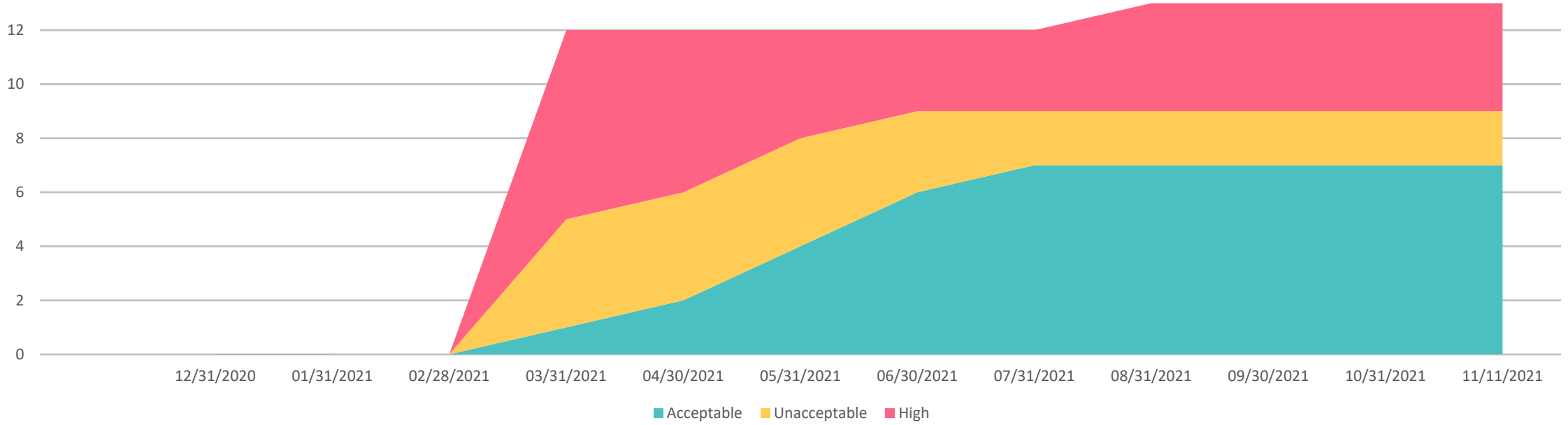
Confidence in the information presented to reach a quality decision

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)

HALOCK®

1. **Big Picture** - Program Progress Over Time

	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021
High				7	6	4	3	3	4	4	4	4
Unacceptable				4	4	4	3	2	2	2	2	2
Acceptable				1	2	4	6	7	7	7	7	7
Total				**12**	**12**	**12**	**12**	**12**	**13**	**13**	**13**	**13**



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	0	0
Risk Count | Current	7	2	4

What contributed to risks since last review:

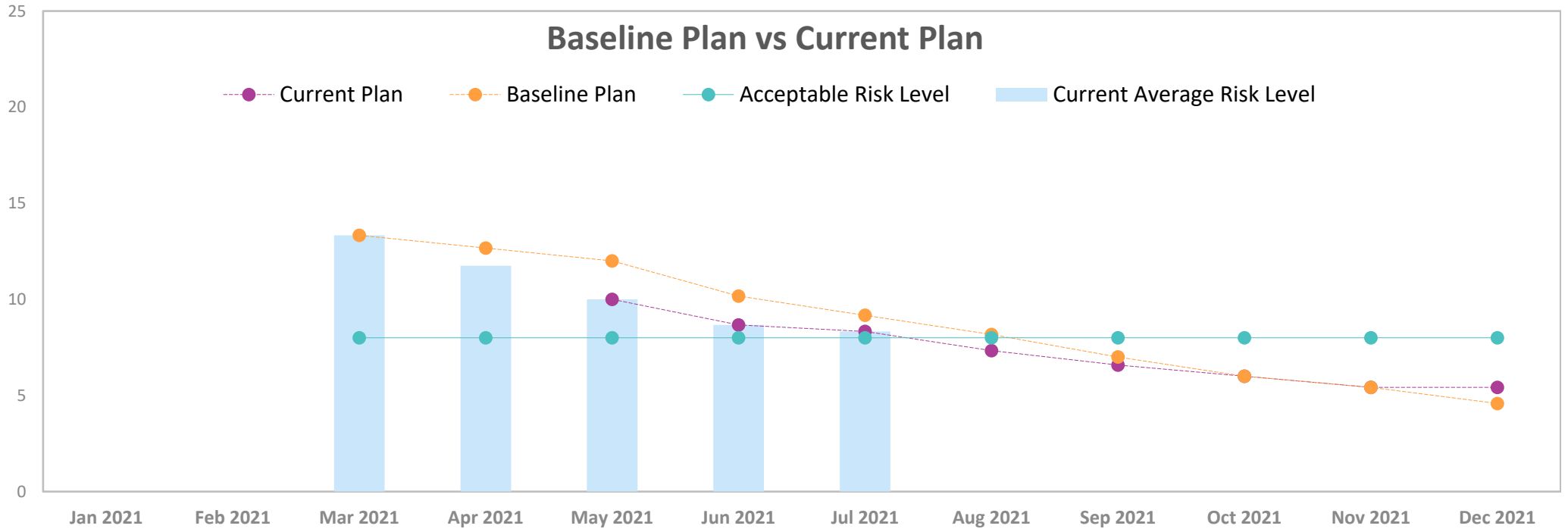
- [ ] Customer Requirements
- [x] Incident
- [ ] Mergers & acquisitions
- [ ] New Technology
- [ ] Other Assessment
- [x] Penetration Test
- [ ] Regulatory Change
- [ ] Scope Increase
- [ ] Threat Landscape
- [ ] Zero Day
- [ ] Other (see below)

Comments	We completed our yearly Pen Test and also had an incident in Finance relating to Business Email Compromise

HALOCK®

3. **Roadmap** – Planned vs. Actual Risk Level

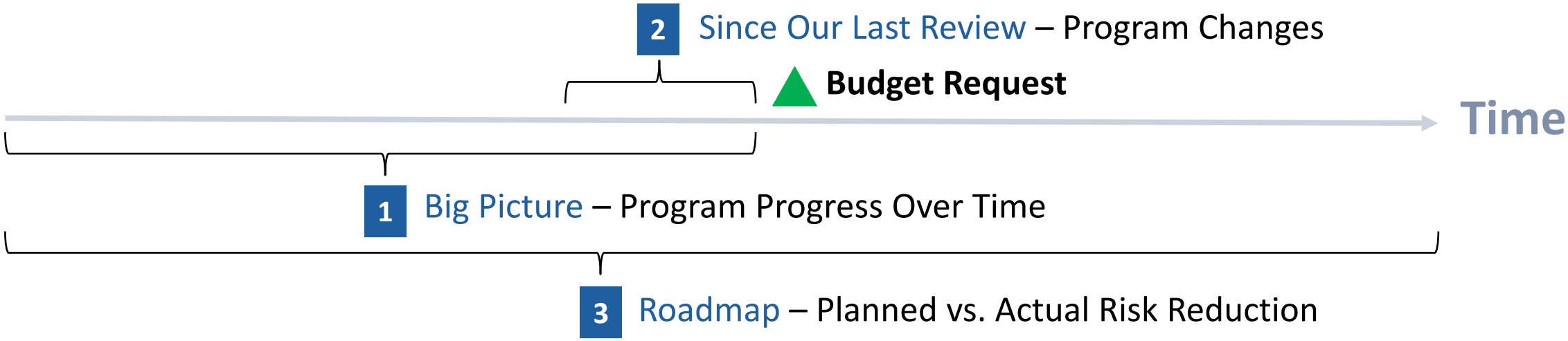
- We stayed ahead of schedule for many months and now below the acceptable risk level
- The decisions you made when you approved resources in March, *enabled the organization to deliver on lowering risks* through July



Proven Budget Request Narrative: How We Have **Established Trust**

Trust:
In how we manage security

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



HALOCK®

Proven Budget Request Narrative:
Next, We **Establish Confidence**

Trust
in how we manage security

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

Confidence
in the information presented to reach a quality decision

4.
5.
6.
7.

Next Focus

4. Risks that Require Treatment

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
2	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

5. Budget Request - 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	
Third Party Risk Management Program	12/31/2022	Open	No	5	$80,000	$10,000	$30,000	$15,000	25 to 6
Secure Application Development program	10/30/2022	Open	No	8	$60,000	$30,000	$20,000	$10,000	20 to 6
Access Control program	12/31/2022	Open	No	9	$45,000	$5,000	$15,000	$5,000	12 to 8
Total					**$185,000**	**$45,000**	**$65,000**	**$30,000**	

Today's Budget Request Summary

- Total Initial **Implementation Costs**: $230,000 ($185,000 Hard Costs + $45,000 Soft Costs)
- Total Ongoing **Yearly Ongoing Costs**: $95,000 ($65,000 Hard Costs + $30,000 Soft Costs)

Yearly Budget Variance Summary

- Yearly Budget Approved: $1,000,000
- Yearly Budget Already Committed: $900,000
- Budget Variance Requested: $130,000 ($230,000 + $900,000 = $1,130,000. This is $130,000 Over Approved Budget)

HALOCK®

Level 1 – Is Budget Level Request Sufficient?

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

YES

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

NO

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

HALOCK®

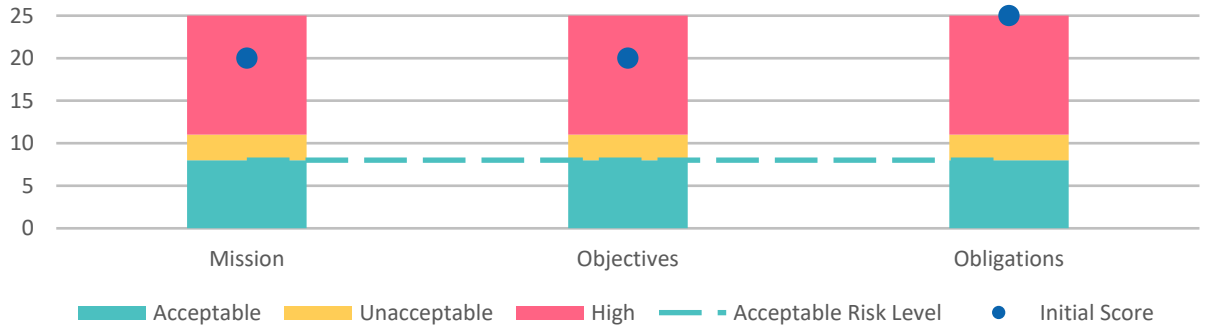
6. **Budget Request - Level 2:** Project Level

Project Name: *Third Party Risk Management Program*

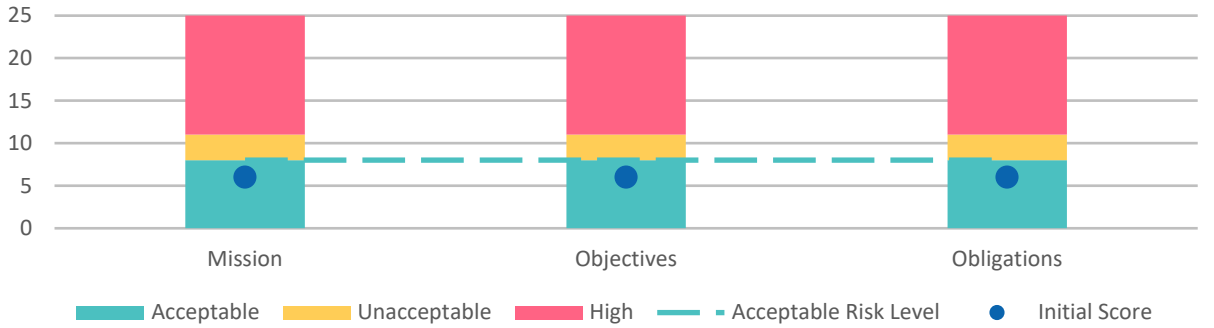
Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
				Hard Costs	Soft Costs	Hard Costs	Soft Costs	
12/31/2021	Open	No	5	$80,000	$10,000	$30,000	$15,000	25 to 6

What This Project Accomplishes	This project would build out a formal program to assess risk and manage risk for third parties.
Notes	Currently no formal program exists for assessing or managing risk to third parties and this is done ad-hoc.

Risk ID 5 | **BEFORE** THE SAFEGUARD



Risk ID 5 | **AFTER** THE SAFEGUARD



HALOCK®

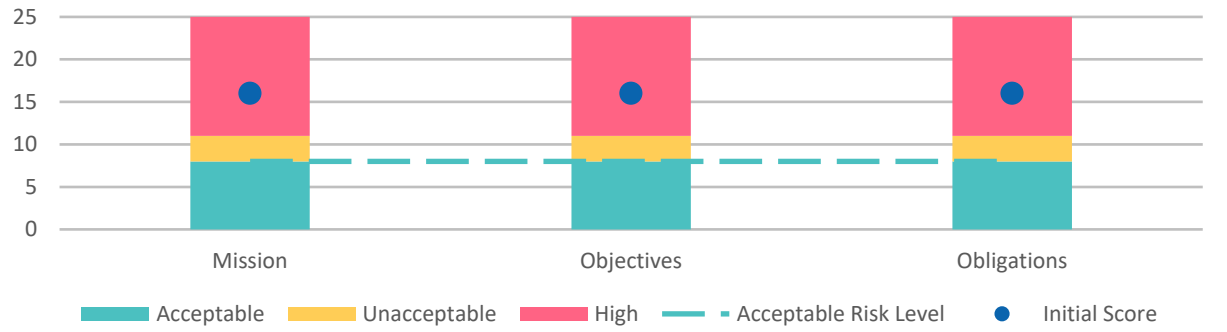
6. **Budget Request - Level 2:** Project Level

Project Name: *Secure Application Development program*

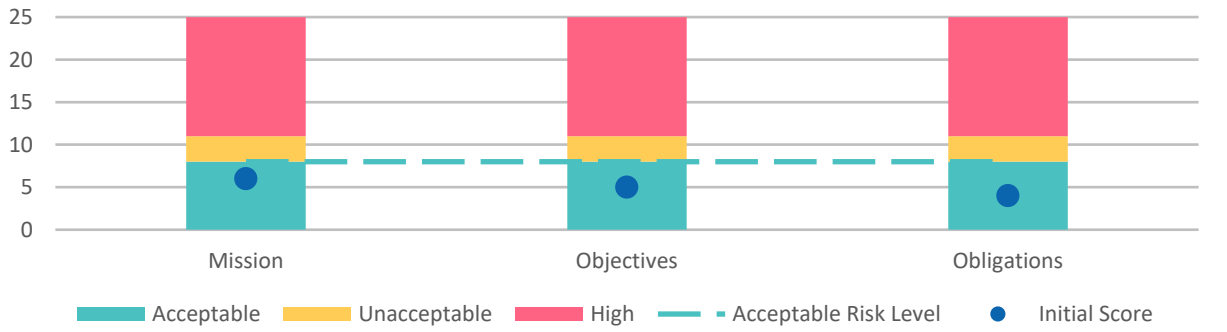
Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
				Hard Costs	Soft Costs	Hard Costs	Soft Costs	
10/30/2021	Open	No	8	$60,000	$30,000	$20,000	$10,000	**20 to 6**

What This Project Accomplishes	This project would put in place the training and implementation of a Secure Application Development program.
Notes	Currently nothing formal exists and this is done in various levels by various individuals.

Risk ID 8 | **BEFORE** THE SAFEGUARD



Risk ID 8 | **AFTER** THE SAFEGUARD



HALOCK®

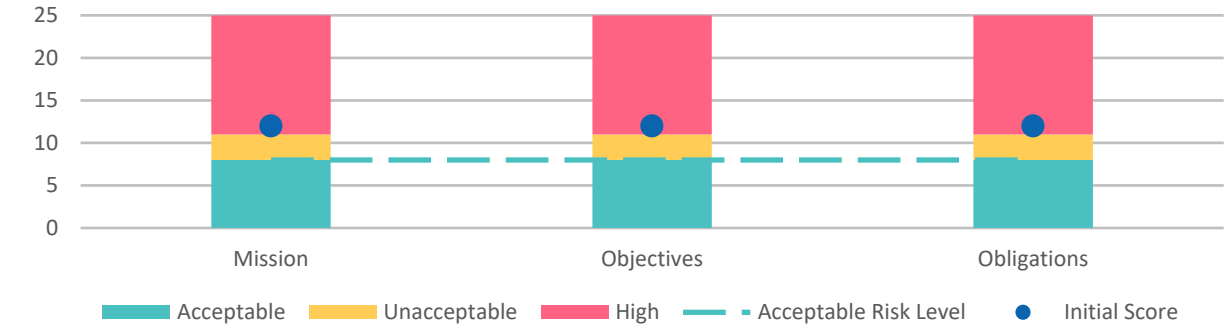
6. **Budget Request - Level 2:** Project Level

Project Name: *Access Control program*

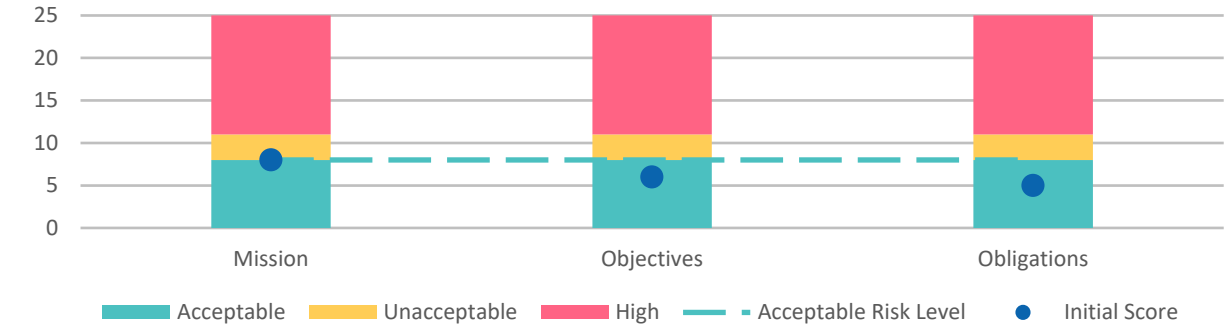
Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
				Hard Costs	Soft Costs	Hard Costs	Soft Costs	
12/31/2021	Open	No	9	$45,000	$5,000	$15,000	$5,000	**12 to 8**

What This Project Accomplishes	Develop and Implement an Access Control Program
Notes	Currently no Access Control Program exists

Risk ID 9 | **BEFORE** THE SAFEGUARD



Risk ID 9 | **AFTER** THE SAFEGUARD



HALOCK®

Level 2 – Is Project Level Request Sufficient?

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

YES

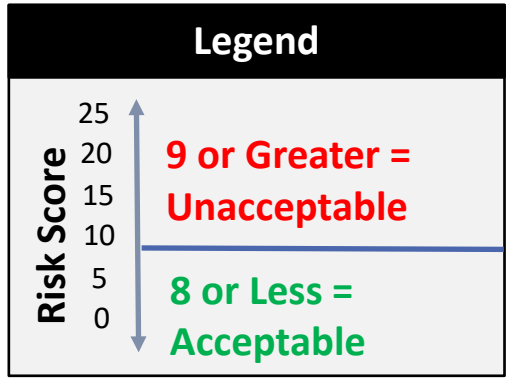
Budget is Approved at this level. **Great job!**

No

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

HALOCK®

7. Budget Request - Level 3: Risk Level



Risk Overview

Risk ID	Risk Description
5	IT Security conducts informal assessments of all third parties prior to contract completion.

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	
Third Party Risk Management Program	12/31/2022	Open	No	5	$80,000	$10,000	$30,000	$15,000	25 to 6

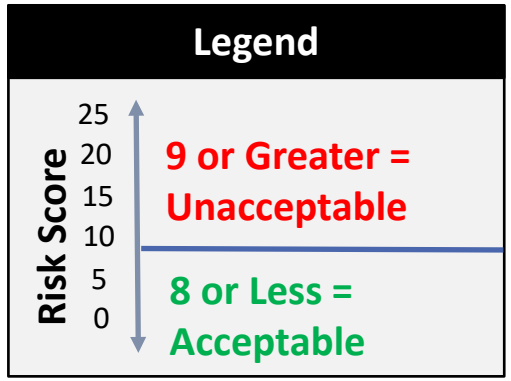
RISK IF PROJECT IS NOT DONE

Risk Score: 20 out of 25 (Catastrophic)	MISSION Score: 20 out of 25	OBJECTIVES Score: 20 out of 25	OBLIGATIONS Score: 20 out of 25
Likelihood = 5 Likelihood (5) x Highest Impact (5) = Risk of 25	**4.00** - Many Customers consistently cannot access beneficial information.	**4.00** - Profits may take more than a fiscal year to recover.	**5.00** - Some Customers may be harmed financially, reputationally, or physically.

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: 6 out of 25
Likelihood = 3 Likelihood (2) x Highest Impact (3) = Risk of 6	**2.00** - Some Customers may not get all the information they need as they request it.	**2.00** - Profits are within planed variance.	**2.00** - Customers may be concerned, but not harmed.

7. Budget Request - Level 3: Risk Level



Risk Overview

Risk ID	Risk Description
8	Secure application development is conducted by a third party that is non-contractually obligated or coding securely.

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	
Secure Application Development program	10/30/2021	Open	No	8	$60,000	$30,000	$20,000	$10,000	20 to 6

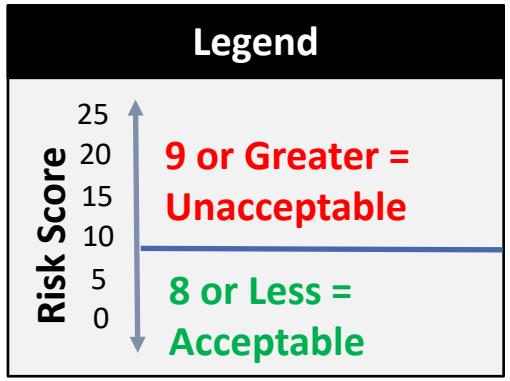
RISK IF PROJECT IS NOT DONE

Risk Score: 12 out of 25 (Catastrophic)	MISSION Score: 20 of out 25	OBJECTIVES Score: 20 of out 25	OBLIGATIONS Score: Score: 20 of out 25
Likelihood = 5 Likelihood (5) x Highest Impact (4) = Risk of 20	**4.00** - Many Customers consistently cannot access beneficial information.	**4.00** - Profits may take more than a fiscal year to recover.	**4.00** - Many Customers may be harmed financially or reputationally.

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: 6 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.	**2.00** - Customers may be concerned, but not harmed.

7. **Budget Request - Level 3:** Risk Level



Risk Overview

Risk ID	Risk Description
9	All access requests are submitted via ServiceNow and executed by IT. Access to SaaS application is not following a standardized access control program

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	
Access control program	12/31/2021	Open	No	9	$45,000	$5,000	$15,000	$5,000	**12** to **8**

RISK IF PROJECT IS NOT DONE

Risk Score: 12 out of 25 (High)	Mission Score: 12 out of 25	Objectives Score: 12 out of 25	Obligations Score: 12 out of 25
Likelihood = 3 Likelihood (3) x Highest Impact (4) = Risk of **12**	**4.00** - Many Customers consistently cannot access beneficial information.	**4.00** - Profits may take more than a fiscal year to recover.	**4.00** - Many Customers may be harmed financially or reputationally.

RISK AFTER DOING THE PROJECT

Risk Score: 8 out of 25 (Acceptable)	Mission Score: 8 out of 25	Objectives Score: 6 out of 25	Obligations Score: 6 out of 25
Likelihood = 2 Likelihood (2) x Highest Impact (4) = Risk of **8**	**4.00** - Many Customers consistently cannot access beneficial information.	**3.00** - Profits are off planned variance and may take a fiscal year to recover.	**2.00** - Customers may be concerned, but not harmed.

Level 3 – Is Risk Level Request Sufficient?

Is the Budget Request **Approved** at ***RISK LEVEL*** of detail?

YES

Budget is Approved at this level. Great job!

No

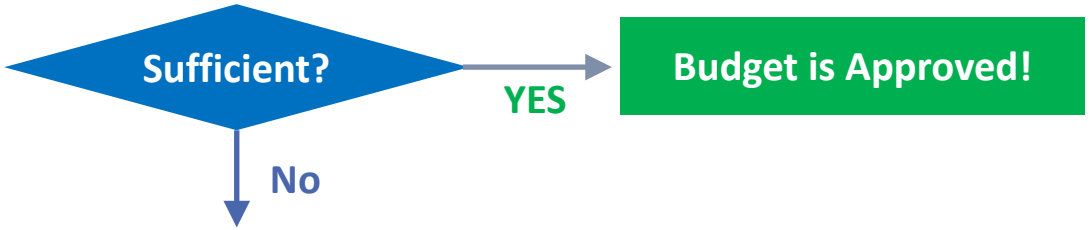
If more detail is required, inquire ***what else Approver needs*** to approve budget.

Budget Narrative – How We **Established Confidence**

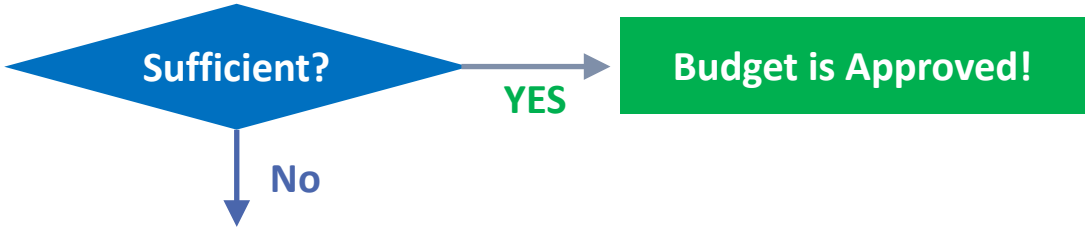
Confidence in the information presented to reach a quality decision

4 List of Risks that Require Mitigation

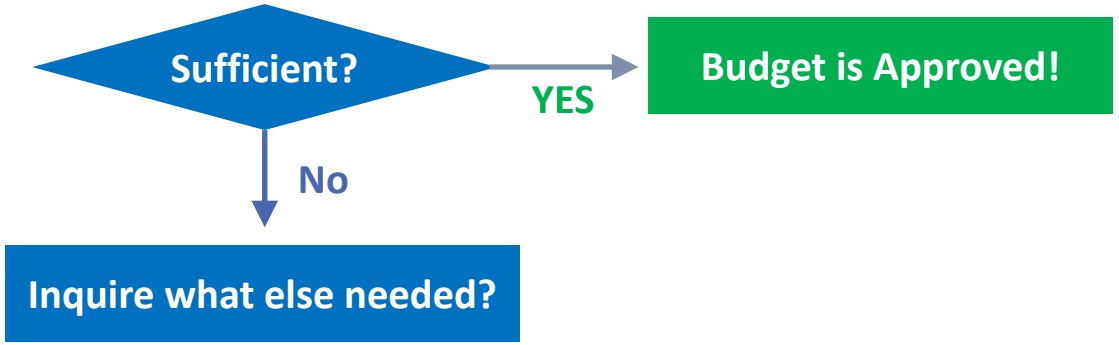
5 Budget Request – Level 1: Budget Level (Projects and Costs)



6 Budget Request – Level 2: Project Level (Projects and Business Impacts)



7 Budget Request – Level 3: Risk Level (Risks and Business Impacts)



HALOCK®

3. Real-Life Examples

How It Works

HALOCK

The Trust & Confidence Meter

Trust

In how you Manage Security

Confidence

In the information presented to reach a Quality Decision

Two Budget Request Approaches with Different Outcomes

Example: Data Loss Prevention (DLP) Budget Approval Request

1. Traditional Approach

2. Proven Budget Narrative Approach

Traditional Approach

Traditional Approach – DLP Budget 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 $250,000 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 it will not eliminate all of our risk."

CFO: "Let's start with approving $50,000 this year and re-evaluate next year."

HALOCK®

Traditional Approach – DLP Budget Request

Does Management Have Information to Answer the 4 Questions?

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

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.*

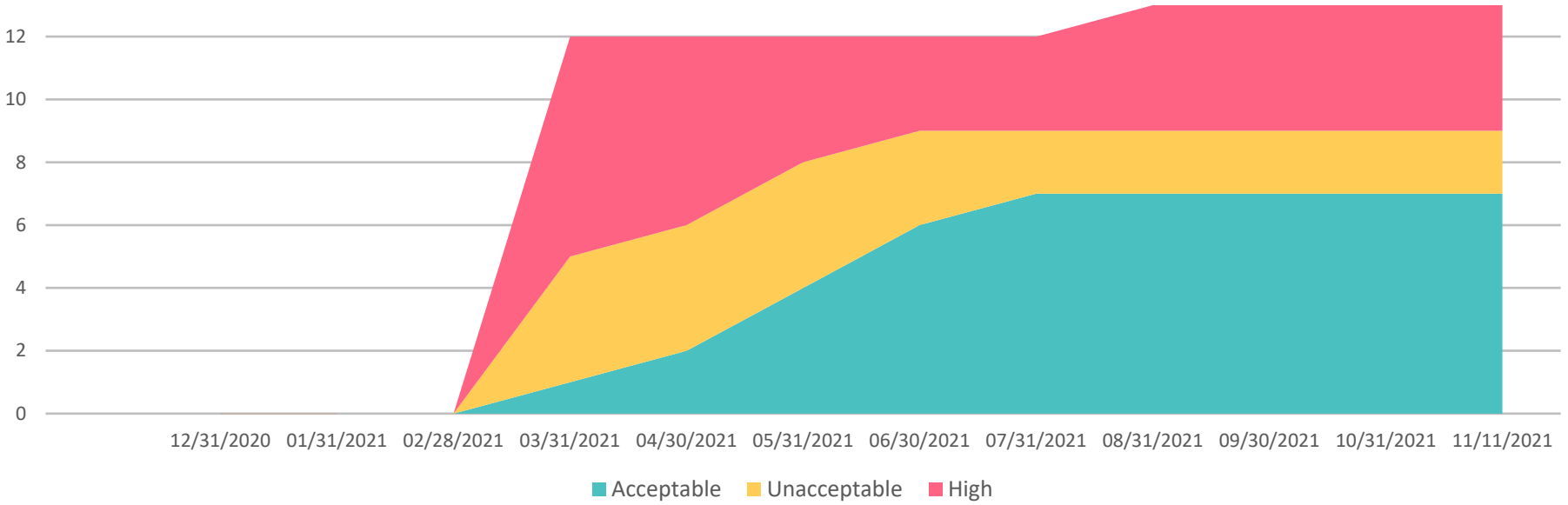
HALOCK®

Proven Budget Narrative Approach

Proven Budget Narrative Approach

1. Big Picture - Program Progress Over Time

	Dec 2020	Jan 2021	Feb 2021	Mar 2021	Apr 2021	May 2021	Jun 2021	Jul 2021	Aug 2021	Sep 2021	Oct 2021	Nov 2021
High				7	6	4	3	3	4	4	4	4
Unacceptable				4	4	4	3	2	2	2	2	2
Acceptable				1	2	4	6	7	7	7	7	7
Total				**12**	**12**	**12**	**12**	**12**	**13**	**13**	**13**	**13**



HALOCK®

Proven Budget Narrative Approach

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	0	0
Risk Count | Current	7	2	4

What contributed to risks since last review:

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

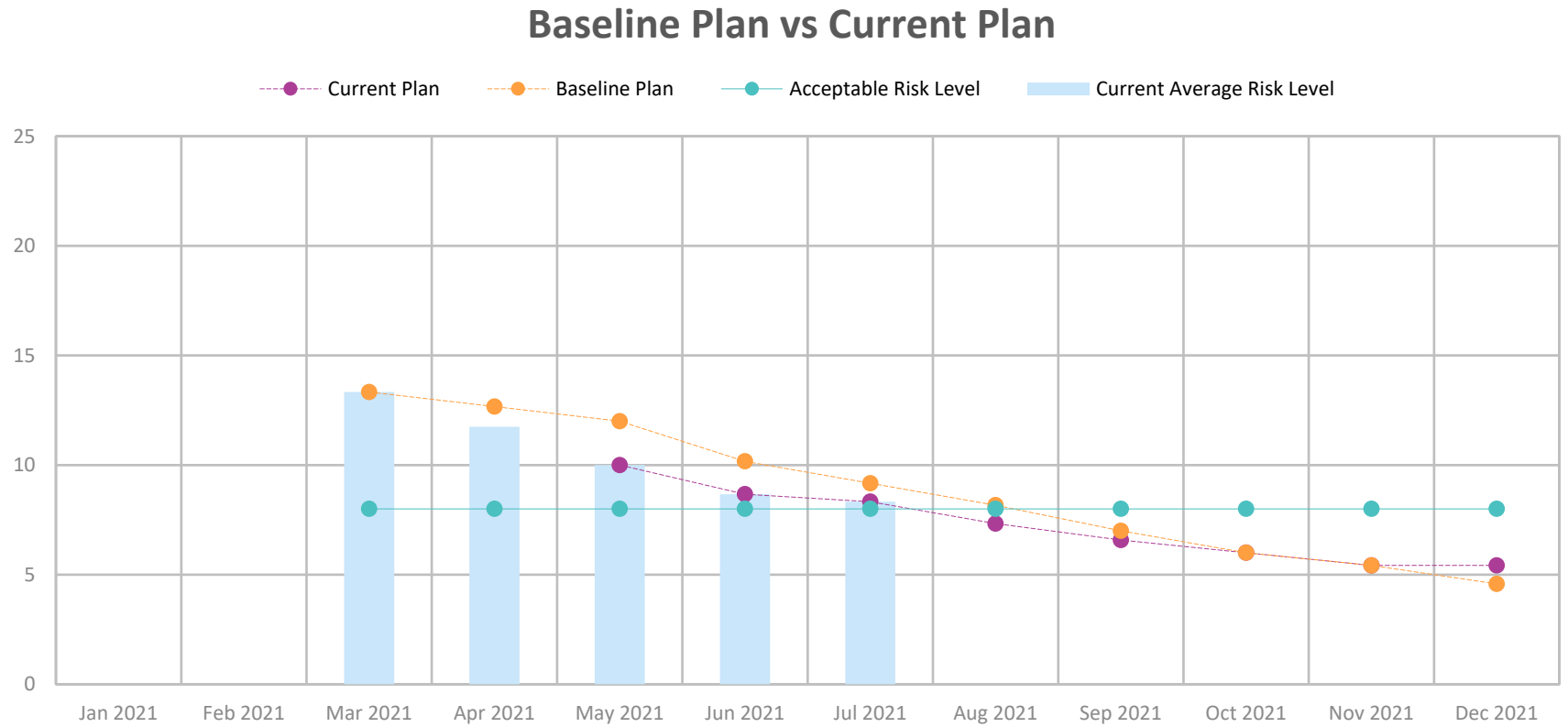
Comments	We completed our yearly Pen Test and also experienced a security incident in the Finance Business Unit relating to Business Email Compromise (BEC)

HALOCK®

Proven Budget Narrative Approach

3. Roadmap – Planned vs. Actual Risk Level

- We have stayed ahead of schedule for many months and below the acceptable risk level
- The decisions you made when you approved resources in March, ***enabled the organization to deliver on lowering risks*** through July



4. Risks That Require Treatment

Personally Identifiable Information (PII) unintentionally leaving the organization is currently the highest risk is 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
2	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

Budget Narrative Approach

5. Budget Request - 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	5	$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®

Level 1 – Is Budget Level Request Sufficient?

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

YES

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

No

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

HALOCK®

Budget Narrative Approach

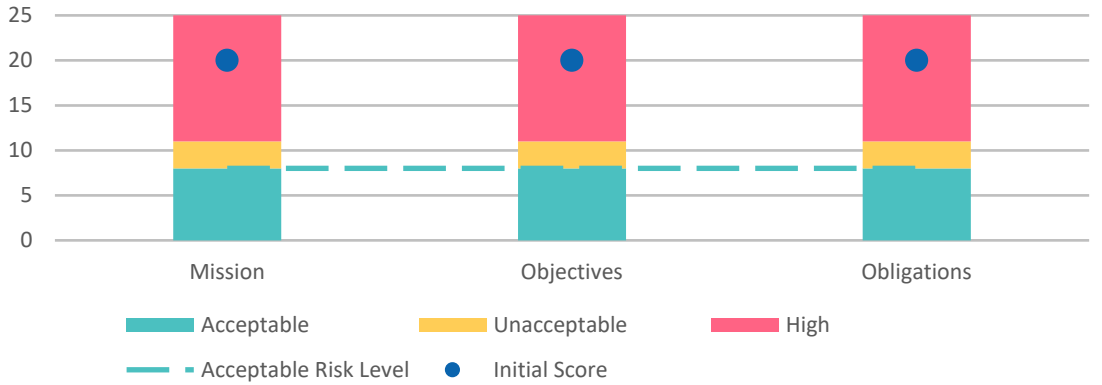
6. Budget Request - Level 2: Project Level

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

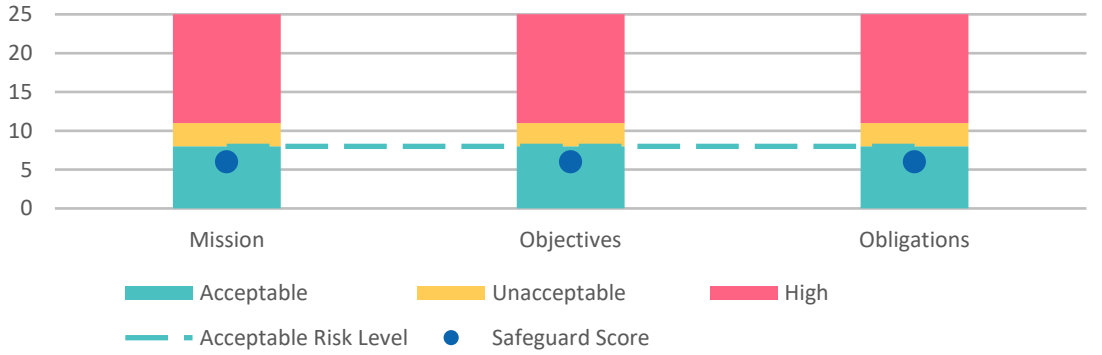
Estimated Completion Date	Status	Approved	RiskIDs Treated	Initial Implementation Costs		Ongoing Yearly Costs		Risk Reduction
				Hard Costs	Soft Costs	Hard Costs	Soft Costs	
12/31/2021	Open	No	5	$250,000	$30,000	$20,000	$10,000	20 to 6

What This Project Accomplishes	PII Leaving Perimeter. Utilizing a $180 cost per lost PII record (IBM Security & Ponemon Institute Report), we calculate a breach cost of $1,800,000 ($180 x 10,000 customer records) with a potential likelihood of (5) multiple time each year. This risk has a potential financial impact of $1,8000,000 multiple times per year
Notes	

Risk ID 5 | **BEFORE** THE SAFEGUARD



Risk ID 5 | **AFTER** THE SAFEGUARD



HALOCK®

Level 2 – Is Project Level Request Sufficient?

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

YES

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

NO

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

HALOCK®

Budget Narrative Approach

7. Budget Request - 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
5	PII Leaving Perimeter. Utilizing a $180 cost per PII lost record (IBM Security & Ponemon Institute Report), we calculate a breach cost of $1,800,000 ($180 x 10,000 customer records) with a potential likelihood of (5) multiple time each year. This risk has a potential financial impact of $1,8000,000 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	5	$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®

Proven Budget Narrative 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 $1.8M potential impact multiple times each year**

Trust and Confidence

What happened?

- Built Trust using the Proven Budget Narrative
- Answered all 4 Questions

Budget Approved!

Managing the "Delta"
Where You Start to Where Budget is Approved

Trust

You may be walking in with a Trust Level that is low for whatever reason and the "delta" to where you need it to be for budget approval will be a greater distance

Managing the "Delta"
Where You Start to Where Budget is Approved

Trust

You will need to get into the yellow to get some/partial level of budget approval.

Managing the "Delta"
Where You Start to Where Budget is Approved

Trust

You will need to get into the yellow to get some/partial level of budget approval.

Confidence

You need to be prepared to provide quality information and Answer the 4 Questions to get into the green and get full budget approval.

Putting it All Together

Budget Requester Provides

Proven 7-Step Budget Request Narrative

Trust: In how we manage security

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 Quality of Decision based on information presented

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)

+

Budget Approver Receives

Ability to Answer 4 Questions

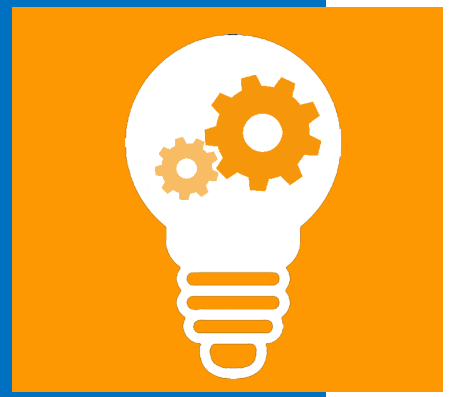
Does Management Have Information to Answer the 4 Questions?

1. **Risk Management:** "clear line" to know if a Risk "is okay" to accept? **Yes**
2. **Communication:** Speaking the same or different languages? **Yes,**
3. **Legal Protection:** Legally protected? **Yes, we're performing "due care"**
4. **Budgeting:** Spending the right amount? **Yes**

=

Budget Approved!

HALOCK®



4. Applying It

Now, Three Months and Six Months

HALOCK

What's Next…

- **Process** - DoCRA
  - DoCRA contains all the information required to communicate in business terms
  - Enlist the help of a professional
- **Output** - Budget Narrative
  - How you present the information is as important as the data you present!
  - If graphic design is not your forte, use a software package

When you are trying to build **trust** and **confidence**, mistakes and unprofessional appearance don't sit well

HALOCK®

Thank You
Now Go Get Your Budgets Approved!

Jim Mirochnik, MBA, PMP, ISO 27001 Auditor
CEO, Senior Partner
HALOCK Security Labs
jmirochnik@halock.com
847.221.0205 office

Download a copy of this presentation:
www.halock.com/CAMPIT2022

HALOCK®