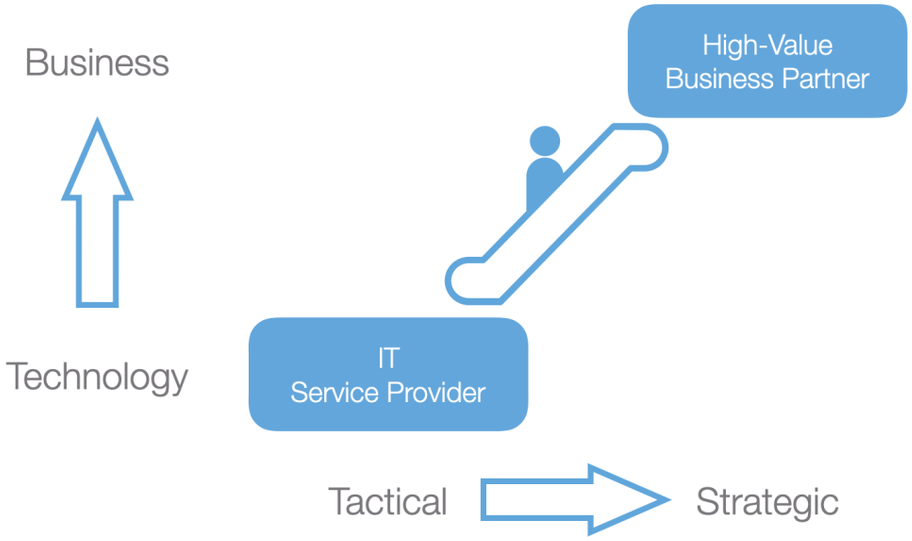
ManagedServices Platform

How to Communicate Cybersecurity to Executives

ManagedServices
Platform

INFOSEC
CONSULTING



IT SERVICE PROVIDERS ARE STRUGGLING TO MONETIZE SECURITY.

WE MAKE SECURITY MAKE SENSE FOR CLIENT DECISION MAKERS SO YOU CAN SELL CYBERSECURITY ASSESSMENTS AND REMEDIATION PROJECTS.

Problem

- Cybersecurity issues are growing
- Executive engagement is low
- Adoption of High Cybersecurity Standards are low
- MSPs have hard time monetizing the opportunities
- Frameworks and assessments have not solved the issues

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

Lack of engagement and direction

Business

Technology

Office Manager

Cybersecurity Engagement
Cybersecurity Roadmap/Budget Reviews
Cybersecurity Service Expansion

CEO

Cybersecurity Strategy Development
Cybersecurity Compliance
Cybersecurity Productivity

IT Coordinator

Cybersecurity Best Practice Adoption
Cybersecurity Awareness Training
Cybersecurity Processes

CFO/COO

Cybersecurity Roadmap
Cybersecurity Budget
Cybersecurity Stack Adoption

Tactical

Strategic

ManagedServices Platform

Lack of communication tools

Business

Technology

Tactical

Strategic

Account Manager

Cybersecurity Engagement
Cybersecurity Roadmap/Budget Reviews
Cybersecurity Service Expansion

vCIO/vCSO

Cybersecurity Strategy Development
Cybersecurity Compliance
Cybersecurity Productivity

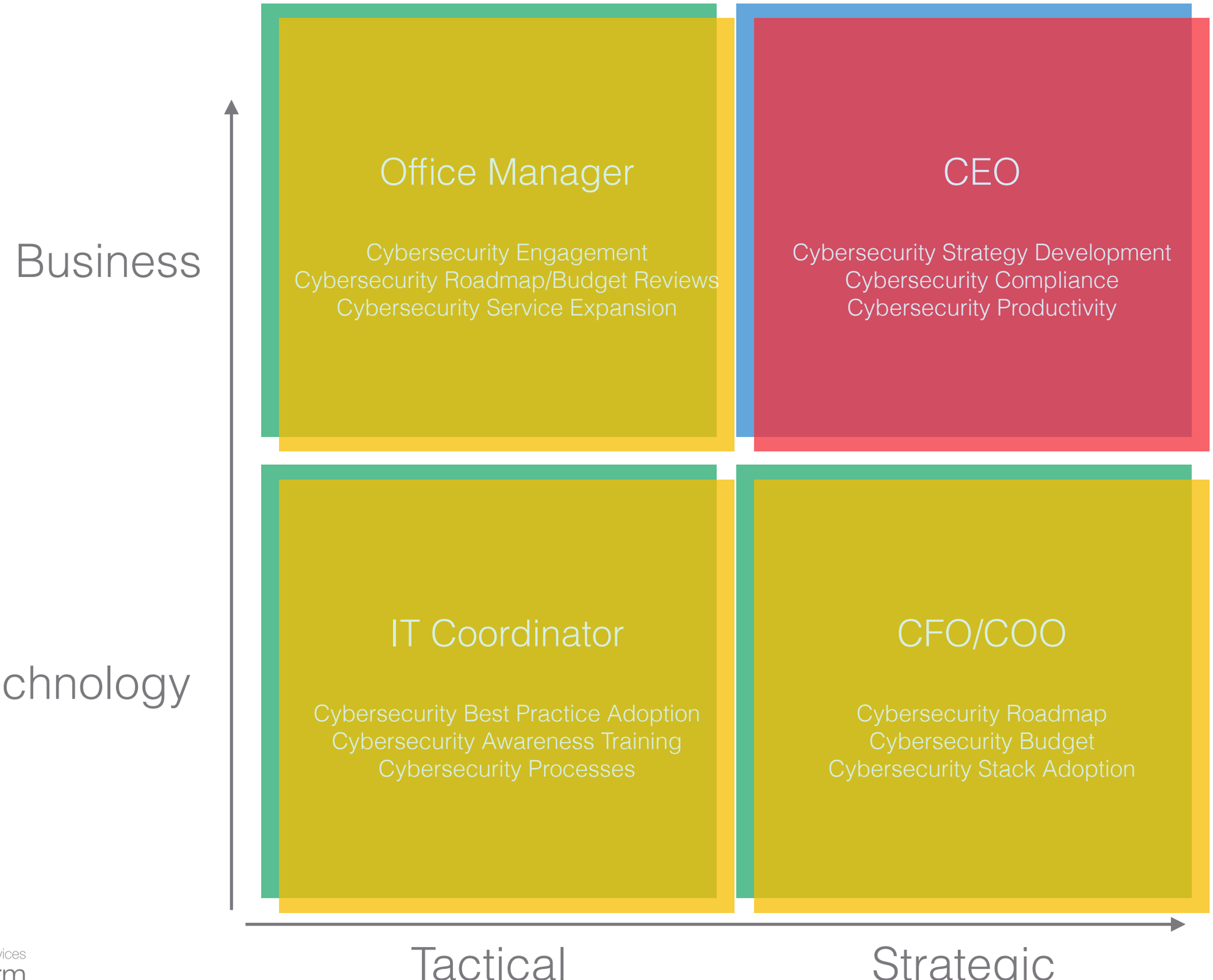
Technical Account Manager

Cybersecurity Best Practice Adoption
Cybersecurity Awareness Training
Cybersecurity Processes

Tech vCIO

Cybersecurity Roadmap
Cybersecurity Budget
Cybersecurity Stack Adoption

Misaligned Communication



Bridge the gap between Cybersecurity and Business

Current	Phase 01	Phase 02	Phase 03	Phase 04	Future
Improvement Need	Pre Qualification	Assessment	Action Plan	**Rinse and Repeat**	**Business Results**
Cyber Security is a concern, no real solution to protect the business	Pre Assessment Gut Check to create context and scope for the assessment	Complete NIST Cyber Security Framework Assessment Workshop	Fit-Gap Analysis followed by a Cyber Security Roadmap and required Compliance Services	Ensure accountability and demonstrate progress over time.	Clear Path to Success

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

Context matters

Firewall needs replacement

MFA should be adopted

Stronger passwords need to be implemented

Vs.

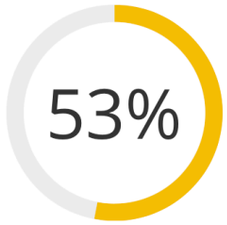
What do you think your role as a business owner is in providing a secure and low risk environment to your employees, clients and stakeholders?

How comfortable are you with your current ability to respond to a detected cyber incident?

What does that mean to your reputation, client's perception or the organization's day if a ransomware attack could lock up your systems?

Pre-Assessment Gut Check

Pre-assessment Gut Check Summary



Where you think you are

Pre-assessment Gut Check

Where you think you are

Pre-assessment Gut Check

How thoroughly have you investigated your regulatory obligations with regard to cybersecurity?	4
How compliant are you with applicable regulatory obligations? (if not-applicable, select 10)	5
How adequate is your current level of protection from cybersecurity incidents?	6
How comfortable are you with your current ability to DETECT a cybersecurity incident? (WHEN protection fails, will you know about it?)	5
How comfortable are you with your current ability to RESPOND to a detected incident?	7
How would your cyber risk management practices compare to peers and competitors? (5=average)	9
How comfortable are you with your current cyber insurance coverage?	5
In the case of a disaster, how confident are you that technical team(s) know the priority/order to restore systems and departments?	4
How aligned is business leadership with technical and cybersecurity management (executives vs IT and infosec teams)	2
How security-conscious is your employee base?	6

Result

- Management Buy-In with clear objectives
- Proper Audience(s) for the Assessment
- Understanding of the stakes and scope

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

Standard Cybersecurity Assessments

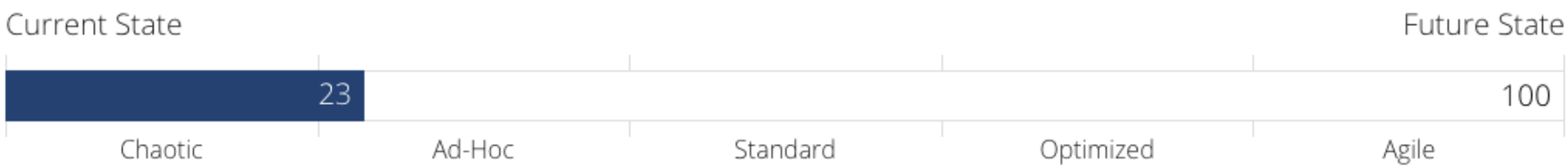
- Delivered by Cybersecurity Experts
- Audience is not defined
- Long and detailed
- Mid Market Focus

Overall NIST Cyber Security Framework Alignment

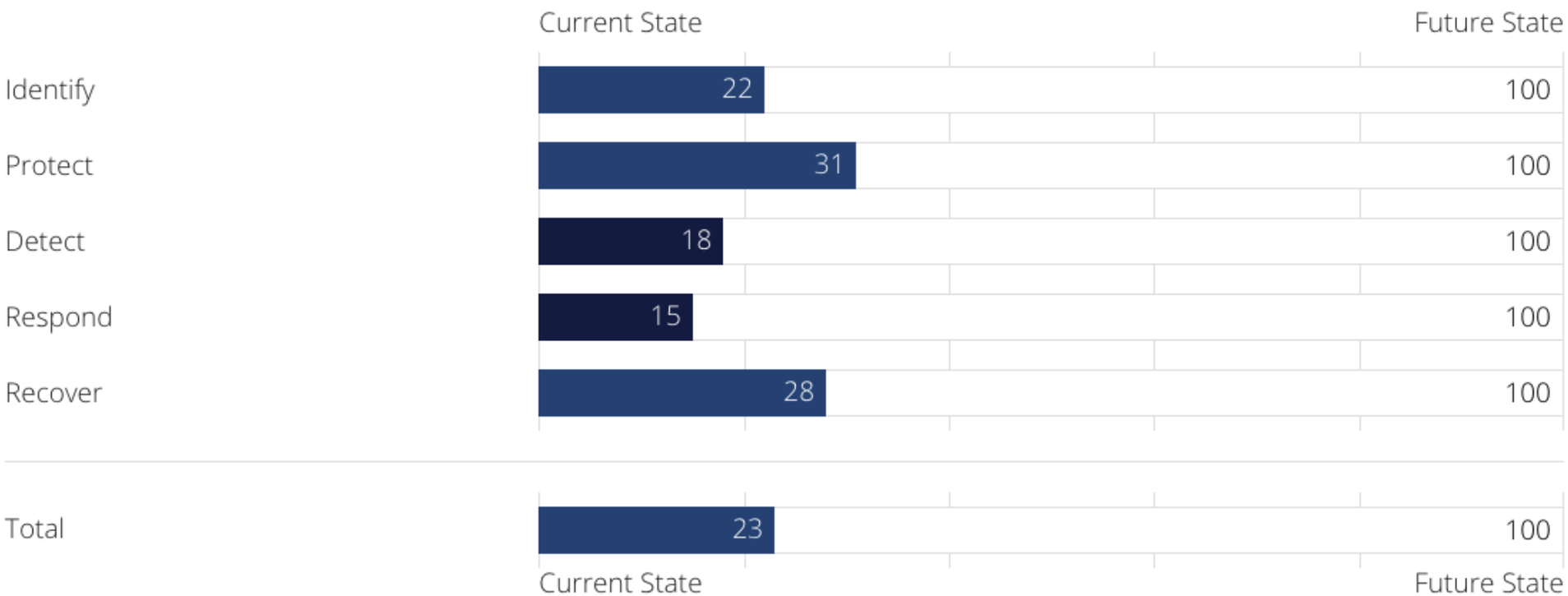
NIST Cyber Security Framework Assessment

2020. Oct. 28.

The colored section of the bar is the current level of alignment with the framework. The empty segment of the bar is the gap between where you are today and where you either should be, or would like to be in the future. The blank space to the right of the bar (if any) represents the controls that are not applicable, or which you don't intend to adopt.



NIST Cyber Security Framework Alignment by Core Function



Tier 1 "Partial"

Tier 2 "Risk Informed"

Tier 2 – Risk Informed

- **Risk Management Process** – Risk management practices are approved by management but may not be established as organizational-wide policy. Prioritization of cybersecurity activities and protection needs is directly informed by organizational risk objectives, the threat environment, or business/mission requirements.
- **Integrated Risk Management Program** – **There is an awareness of cybersecurity risk at the organizational level, but an organization-wide approach to managing cybersecurity risk has not been established**. Cybersecurity information is shared within the organization on an informal basis. Consideration of cybersecurity in organizational objectives and programs may occur at some but not all levels of the organization. Cyber risk assessment of organizational and external assets occurs, but is not typically repeatable or reoccurring.
- **External Participation** – Generally, the organization understands its role in the larger ecosystem with respect to either its own dependencies or dependents, but not both. The organization collaborates with and receives some information from other entities and generates some of its own information, but may not share information with others. Additionally, **the organization is aware of the cyber supply chain risks associated with the products and services it provides and uses, but does not act consistently or formally upon those risks.**

Tier 3 "Repeatable"

Tier 4 "Adaptive"

Asset Management (ID.AM)

Statement	Current State	Future State	Recommendations
ID.AM-1: Physical devices and systems within the organization are inventoried	☐	☑	Remote Monitoring and Management
ID.AM-2: Software platforms and applications within the	☐	☑	Remote Monitoring and Management
ID.AM-3: Organizational communication and data flows are mapped	☐	☐	
ID.AM-4: External information systems are catalogued	☑	☑	
ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	☑	☑	
ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	☑	☑	

ID.AM-4 Identify your external information systems.

- Identify the external systems that enable you to achieve business purposes.

Note

Comment

Tickets

Add New Todo Item +

Result

- Involvement with a thinking framework
- Set real expectations of goals
- Conversation instead interrigation

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

Executive Overview

Top Observations

- NOTHING DONE to assess supply chain / 3rd party risks
  - "I don't think we handle 3rd party risk very well at all." ~ Joe G.
- No 2FA on remote logins
- Systems diagrams incomplete
- Documentation doesn't list what types of data (PII etc) are stored on what systems
- Documentation doesn't show PII data flows (push, pull, data type, etc)
- No 24/7 monitoring
- Need compliant Policies
- Need to create/update IRP, BCP, & DRP
  - Need to run tabletop exercises

Action Items

- Start our NIST CSF Compliance Bundle
- Set up 2FA immediately for all remote access
  - Federate accounts/identities and enable 2FA
- Set up 24/7 monitoring immediately
- Work with developers to build a complete logical diagram including data flows and data types for all systems

Discussion Points & Other Notes

- Don't need physical security at reception because all sensitive data is in locked areas
- .....

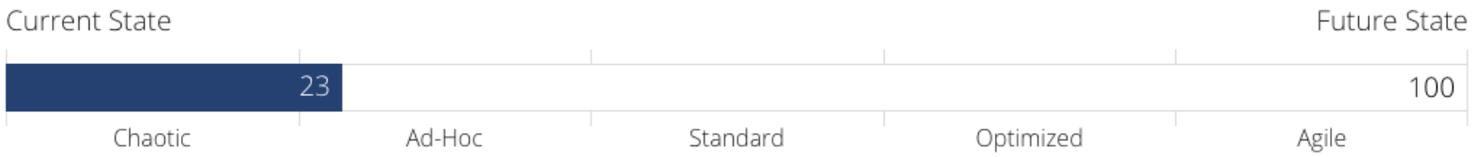
Business Case - Compliance

Overall NIST Cyber Security Framework Alignment

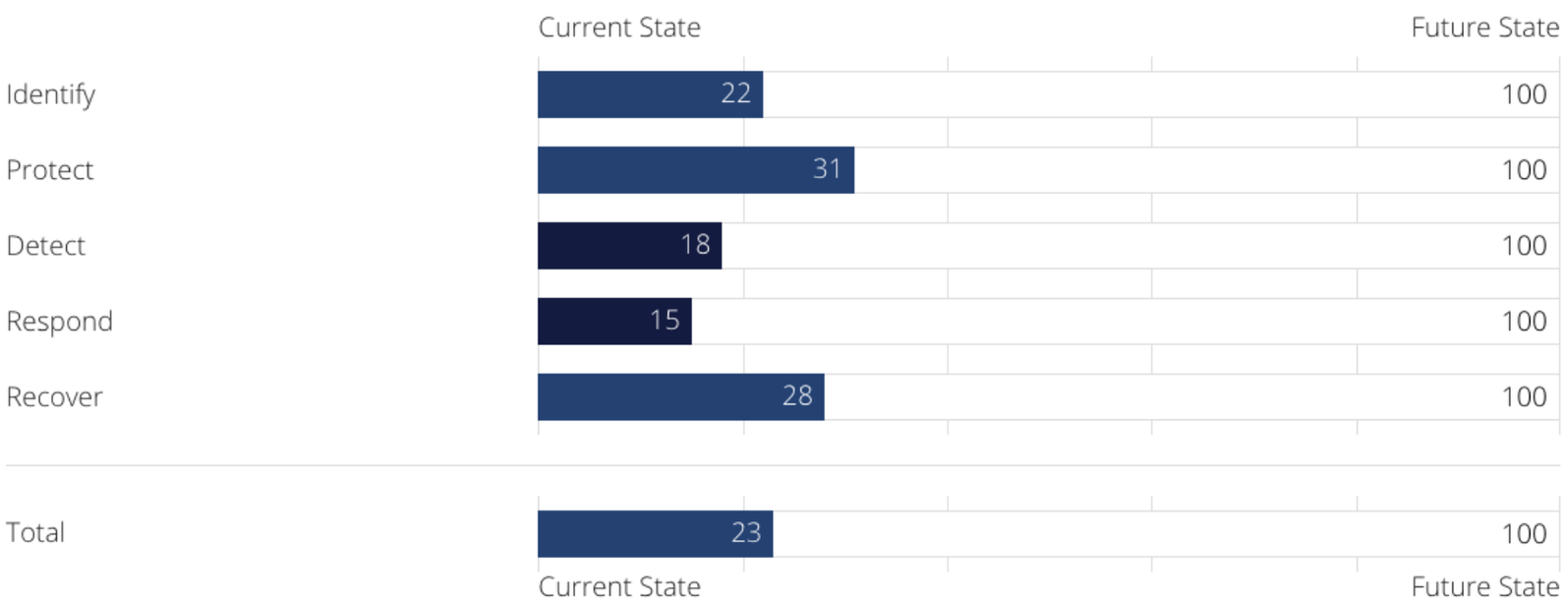
NIST Cyber Security Framework Assessment

2020. Oct. 28.

The colored section of the bar is the current level of alignment with the framework. The empty segment of the bar is the gap between where you are today and where you either should be, or would like to be in the future. The blank space to the right of the bar (if any) represents the controls that are not applicable, or which you don't intend to adopt.



NIST Cyber Security Framework Alignment by Core Function

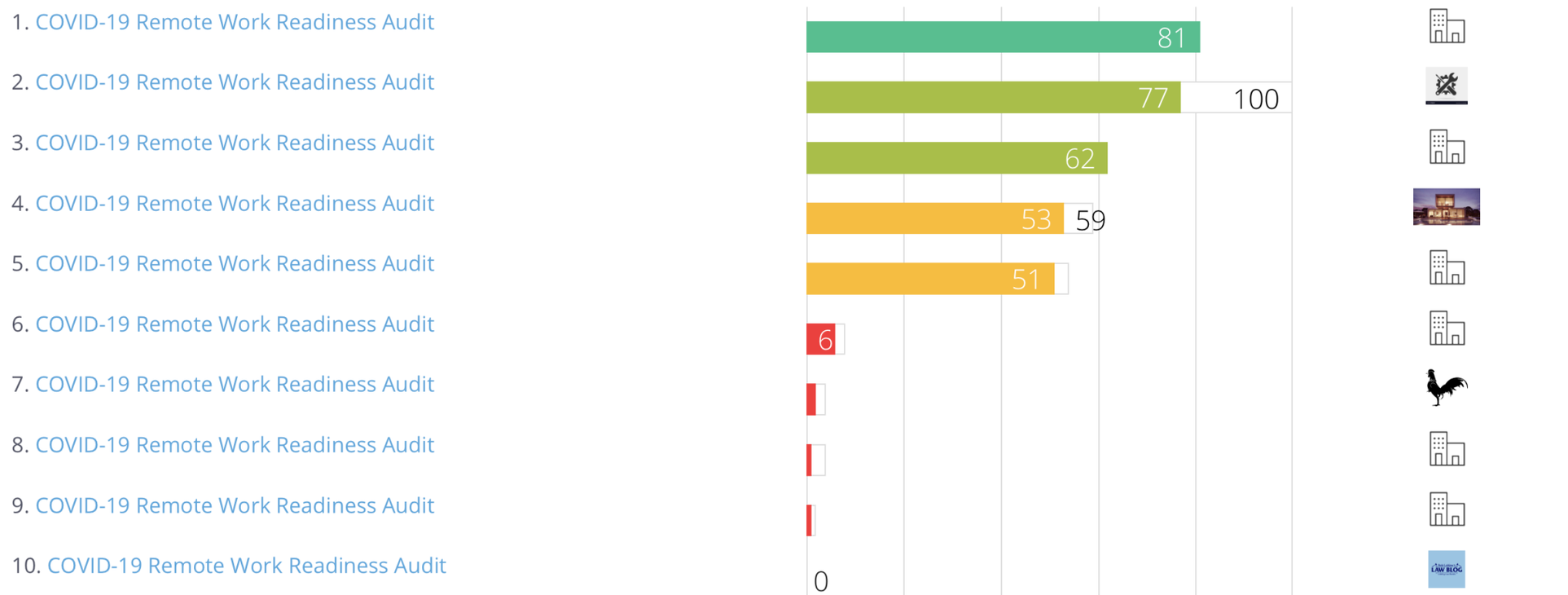


Business Case - Benchmark

COVID-19 Remote Work Readiness Audit

15 reports average based on 13 clients

Webinarski Tools Inc., Turner's Machine, Tom's Co, New Corp, Big Design, Inc., Black Rooster, Inc., Thompson, Lisa, Client A Awesome, NewCoTuesday, Thursday Co, msp.app, Bob Loblaw, Bene Partum Law Group



Business Case - Responsibilities

GRC RACI Chart **R - Responsible | A - Accountable** **C - Consulted | I - Informed**	You	Me	Nobody
GRC - Governance Risk and Compliance			
GOVERNANCE			
Policy enforcement			
Training - being prepared and reporting potential incidents			
Monitor for security incidents and violations			
Desktop and server security			
Network infrastructure security			
Website security			
Physical / premises security			
Procurement of IT and security products and services			
Plan testing			
Declare MTD, RPO, RTO for critical systems			
Design & recommend solutions to meet MTD, RPO, and RTO requirements			
Fund solution implementation			
Incident Response			
Backup configuration and testing			
RISK			
Provide periodic summary of top risks, impacts, and likelihood to senior leadership			
Identify cyber risks			
Prioritize risks			
Make and fund risk decisions (mitigate, transfer, accept)			
3rd party / vendor security evaluations, NDAs, partnership agreements			

Business Case -Roadmap Plan

Cyber Security Roadmap

ManagedServices Platform

Client Proposal

Bob's Trucking

imported

Client Segment: A - Monthly Engagement - VIP Client

12440 73rd Ct
Clearwater, FL
33612

Contacts | Project Roadmap | Assets | Marketing | Delivery | Contracts | Proposals | Reports | CES™

Search for Proposals...

Create New Proposal

Implement Multi Factor Authentication Solution

Problem: Hacking passwords is hard but not impossible. As we get more and more authentication to more and more apps our passwords are more exposed to non-encrypted databases open for hackers to invade. Knowing email addresses and passwords gives them leverage to infiltrate public services we use. Getting more information allows them to access more data, and to hack passwords for more sensitive services like our emails. There are methods and automation available to work on thousands of victim...

0 assets belongs to this project

	$4,500.00
	$3,500.00
Implement Multi Factor Authentication So...	$2,500.00

No addible projects

Sum Price:	$10,500.00
Discount:	3000
Proposal Price:	**$7,500.00**

Note

Save | Save & Share | Cancel

Result

- Business Cases for Decision Making
- Roadmap for progress
- Quick decision making

How to Communicate Cybersecurity to Executives

- Gap between Cybersecurity Services and Business
- 1. Business Context for Cybersecurity
- 2. Business Assessment for Cybersecurity
- 3. Business Action Plan for Cybersecurity
- 4. Remediation Process for Cybersecurity

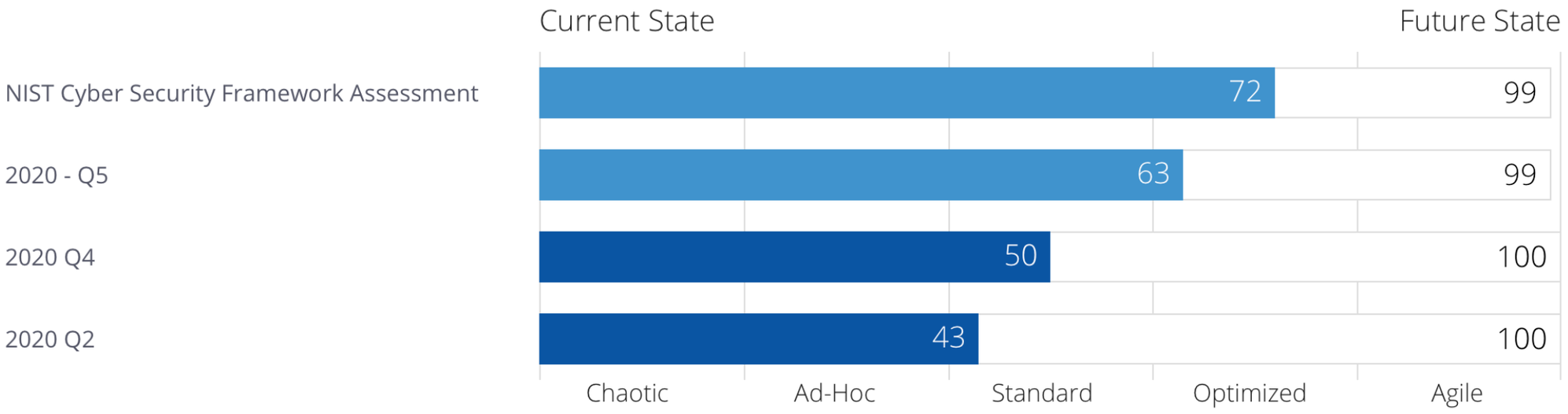
Clear progress

Overall NIST Cyber Security Framework Alignment

NIST Cyber Security Framework Assessment

2020. Dec. 1.

The colored section of the bar is the current level of alignment with the framework. The empty segment of the bar is the gap between where you are today and where you either should be, or would like to be in the future. The blank space to the right of the bar (if any) represents the controls that are not applicable, or which you don't intend to adopt.



Responsibility Distribution

Cyber Security Compliance Services

Add Service Bundle

Price Calculator

	NIST Cyber Security Framework Compliance - Client Side	NIST Cyber Security Framework Compliance - Service Provider Side
Unit	User	User
Unit Price (Monthly)	$0.00	$50.00
Number of Units		
Price (Monthly)	$	$

Current State — Recommended State

43 — 100

Chaotic | Ad-Hoc | Standard | Optimized | Agile

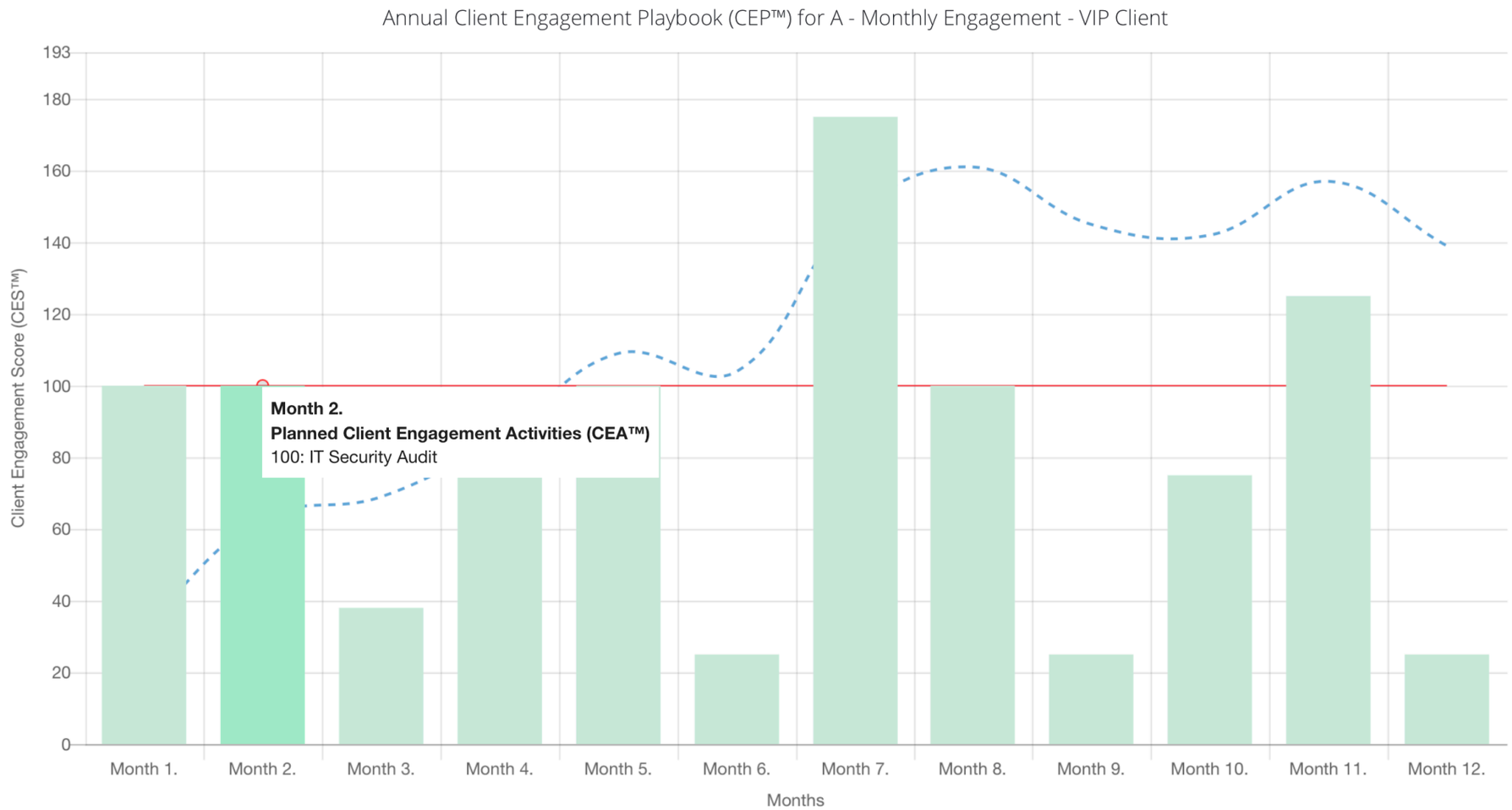
	NIST Cyber Security Framework Compliance - Client Side	NIST Cyber Security Framework Compliance - Service Provider Side
Future Services		
Remote Monitoring and Management		✔
Vulnerability Management		✔
Change control		✔
Multifactor Authentication		✔
Advanced Endpoint Protection		✔
Secure Network Segmentation		✔
Advanced integrity controls		✔
Policies, Procedures and Plans	✔	✔
Lifecycle management		✔
Security Awareness Training	✔	✔
Cyber Risk Assessment		✔
Supply Chain Documentation	✔	
Roles and Responsibilities Documentation	✔	
Security Operations Center (SOC)		✔
Tabletop Exercises	✔	✔
Risk Management	✔	
Current Services		
Remote Monitoring and Management		✔
Penetration Testing		✔
Cyber Insurance	✔	
Logging archival and review		✔
High availability		✔
Physical monitoring and security services	✔	
USB storage disablement		✔

Holistic Process

A - Monthly Engagement - VIP Client

Frequency: None

Target Score: 100



Holistic Process

100

IT Strategy Workshop

Report

Activitiy planned fot the 1. month of the template

CEO

100

IT Security Audit

Report

Activitiy planned fot the 2. month of the template

Top Manager

25

Lunch & Learn

Lunch & Learn

Activitiy planned fot the 3. month of the template

Middle Manager

13

Regular Webinars

Regular Webinars

Activitiy planned fot the 3. month of the template

IT Coordinator

75

Strategic Business Review

Report

Activitiy planned fot the 4. month of the template

Senior Manager

100

Office365 Productivity Audit

Report

Activitiy planned fot the 5. month of the template

Top Manager

Track Account Activities

Status

- ☐ Planned
- ☐ Completed
- ☐ Missed

Account Manager

- ☐ Denes Purnhauser
- ☐ Myles Olson
- ☐ Skip Ziegler
- ☐ Caleb Christopher
- ☐ Not set

Client Segment

- ☐ D - Micro
- ☐ Strategic Prospect
- ☐ Onboarding Process
- ☐ A - Monthly Engagement - VIP Client
- ☐ B - Quarterly Reviews - Standard Client
- ☐ C - Semi-Annual - Low Touch Client
- ☐ Onboarding Big
- ☐ Not set

Engagement Level

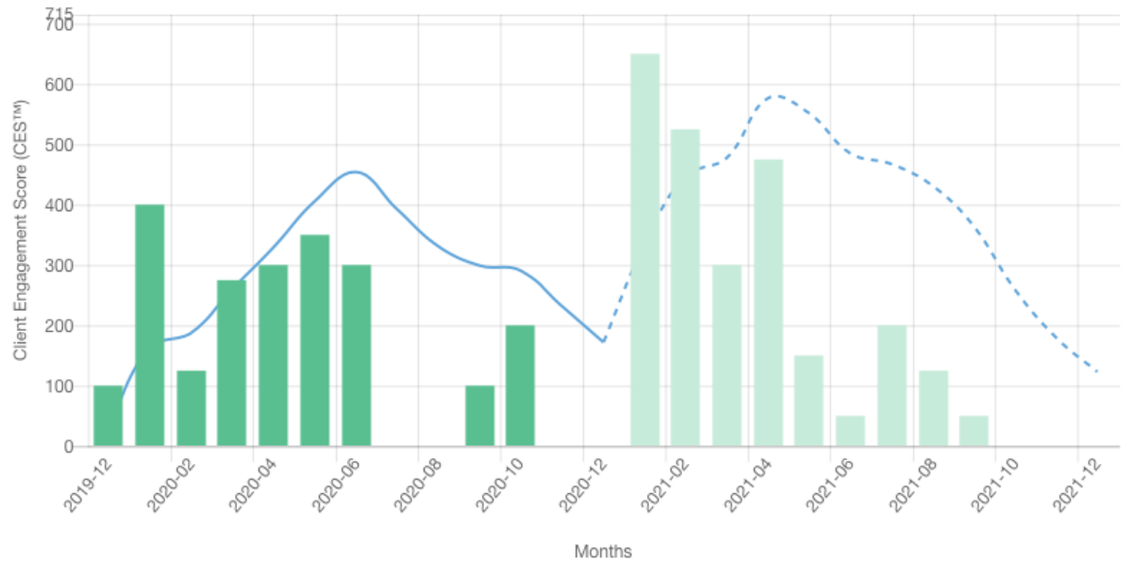
- ☐ On Target
- ☐ Below Target
- ☑ Off Target
- ☐ Not Set

Activity Type

- ☐ Grader
- ☐ Email Campaign
- ☐ Report
- ☐ Custom

Subscribe to iCAL Activities

Activites



100 Report

Report

Dec 23, 2019

1 contact involved

Acme Corp.

50 Lunch & Learn

Regular live events around a specific topic.

Lunch & Learn

Jan 15, 2020

1 contact involved

Holy Trinity

100 IT Infrastructure Audit

Report

Jan 15, 2020

1 contact involved

Bob's Trucking

ManagedServices Platform

Result

- Clear Responsibilites
- Clear Progress
- Clear Motivation

Cybersecurity Engagement

Business

Technology

Office Manager

Cybersecurity Engagement
Cybersecurity Roadmap/Budget Reviews
Cybersecurity Service Expansion

CEO

Cybersecurity Strategy Development
Cybersecurity Compliance
Cybersecurity Productivity

IT Coordinator

Cybersecurity Best Practice Adoption
Cybersecurity Awareness Training
Cybersecurity Processes

CFO/COO

Cybersecurity Roadmap
Cybersecurity Budget
Cybersecurity Stack Adoption

Tactical

Strategic

ManagedServices Platform

Bridge the gap between Cybersecurity and Business

Current	Phase 01	Phase 02	Phase 03	Phase 04	Future
Improvement Need	Pre Qualification	Assessment	Action Plan	**Rinse and Repeat**	**Business Results**
Cyber Security is a concern, no real solution to protect the business	Pre Assessment Gut Check to create context and scope for the assessment	Complete NIST Cyber Security Framework Assessment Workshop	Fit-Gap Analysis followed by a Cyber Security Roadmap and required Compliance Services	Ensure accountability and demonstrate progress over time.	Clear Path to Success

Steps to start Business Conversations

NIST Cybersecurity Framework Quickstarter Pack

Promotion - ~~$500 one time~~ - Free

Before 15th of January 2021

- For Existing Members

  - Go To Marketplace use coupon **MERRY-NISTMAS**

- For Non Members

  - Schedule a Demo pick a plan and get onboarded