

Streamlining CMMC 2.0 & FRCS Compliance: Software Solutions for Small DoD Contractors



H&V Complynt

Fortifying the Future: Mastering Cyber Resilience for Critical Operations

Panelists:

- Josh Hammer – VP Business Development, H&V Facility Solutions Inc.

Moderator:

Doug DeFazio

**TRI - REGIONAL
JETS 2025**

Society of
SAFETY
American Military Engineers



Panelist

Josh Hammer

H&V Facility Solutions

VP Business Development



- **Sports Teams: USF, Bucs, Jags, Tampa bay Lightning**
- **Vacation Spots: North Carolina, Bahamas**
- **Did You Know: I've marched in the Macy's Thanksgiving Day Band**
- **Hobbies: Music Education, Weightlifting, Coffee**
- **Cooler Project(s): New JEA Headquarters, Guam new BEQ Building Automation**

CMMC and other compliance certifications are costly, time consuming, and difficult to understand. Rather than do it manually, we should begin to use software tools to automate and speed up the compliance process saving both time and money.

Learning Objectives

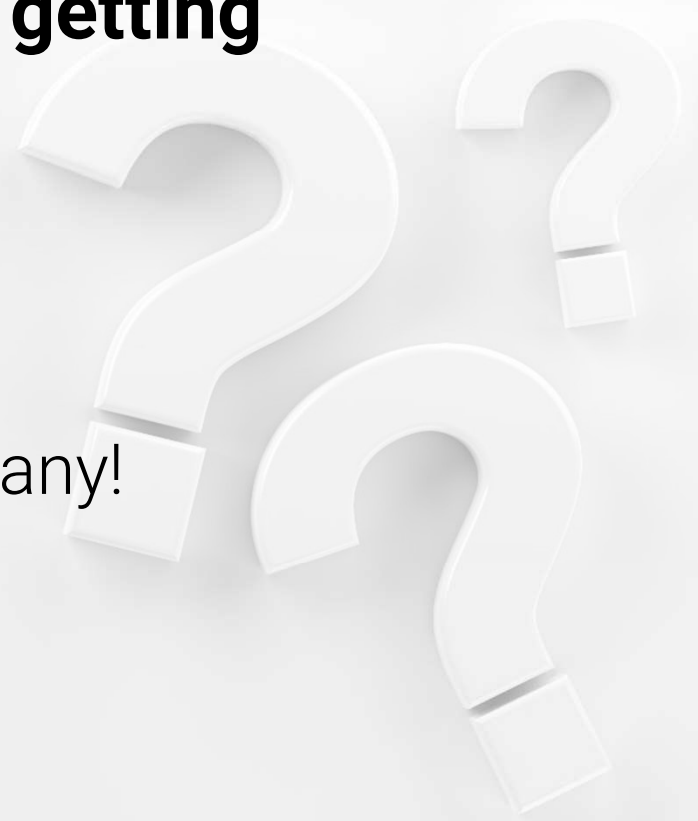
- Learn the 6 Steps to CMMC 2.0 Certification and understand the basic roadmap
- Understand the savings in utilizing software solutions vs. manual solutions
- Learn how to evaluate what the right practical approach is for your CMMC needs.

Agenda

- Overview of CMMC Compliance
- A Roadmap to Compliance
- Case Study – Manual vs. Automated
- Q&A / Discussion

How many hours have you spent getting your CMMC Certification?

- a) 0
- b) 1-40+
- c) I can't remember because it's so many!



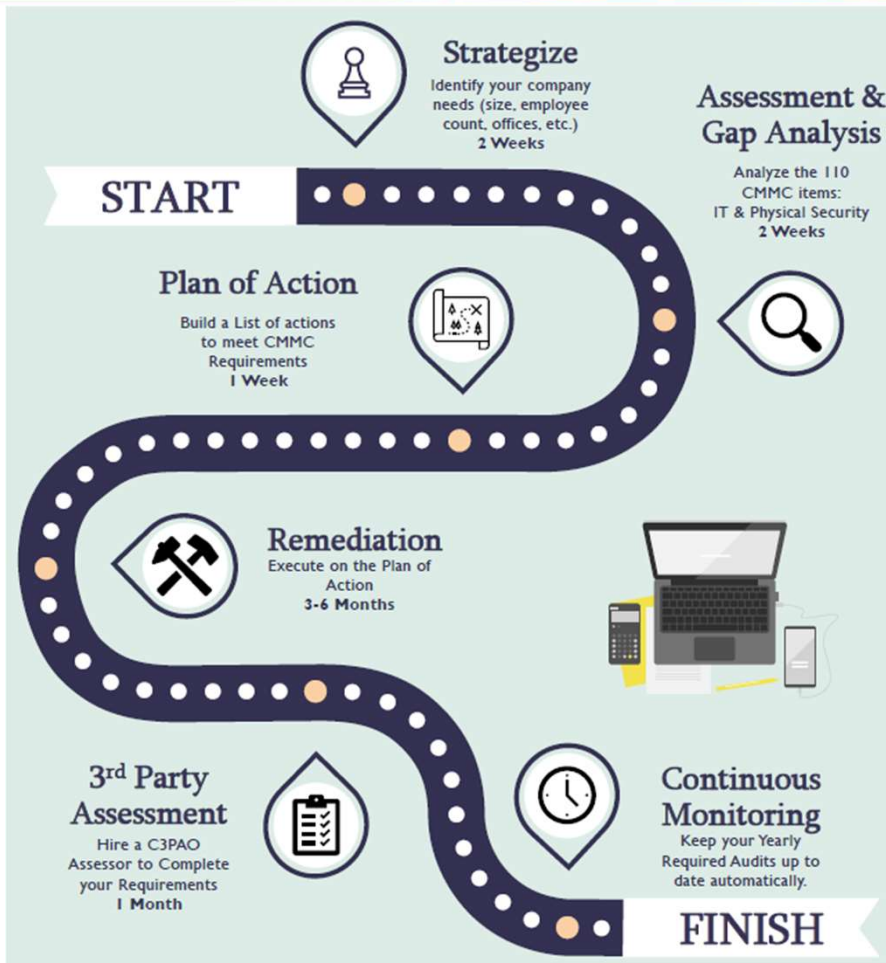
How many hours have you spent getting your CMMC Certification?

- Free resources by project Spectrum help small business achieve CMMC 2.0
 - Often reported to take between 1000 & 1700 manhours to achieve this using internal manpower!
- Software Tools are like the difference between a manually drawing something vs. using AutoCAD

Even free resources are expensive to implement!

A Simple Roadmap to Compliance

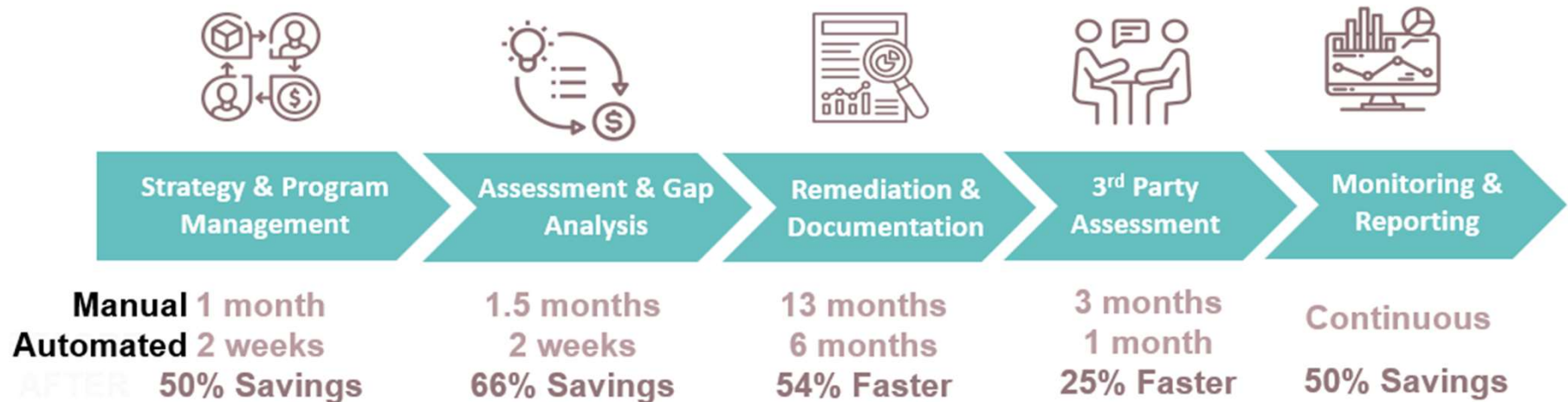




CMMC Compliance has 5 Main Steps + Monitoring

1. Strategize
 - Company size, CUI requirements, User Count, etc.
2. Assessment & Gap Analysis
 - 110 CMMC Controls including networks, employee handbooks, & physical security
3. Plan of Action
 - Build a list of action items to meet compliance requirements
4. Remediation
 - Execute on the Plan of Action
5. 3rd Party Assessment
 - Hire a C3PAO Assessor
6. Continuous Monitoring and Updating
 - Recertifications done every 3 years for compliance

Timeline using Traditional vs. Software Augmented Solutions



Strategy & Program Management

Initial Readiness Questionnaire

1. Organization Profile & Environment
2. Access Control/Audit – Internal IT or External MSP (technical)
3. Personal Security / Awareness & Training
4. Physical Protection
5. Risk-Security Assessment/Incident Response
6. System & Information Integrity/Maintenance



Initial NIST 800-171/CMMC Readiness Questionnaire

The questions compiled below are geared toward providing H&V Facility Solutions with an initial system evaluation for protecting Controlled Unclassified Information (CUI) and a basic system scope for CUI preparedness. For the purpose of this assessment, CUI includes both CDI and CTI, as well as any contract related information. This questionnaire will assist in developing an overall assessment strategy.

Internal Stakeholders, HR, FSO, and internal/external IT/Cyber POCs will be required to answer these questions. Meetings(s) can also be scheduled with POCs to go over these questions and assist/offer guidance.

1. Organization Profile and Environment

Typically, **Internal Stakeholders** and **internal/external IT/Cyber POCs** can answer these questions. Meetings(s) can also be scheduled with POCs to go over these questions and assist/offer guidance.

1.1.1. How many locations (satellite offices, ~~ect.~~) does the organization have?

2

1.1.2. How many employees does the organization currently employee?

1



23-35

1.1.3. Does the organization employee any remote workers?

No

1.1.4. Does the organization currently access, handle, or process CUI? Or have plans, future contracts that would require them to access, handle, or process CUI?

800-171 Req

1.1.5. Does the organization employ any internal IT staff? If yes, please explain.

Internal

Assessment & Gap Analysis - Manual

SPRS Score: -202 / 110																
Organization Name: _____ System Security Plan (SSP) / System Name: _____ CAGE Code(s) Supported by SSP: _____																
SSP Version / Revision: 1.0				SSP Date: 08/01/2023												
Assessment Scope: Enterprise				[Assessment Scope] Enterprise = Entire organization network under the listed CAGE codes.												
Assessment Date: 10/03/2022																
Plan of Action Completion Date: 10/03/2023																
Contr	Famil	Description	Type	Weight	Partial	Examine	Interview	Test	Status	POA&M	Notes	Score	Assessor Guidance	FAR	CMMC Level	CMMC 1.0
3.11	Assessor Control	Limit system access to authorized users, processes, systems, hardware, software, and devices (including other systems).	Basic	5	0							-5		b.1.i	L1	AC.1.001
3.12	Assessor Control	Limit system access to the type of transaction and function that authorized users are permitted to execute.	Basic	5	0							-5		b.1.ii	L1	AC.1.002
3.13	Assessor Control	Control the flow of OUI in accordance with approved authorization.	Derived	1	0							-1			L2	AC.2.016
3.14	Assessor Control	Separate the duties of individuals to reduce the risk of malfeasance activity without collusion.	Derived	1	0							-1			L2	AC.3.017
3.15	Assessor Control	Employ the principle of least privilege, including for specific execution functions and privileged accounts.	Derived	3	0							-3			L2	AC.2.007
3.16	Assessor Control	Use non-privileged accounts or roles when accessing secure systems.	Derived	1	0							-1			L2	AC.2.008
3.17	Assessor Control	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in an audit log.	Derived	1	0							-1			L2	AC.3.018
3.18	Assessor Control	Limit unsuccessful login attempts.	Derived	1	0							-1			L2	AC.2.009
3.19	Assessor Control	Provide privacy and security notices consistent with applicable OUI rules.	Derived	1	0							-1			L2	AC.2.005
3.110	Assessor Control	Use session lock with pattern-hiding display to prevent access to OUI data and data in memory.	Derived	1	0							-1			L2	AC.2.010

Assessment & Gap Analysis – Semiautomated

Project: MyCMM Cv2

Filter

Control	IS	PP	E	G	W
AC.L1-3.1.1	●	●	●	●	●
AC.L1-3.1.2	●	●	●	●	●
AC.L2-3.1.3	●	●	●	●	●
AC.L2-3.1.4	●	●	●	●	●
AC.L2-3.1.5	●	●	●	●	●
AC.L2-3.1.6	●	●	●	●	●
AC.L2-3.1.7	●	●	●	●	●
AC.L2-3.1.8	●	●	●	●	●
AC.L2-3.1.9	●	●	●	●	●
AC.L2-3.1.10	●	●	●	●	●
AC.L2-3.1.11	●	●	●	●	●



Category ↑↓

ID ↑↓

Responsibility ↑↓

Name ↑↓

I

⌵

⌵

⌵

☑ CMM Cv2 - Access Control

🔔 Access Control	AC.L1-3.1.1	Authorized Access Control
🔔 Access Control	AC.L1-3.1.2	Transaction & Function Control
🔔 Access Control	AC.L2-3.1.3	Control CUI Flow
🔔 Access Control	AC.L2-3.1.4	Separation of Duties
🔔 Access Control	AC.L2-3.1.5	Least Privilege

Remediation

POAM Date _____		Plan of Action and Milestones (POA&M)			
POAM #	Applicable Control(s)	Deficiency	Status	POAM	Assessor Guidance
1	3.1.1	Generic Accounts Exist	Not Implemented		On-Premise Active Directory and Group Policy should be used for user Authentication, Security Groups, Policies, and RBAC.
2	3.1.2	Limit System Access to Least Privilege	Not Implemented	Document user roles and Groups and Policies associated to those roles	On-Premise Active Directory and Group Policy should be used for user Authentication, Security Groups, Policies, and RBAC.
3	3.1.3	Control Flow of CUI Data with approval controls	Not Implemented	Identify Data and configure user access to only allow access to data according to their role(s)	File Server, storage folders, utilize Security Groups and Permission Shares. This permit only authorized users with roles that require access to the specific Data. Levels of access is determined and authorized by Information System Owner.
4	3.1.4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion	Partially Implemented	Document user roles and users associated to those roles. Verify all access is granted on a need to know basis.	All system resources are shared on a local file server, this should be connected to a domain controller (AD) with user roles and separation of duties, utilizing both system access group and data owner group memberships.
5	3.1.5	Employ the principle of least privilege, including for specific security functions and privileged accounts	Partially Implemented	Configure user roles according to user tasks and functions. No users should have administrative a	On-Premise Active Directory and Group Policy should be used for user Authentication, Security Groups, Policies, and RBAC.
6	3.1.6	Use non-privileged accounts or roles when accessing no security functions.	Partially Implemented	Verify only authorized users and only use administrative	
7	3.1.7	Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	Partially Implemented	Verify users and administ	accor
8	3.1.8	Limit unsuccessful login attempts.	Not Implemented	This is ODP (Org defined perm	an unsuccessful l
9	3.1.9	Provide privacy and security notices consistent with applicable CUI rules.	Not Implemented	Configure login banner with specific banners for Gov d	standard banner but for Ser
10	3.1.10	Use session lock with pattern-hiding displays to prevent access and viewing of data after a period of inactivity.	Not Implemented	Verify or configure a time	Verify st
11	3.1.11	Terminate (automatically) a user session after a defined condition.	Not Implemented	Verify or configure a time	
12	3.1.12	Monitor and control remote access sessions	Not Implemented		VI Remote Are connect

Compliance Framework Forecast: CMMCv2

None : 97
Implemented : 7
Partially Implemented : 0
Planned : 0
Alternative Implementation : 0
Not Applicable : 0



3rd Party Assessor – C3PAO

BECOMING A CMMC ASSESSOR

Are you qualified to become an assessor?

NO

Instead check out becoming a Registered Practitioner (RP) to build your CMMC Knowledge!

YES

In reviewing the CMMC Certified Professional (CCP) Blueprint you meet the recommended pre-requisites to start your assessor journey.

Begin Your Assessor Journey

1. Apply for Tier 3 background investigation.
2. Once your Tier 3 application and resume have been submitted, there will be no updates or visibility on where your application is in process. This can be a lengthy process and can take months for WHS to complete the investigation. Once the investigation is complete, you will be notified of your determination status.
3. Once you've successfully completed CCP training, passed the CCP exam, and earned a favorable Tier 3 determination you'll be considered "certified". As a CCP you can then participate on assessments working on a team with CCAs, assessing only Level 1 practices.

03 Complete and Submit DoD Tier 3 Application and Resume
Avg processing time 3-6 months

04 Train for CMMC Certified Assessor (CCA)
Avg training time 3.5 days

05 Take and Pass the CCA Exam
Avg testing time 3.4 hours

06 Met all DoD Requirements

YOU ARE NOW A DoD CMMC CERTIFIED ASSESSOR

Are you qualified to be a Lead CCA?

1. Hold an active certified CCA
2. Have five (5) years of cybersecurity experience
3. Have five (5) years of management experience
4. Have three (3) years of audit or assessment experience
5. Hold at least one active baseline certification from 8140.3, Job ID 612 at the Advanced Level

1. Start by finding an Approved Training Provider (ATP) from The Cyber AB Marketplace to train for CMMC Certified Professional (CCP) CyberAB > Directory

2. Successfully complete CCP training with a selected ATP. If you plan to take the CCP exam, you must obtain your CMMC Professional Number (CPN) by completing the CCP application process. CCP Candidate Application - CyberAB The ATP will submit your successful training completion using your CPN

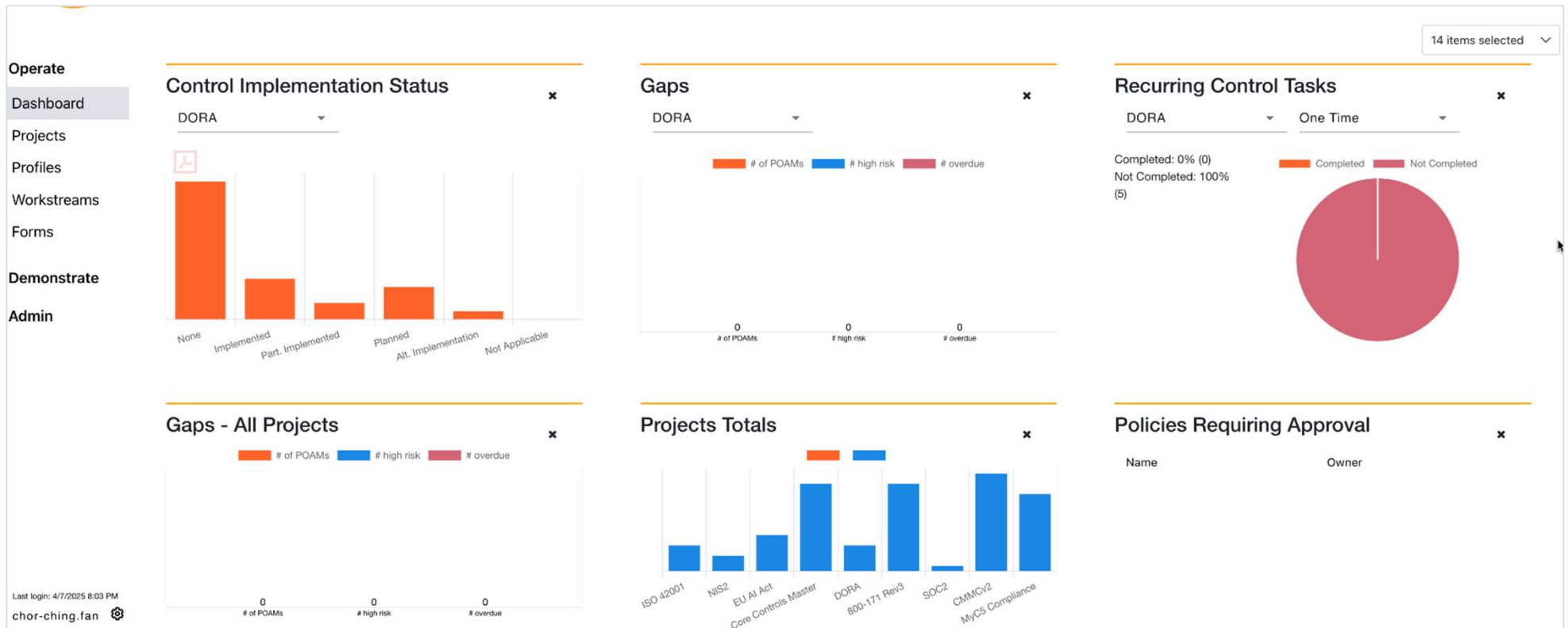
3. Highly recommend you take the DoD CUI Awareness Training DoD CUI Program > Training > DoD Training before starting your CCP training

1. Must have successfully completed CCP Training and passed CCP examination
2. Complete CCA Application Process CCA Registration | CyberAB (cyberab.org)
3. Find an Approved Training Provider (ATP) from The Cyber AB Marketplace to train for CMMC Certified Assessor (CCA) CyberAB > Directory
4. Successfully complete the CCA training with selected ATP The ATP will submit your successful training completion using your CPN

- DoD CMMC Certified Assessor Requirements:
1. Hold an active CCP Certification
 2. Hold an active Tier 3
 3. Hold a CCA Certification which also requires:
 - A. Three (3) years of cybersecurity experience
 - B. One (1) year of audit or assessment experience
 4. Hold at least one active baseline certification from 8140.3, Job ID 612 at either the Intermediate or Advanced Level



Continuous Monitoring & Reporting



Case Study



Manual Assessment – 20 users

- Audit required interviews and manual inputting of system, personnel, and CCI Generation.
- Audit to POAM: 3-4 months
- Remediation & upgrades: 8-13 months
- C3PAO Certification: 3 months
- Total 1.5 years
- Audit Cost: ~ \$60K

Semi-Automated Assessment

- Automated Scanning and system Mapping augments personnel and physical security mapping.
- Audit to POAM: 1 month
- Remediation & Upgrades: 6 months
- C3PAO Certification: 1 month
- Total 8 Months
- Audit + Continuous Compliance ~ \$30K

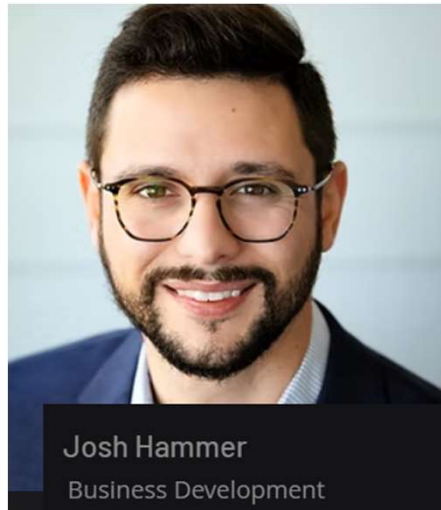
REMEDATION COST VARY WIDELY FROM \$10K'S TO \$100K

Q&A / Discussion

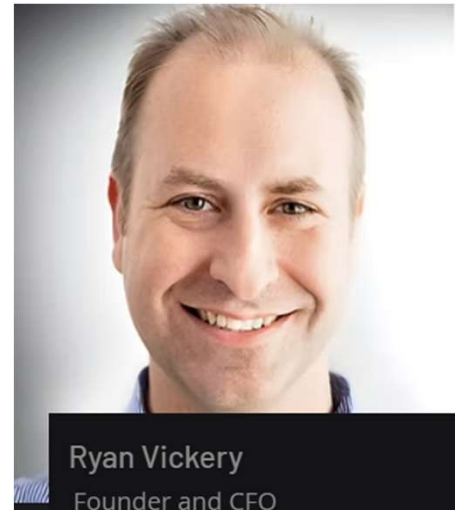




Contact Us



Mr. Josh Hammer
jhammer@hvfsusa.com
352-467-9699



Mr. Ryan Vickery
rvickery@hvfsusa.com
904-234-4123