Accelerating CMMC Compliance with Amazon Web Services, Coalfire Federal & PreVeil

September 14, 2021

Panelists

Stuart Itkin
VP Coalfire Federal

Ted Steffan
Sr. Security Partner Strategist
Amazon Web Services

Sanjeev Verma
Co-founder @PreVeil

COALFIRE FEDERAL

aws

PREVEIL

About Coalfire Federal

Coalfire Federal provides cybersecurity services to government and commercial organizations helping them protect their mission-specific cyber objectives.

Coalfire Federal is the leading FedRAMP 3PAO, a CMMC C3PAO and CMMC RPO and offers a full spectrum of cybersecurity risk management and compliance services.

About Stuart Itkin

- Coalfire Federal VP CMMC and FedRAMP Assurance
- Previously VP Product Management and Marketing at Exostar, Global CMO at CEB
- Executive roles in several cybersecurity businesses
- Lead mentor at MACH 37 cyber product accelerator

COALFIRE FEDERAL

About Amazon Web Services

Since 2006, Amazon Web Services (AWS) has offered IT infrastructure services to businesses in the form of cloud computing. Today, Amazon Web Services provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world.

About Ted Steffan

- Sr. Security Partner Strategist at AWS
- Created Amazon's Authority to Operate program
- Coordinates AWS team focused on helping national security and defense customers who work on CMMC
- 26 years in the US Air Force

About PreVeil

PreVeil is a simple, inexpensive and secure SaaS platform for storing and sharing CUI and ITAR data in email and files.

Designed for the enterprise, PreVeil is used by leading defense contractors for CMMC compliance, Supply Chain Collaboration and Incident Response.

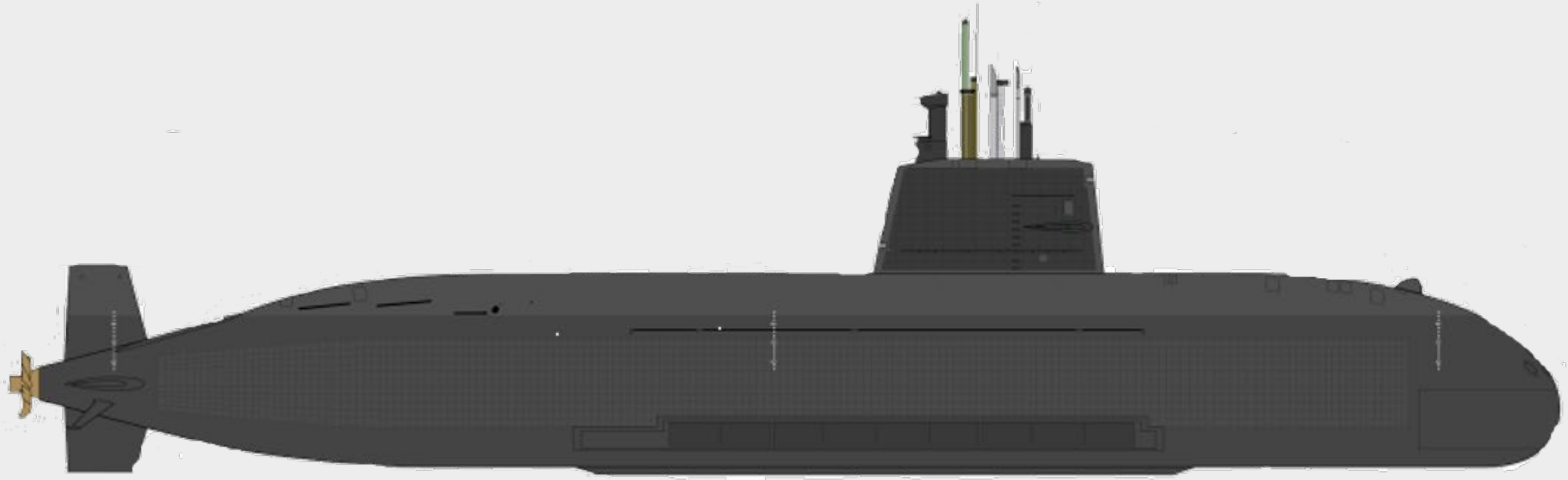
About Sanjeev Verma

- Co-founder & Chairman @ PreVeil since 2015
- Previously, co-founder Airvana
- Business leadership roles, Motorola
- MBA, MIT Sloan School of Management
- BS Electrical Engineering, Delhi College of Eng.

PREVEIL

Coalfire Federal

Why CMMC is important has to do with submarines



Alan Turing and Why CMMC is Important

Broke German Enigma code in 1943

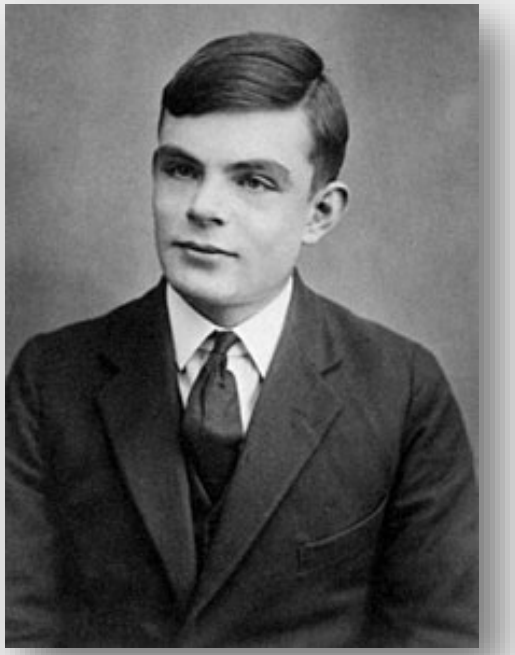
- Decoded >84,000 secret messages/month
- Protected North Atlantic merchant convoys

Credited with saving > 21 million lives

- Accelerated the end of WWII

Educated at Princeton University:

- English mathematician
- Computer scientist
- Logician
- Cryptanalyst
- Philosopher
- Theoretical biologist



- Alan Mathison Turing OBE FRS
- (June 1912 – June 1954)

Alan Turing and Why CMMC is Important

- Sea Dragon – June 2018
  614 gigabytes of data stolen by the Chinese
  - Undersea warfare data
  - Plans for a submarine-based, supersonic anti-ship missile
  - Sensor and cryptographic information
  - Navy submarine development unit's electronic warfare library

- Lockheed F35 Strike Fighter
  - Almost a decade to develop
  - Total program cost > $1 Trillion
  - Chinese J-31 introduced within 2 years
  - Based on CUI stolen from U.S. defense

Motivations for CMMC

- CMMC is designed to enhance the protection of CUI and FCI in the DoD supply chain
- *(NIST 800-171 was not effective)*

  - Compliance is not security
  - Promising to implement security and implementing security are not equal
  - Allowing POAMs disadvantages those that are secure
  - Allowing companies to grade their own tests was not a good idea

How has CMMC improved on NIST 800-171?

- Combines various cybersecurity standards and best practices
- CMMC looks at maturity, it's no longer about compliance
- CMMC requires third party assessment, no more self-grading and self-reporting
- Requirements are pass-fail, requirements must be satisfied, not just addressed
- Not one size fits all: 5 Maturity Levels based on information exchanged

What Makes CMMC Challenging?

It's about protecting Controlled Unclassified Information, not systems.

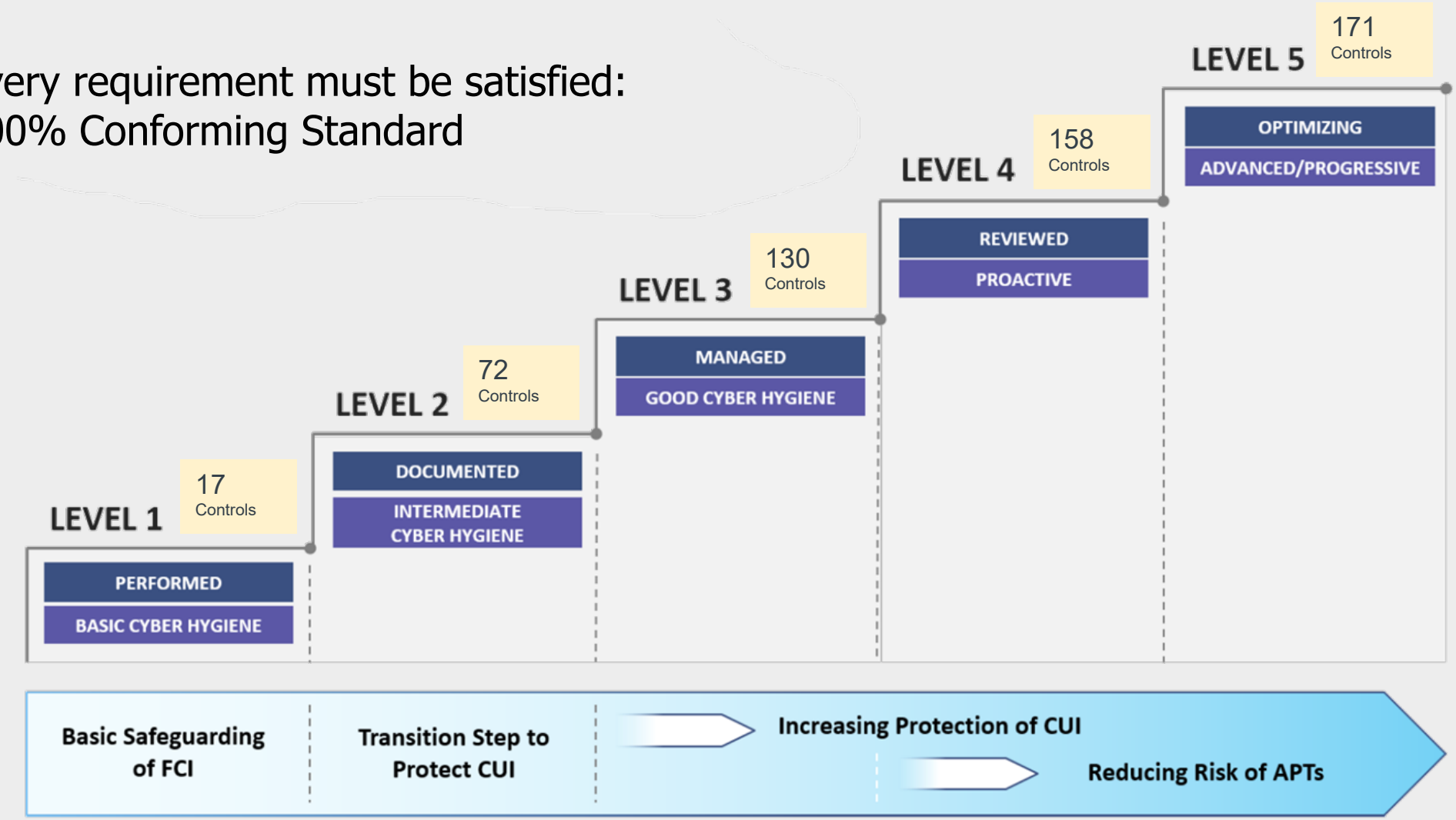
- Step 1 is finding and identifying the CUI that needs to be protected
- Step 2 is isolating and protecting CUI and controlling access

- This can be expensive.
  Estimated average compliance related technology expenditure:

		One-Time	Recurring
ENT	ML3	$166,667	$333,333
SMB	ML3	$58,333	$116,667

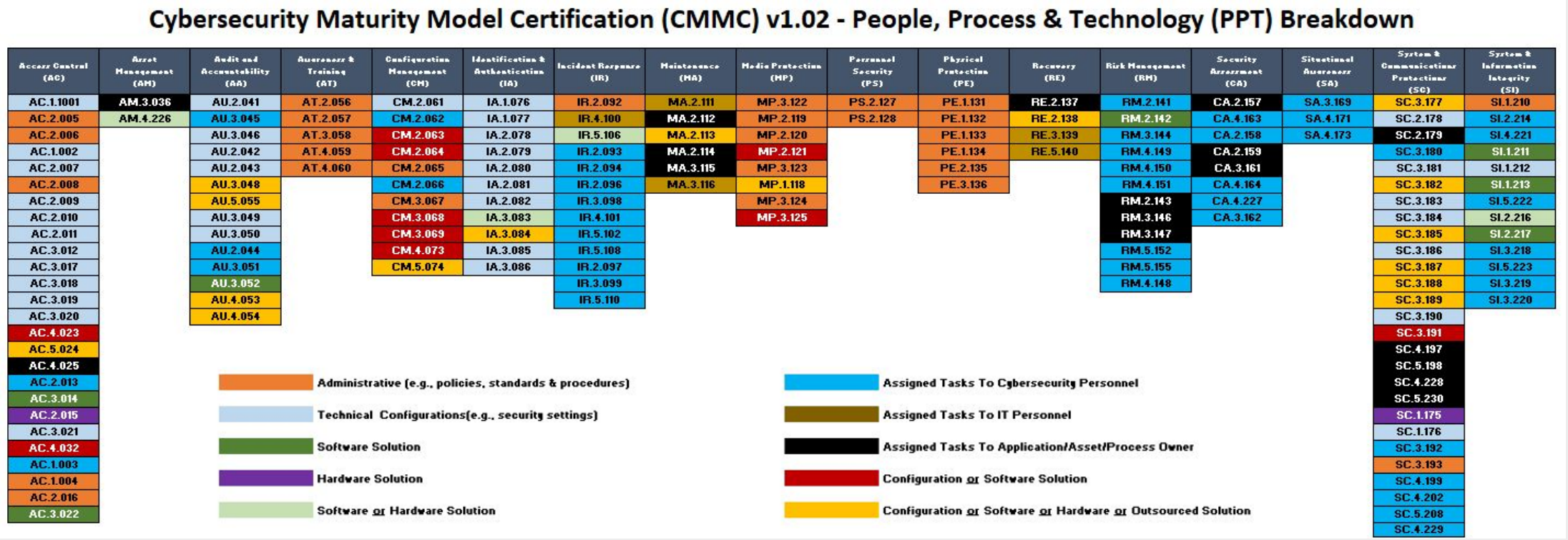
CMMC is a 100% Conforming Standard

Every requirement must be satisfied:
100% Conforming Standard



COALFIRE FEDERAL aws PREVEIL

CMMC Practices and Requirements



ComplianceForge

Every requirement must be fully Documented and supported with Objective Evidence.

COALFIRE FEDERAL aws PREVEIL

CMMC Requirements are Exacting

Cybersecurity Maturity Model Certification (CMMC) v1.02 - People, Process & Technology (PPT) Breakdown

Access Control (AC)	Asset Management (AM)	Audit and Accountability (AA)	Awareness & Training (AT)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	System & Communications Protection (SC)	System & Information Integrity (SI)
AC.1.1001	AM.3.036	AU.2.041	AT.2.056	CM.2.061	IA.1.076	IR.2.092	MA.2.111	MP.3.122	PS.2.127	PE.1.131	RE.2.137	RM.2.141	CA.2.157	SA.3.169	SC.3.177	SI.1.210
AC.2.005	AM.4.226	AU.3.045	AT.2.057	CM.2.062	IA.1.077	IR.4.100	MA.2.112	MP.2.119	PS.2.128	PE.1.132	RE.2.138	RM.2.142	CA.4.163	SA.4.171	SC.2.178	SI.2.214
AC.2.006		AU.3.046	AT.3.058	CM.2.063	IA.2.078	IR.5.106	MA.2.113	MP.2.120		PE.1.133	RE.3.139	RM.3.144	CA.2.158	SA.4.173	SC.2.179	SI.4.221
AC.1.002		AU.2.042	AT.4.059	CM.2.064	IA.2.079	IR.2.093	MA.2.114	MP.2.121		PE.1.134	RE.5.140	RM.4.149	CA.2.159		SC.3.180	SI.1.211
AC.2.007		AU.2.043	AT.4.060	CM.2.065	IA.2.080	IR.2.094	MA.3.115	MP.3.123		PE.2.135		RM.4.150	CA.3.161		SC.3.181	SI.1.212
AC.2.008		AU.3.048		CM.2.066	IA.2.081	IR.2.096	MA.3.116	MP.1.118		PE.3.136		RM.4.151	CA.4.164		SC.3.182	SI.1.213
AC.2.009		AU.5.055		CM.3.067	IA.2.082	IR.3.098		MP.3.124				RM.2.143	CA.4.227		SC.3.183	SI.5.222
AC.2.010		AU.3.049		CM.3.068	IA.3.083	IR.4.101		MP.3.125				RM.3.146	CA.3.162		SC.3.184	SI.2.216
AC.2.011		AU.3.050		CM.3.069	IA.3.084	IR.5.102						RM.3.147			SC.3.185	SI.2.217
AC.3.012		AU.2.044		CM.4.073	IA.3.085	IR.5.108						RM.5.152			SC.3.186	SI.3.218
AC.3.017		AU.3.051		CM.5.074	IA.3.086	IR.2.097						RM.5.155			SC.3.187	SI.5.223
AC.3.018		AU.3.052				IR.3.099						RM.4.148			SC.3.188	SI.3.219
AC.3.019		AU.4.053				IR.5.110									SC.3.189	SI.3.220
AC.3.020		AU.4.054													SC.3.190	
AC.4.023															SC.3.191	
AC.5.024															SC.4.197	
AC.4.025															SC.5.198	
AC.2.013															SC.4.228	
AC.3.014															SC.5.230	
AC.2.015															SC.1.175	
AC.3.021															SC.1.176	
AC.4.032															SC.3.192	
AC.1.003															SC.3.193	
AC.1.004															SC.4.199	
AC.2.016															SC.4.202	
AC.3.022															SC.5.208	
															SC.4.229	

AC.1.001 "*Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).*"

ASSESSMENT OBJECTIVE

Determine if:	
AC.1.001[a]	Authorized users are identified.
AC.1.001[b]	Processes acting on behalf of authorized users are identified.
AC.1.001[c]	Devices (and other systems) authorized to connect to the system are identified.
AC.1.001[d]	System access is limited to authorized users.
AC.1.001[e]	System access is limited to processes acting on behalf of authorized users.
AC.1.001[f]	System access is limited to authorized devices (including other systems).

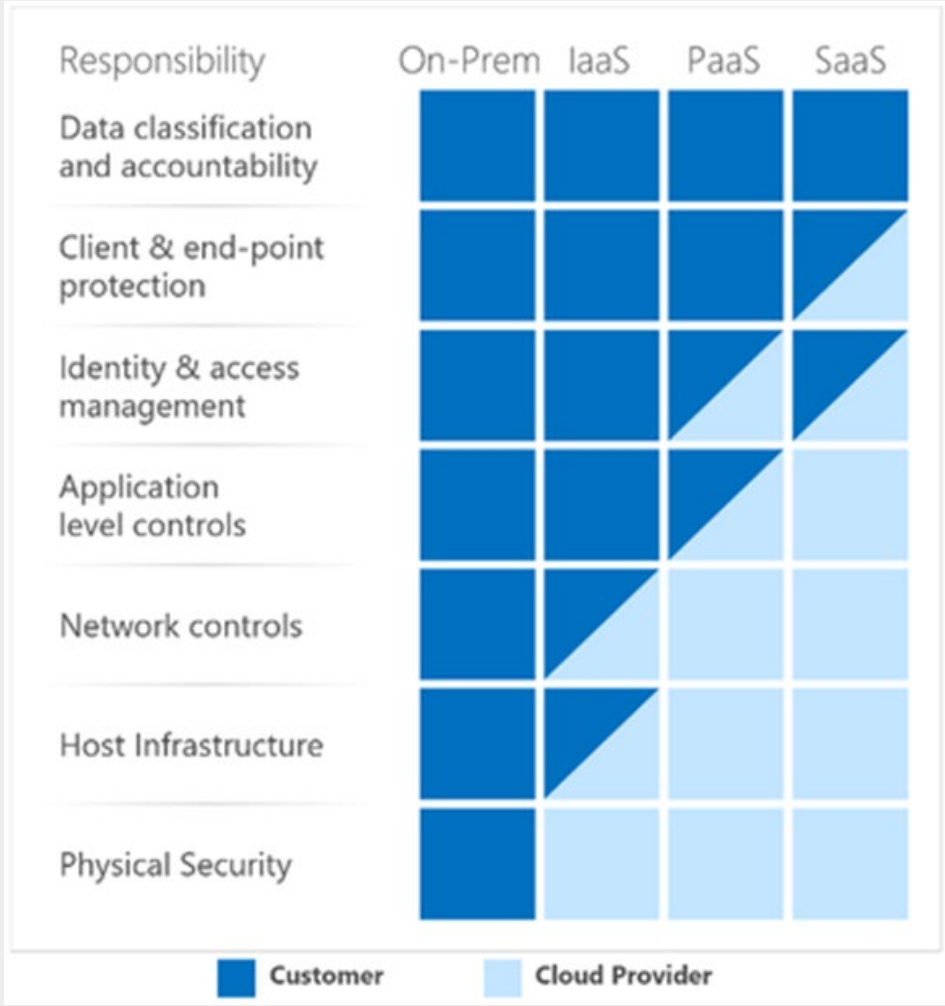
Every requirement must be:

- Satisfied
- Documented: SSP, Policy, Procedure
- Corroborated: evidence/artifacts
- Mature

COALFIRE FEDERAL aws PREVEIL

Minimizing Cost, Risk, and Time

1. Engage an Advisor:
   - A qualified, experienced RPO who knows the journey
2. Use an established, proven blueprint:
   - A reference architecture
3. Share the responsibility:
   - Leverage Cloud Services



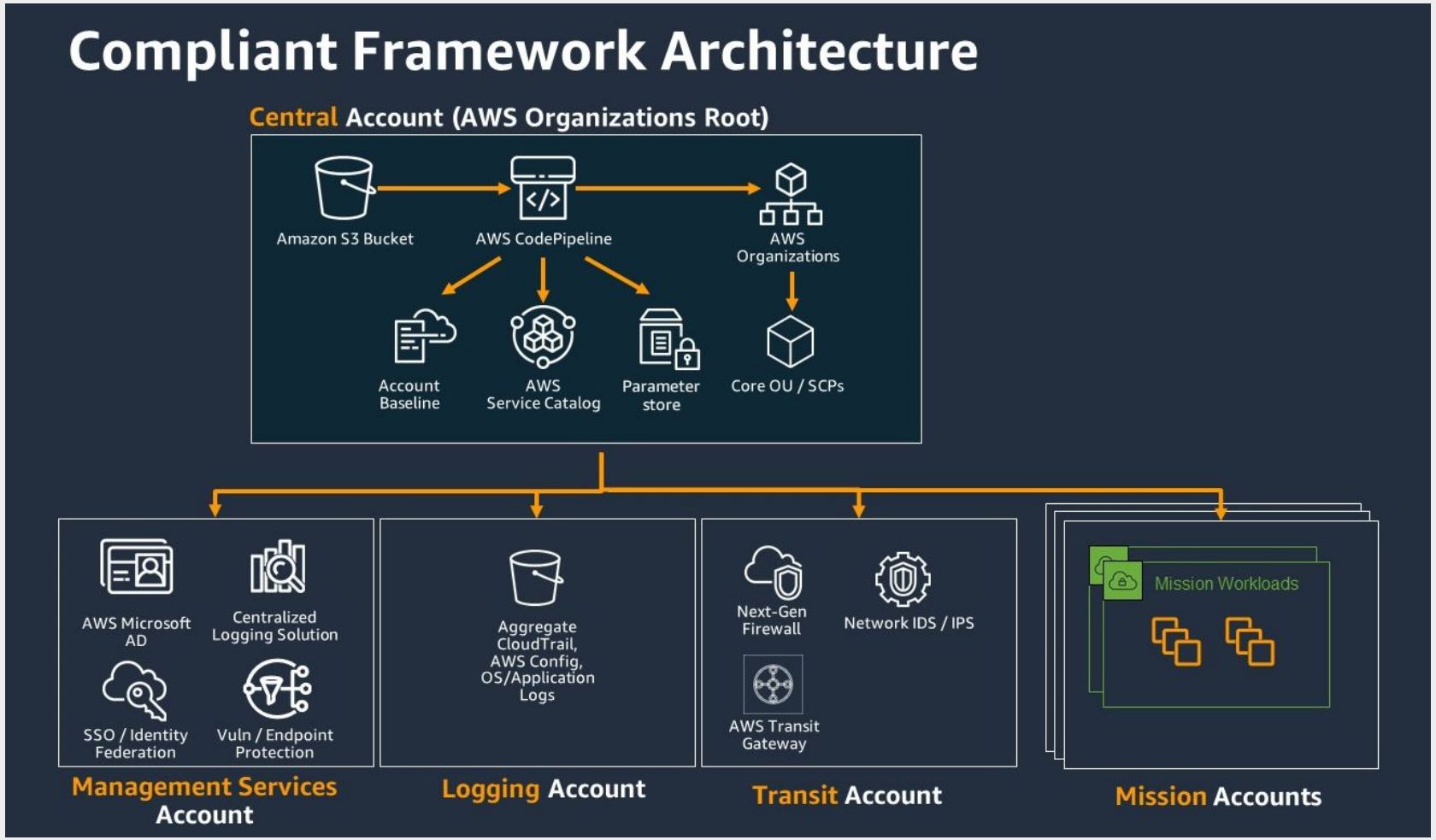
Amazon Web Services

AWS GovCloud (US)

- GovCloud designed to handle ITAR (International Traffic in Arms Regulation)
  - JAB Provisional Authorization at the FedRAMP High Impact level
  - Community Cloud: access controlled, US Citizens for physical and logical access to the AWS infrastructure
- Separate Isolated Credential Database
- Physically Isolated Regions East/West (Oregon & Ohio)
- 3 Availability Zones per Region
- Logical Network Isolation – all users run in VPCs
- FIPS 140-2 Validated Hardware & Cryptographic Services for VPNs and AWS Service API End Points
- Service(s) are only deployed into the Region based on customer demand

Offers the same high level of security as the other AWS Regions. Access is restricted to customers who are US Persons, not subject to export restrictions, and who comply with US export control laws and regulations, including the International Traffic in Arms Regulations (ITAR).

AWS Compliant Framework

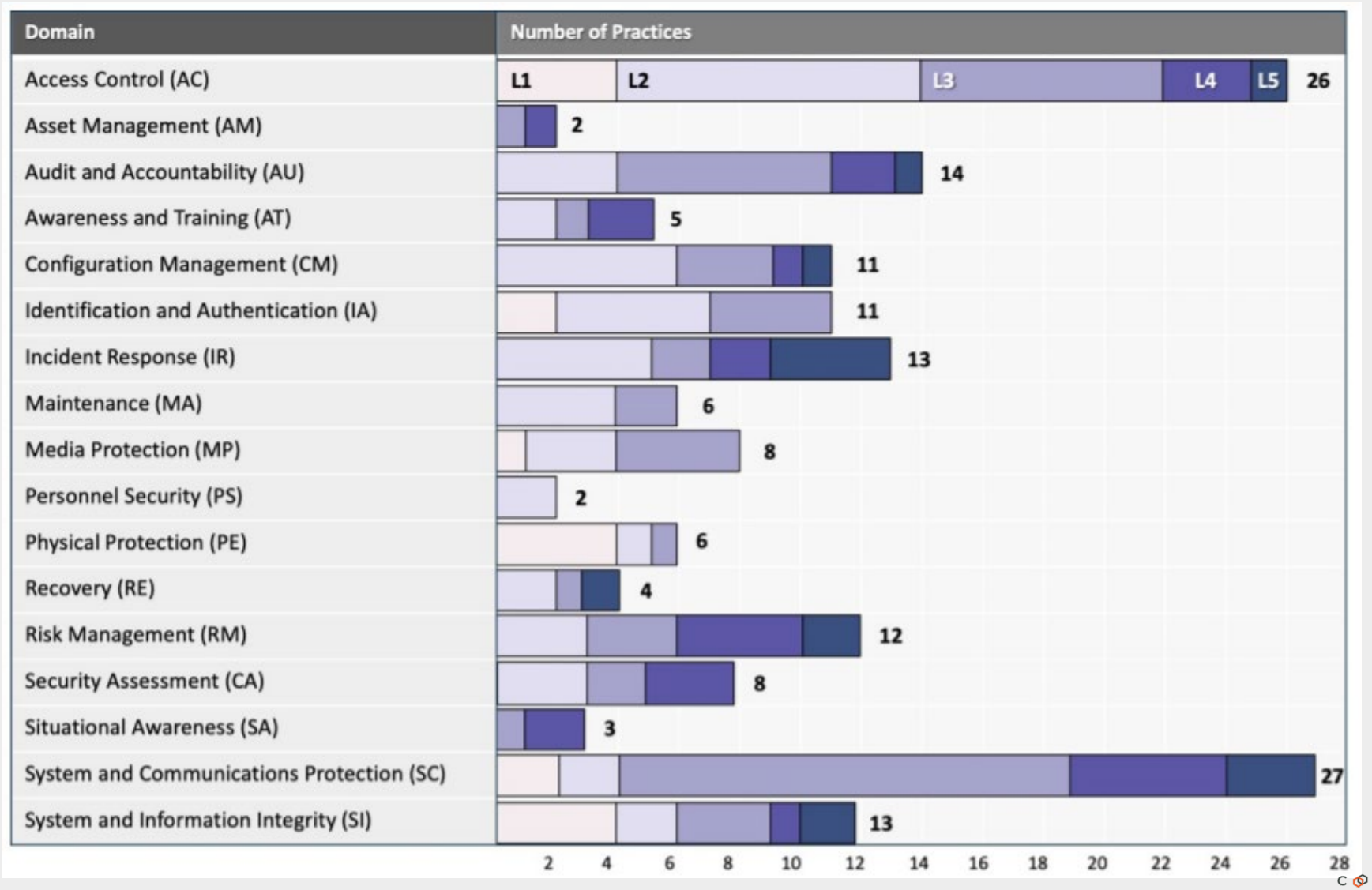


AWS Compliant Framework

1. Fully automated infrastructure as code including account structure and networking
    1. Automation solutions such as AWS CloudFormation and the AWS Cloud Development Kit (AWS CDK)
    2. Deploys an account structure that meets CMMC requirements
2. Aggregation of AWS environment logs for security information and event management (SIEM) integration
    1. Includes a logging account to provide centralized and immutable logs
    2. Log data is collected in Amazon S3
3. Continuous auditing using AWS security services
    1. In addition to AWS CloudTrail and AWS Config additional AWS services are enabled in all accounts
4. Extensibility plug in architecture
    1. All automation inputs/outputs are stored in the AWS Systems Manager Parameter Store
    2. Allows customers to access and modify information about deployed resources
    3. Codebase that is fully available as an open source project hosted on GitHub

COALFIRE FEDERAL aws PREVEIL

Inheriting CMMC Practices



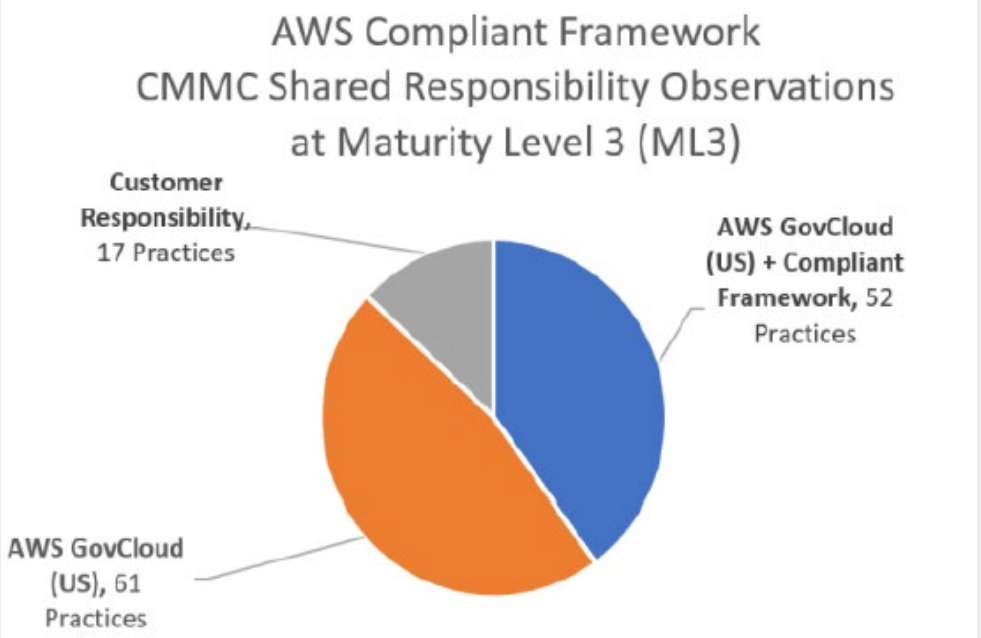
Inheriting CMMC Practices (from AWS FedRAMP pATO)

Based on a review conducted by Coalfire, there are many of the 130 CMMC Level 3 Practices that could be inherited from AWS

- 61 inherited from AWS
- 52 that are Shared between AWS and the Customer
- 17 that are fully Customer Responsibility

Details of this review is located in the AWS service Artifact under the CMMC Customer Package

NOTE – Practices can only be inherited for the organizations that run in AWS. Any system component that is external to AWS will have to be documented and tested as part of the accreditation process



Inheriting CMMC Practices (from AWS FedRAMP pATO)

Inherited CMMC Practices – Examples of practices that a customer can inherit from AWS IaaS, PaaS, and SaaS

- Maintenance (MA)
  - Hardware maintenance is the responsibility of AWS
- Media Protection (MP)
  - Media sanitization is the responsibility of AWS
- Physical Protection (PE)
  - Physical security of the data centers is the responsibility of AWS

Inheriting CMMC Practices (from AWS FedRAMP pATO)

Shared CMMC Practices – Practices that customers and AWS have responsibility for (examples)

- Patch Management
  - AWS is responsible for patching and fixing flaws within the infrastructure, but customers are responsible for patching their guest operating system (OS) and applications.
- Configuration Management
  - AWS maintains the configuration of its infrastructure devices, but a customer is responsible for configuring their own guest operating systems, databases, and applications.
- Awareness and Training
  - AWS trains AWS employees, but a customer must train their own employees.

Inheriting CMMC Practices (from AWS FedRAMP pATO)

Customer Specific CMMC Practices – Practices that are solely the responsibility of the customer (examples)

- Service and Communications Protection or Zone Security
  - Customers may be required to route or zone data within specific security environments


PREVEIL

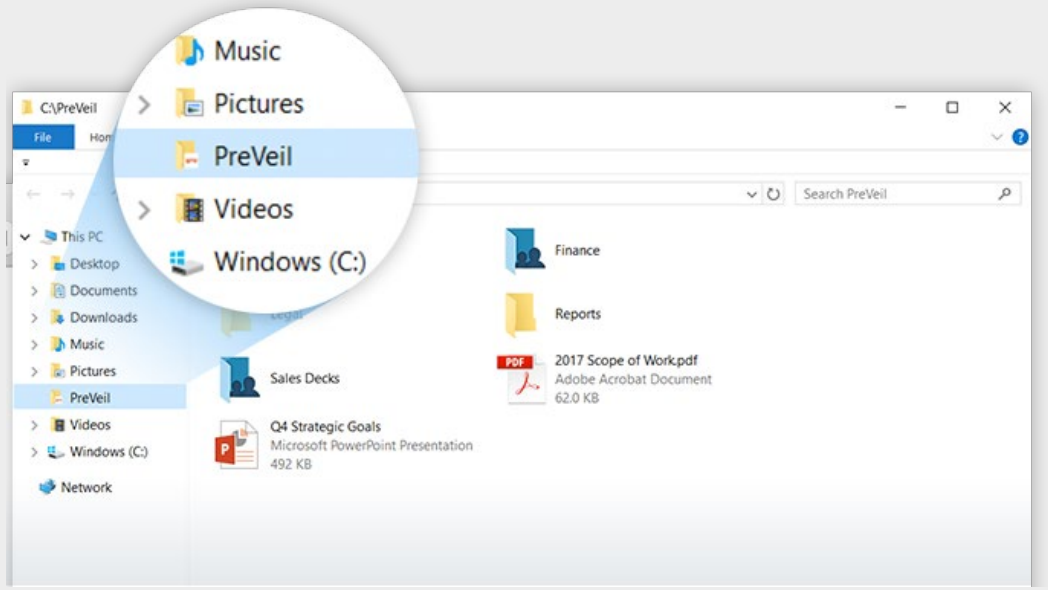
CMMC: Secure & Compliant Storing and Sharing of CUI

Simple. Secure. Inexpensive. Compliant.

PreVeil Encrypted Email & Document Collaboration

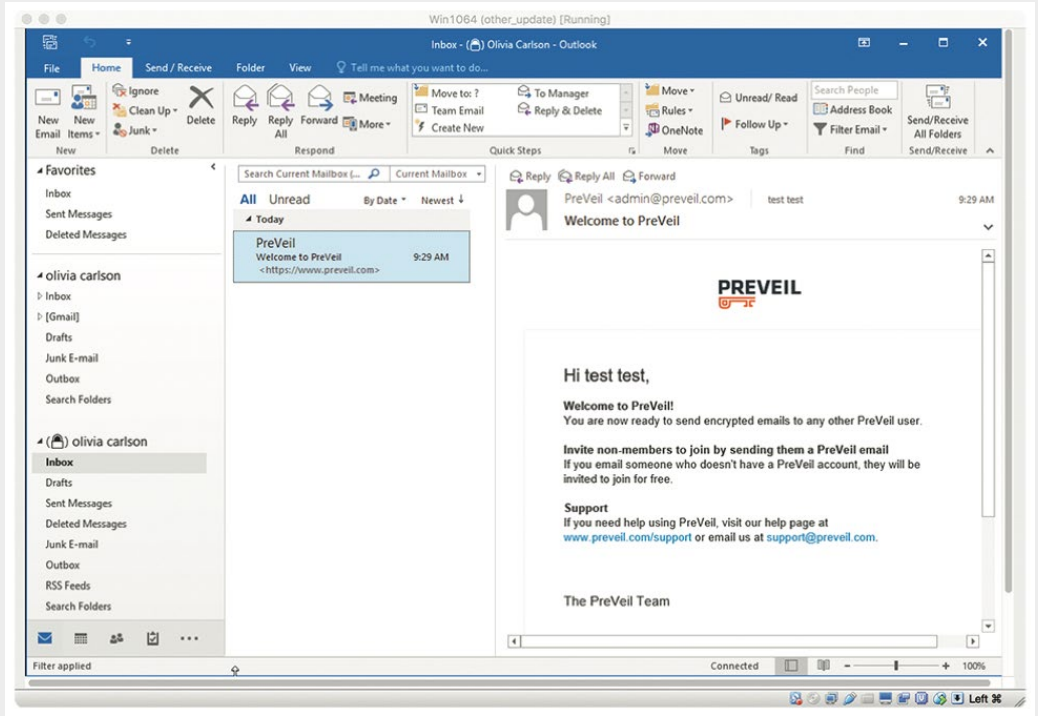
PreVeil Drive & Mail

Document Collaboration



Integrated with file system (File Explorer/Mac Finder)

Encrypted Messaging



Works with Outlook & GMail

COALFIRE FEDERAL aws PREVEIL

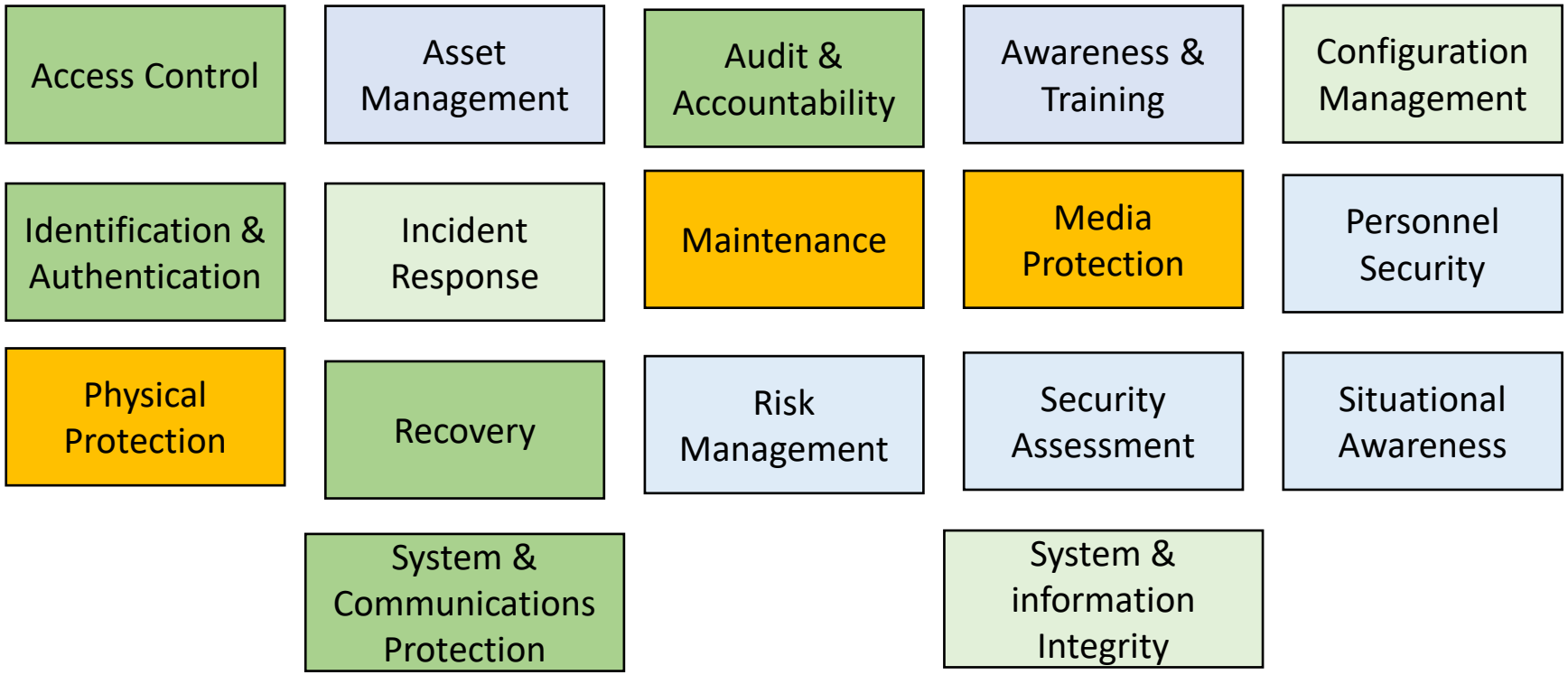
PreVeil for Simplified CMMC Compliance

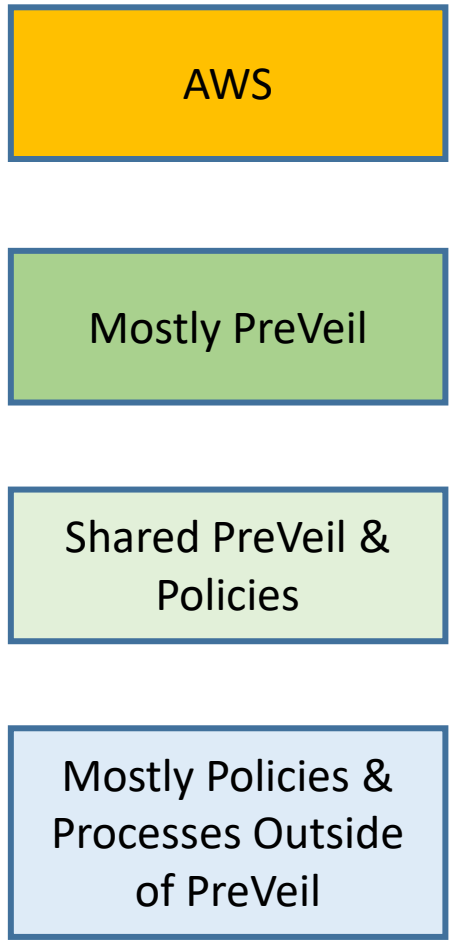
17 CMMC Domains / 130 Cyber Practices

Access Control	Asset Management	Audit & Accountability	Awareness & Training	Configuration Management
Identification & Authentication	Incident Response	Maintenance	Media Protection	Personnel Security
Physical Protection	Recovery	Risk Management	Security Assessment	Situational Awareness
	System & Communications Protection		System & information Integrity	

PreVeil + Policies + AWS => CMMC Compliance

The 17 CMMC Domains





PreVeil Compliance Basics

FedRAMP Baseline Moderate Equivalent

All PreVeil Data is Stored on AWS Gov Cloud FedRAMP High

FIPS 140-2 Validated Encryption

DFARS 7012 c-g compliant

Supports ITAR and NIST 800-171 Compliance

PreVeil Compliance Documentation

PreVeil CMMC Documentation for SSP

Simplifying Compliance

Provides a strong foundation for CMMC SSP and Policy Documents

200+ Pages

Created by 3rd Party CMMC Compliance Experts

Still needs a strong CMMC advisor

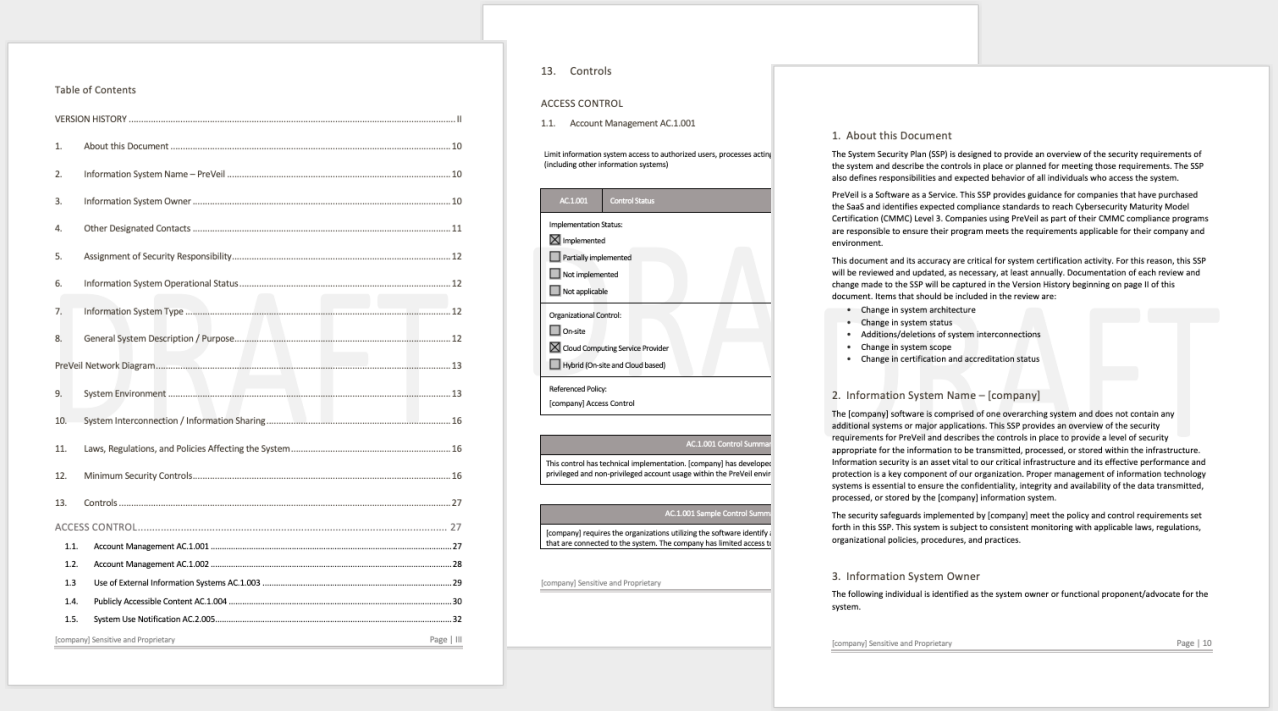


Table of Contents

[company] Sensitive and Proprietary Page | III

13. Controls

ACCESS CONTROL

1.1. Account Management AC.1.001

Limit information system access to authorized users, processes acting (including other information systems)

AC.1.001	Control Status

Implementation Status:
- [x] Implemented
- [ ] Partially implemented
- [ ] Not implemented
- [ ] Not applicable

Organizational Control:
- [ ] On-site
- [x] Cloud Computing Service Provider
- [ ] Hybrid (On-site and Cloud based)

Referenced Policy:
[company] Access Control

AC.1.001 Control Summar

This control has technical implementation. [company] has developec privileged and non-privileged account usage within the PreVeil envir

AC.1.001 Sample Control Summ

[company] requires the organizations utilizing the software identify that are connected to the system. The company has limited access t

[company] Sensitive and Proprietary

1. About this Document

The System Security Plan (SSP) is designed to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The SSP also defines responsibilities and expected behavior of all individuals who access the system.

PreVeil is a Software as a Service. This SSP provides guidance for companies that have purchased the SaaS and identifies expected compliance standards to reach Cybersecurity Maturity Model Certification (CMMC) Level 3. Companies using PreVeil as part of their CMMC compliance programs are responsible to ensure their program meets the requirements applicable for their company and environment.

This document and its accuracy are critical for system certification activity. For this reason, this SSP will be reviewed and updated, as necessary, at least annually. Documentation of each review and change made to the SSP will be captured in the Version History beginning on page II of this document. Items that should be included in the review are:

- Change in system architecture
- Change in system status
- Additions/deletions of system interconnections
- Change in system scope
- Change in certification and accreditation status

2. Information System Name – [company]

The [company] software is comprised of one overarching system and does not contain any additional systems or major applications. This SSP provides an overview of the security requirements for PreVeil and describes the controls in place to provide a level of security appropriate for the information to be transmitted, processed, or stored within the infrastructure. Information security is an asset vital to our critical infrastructure and its effective performance and protection is a key component of our organization. Proper management of information technology systems is essential to ensure the confidentiality, integrity and availability of the data transmitted, processed, or stored by the [company] information system.

The security safeguards implemented by [company] meet the policy and control requirements set forth in this SSP. This system is subject to consistent monitoring with applicable laws, regulations, organizational policies, procedures, and practices.

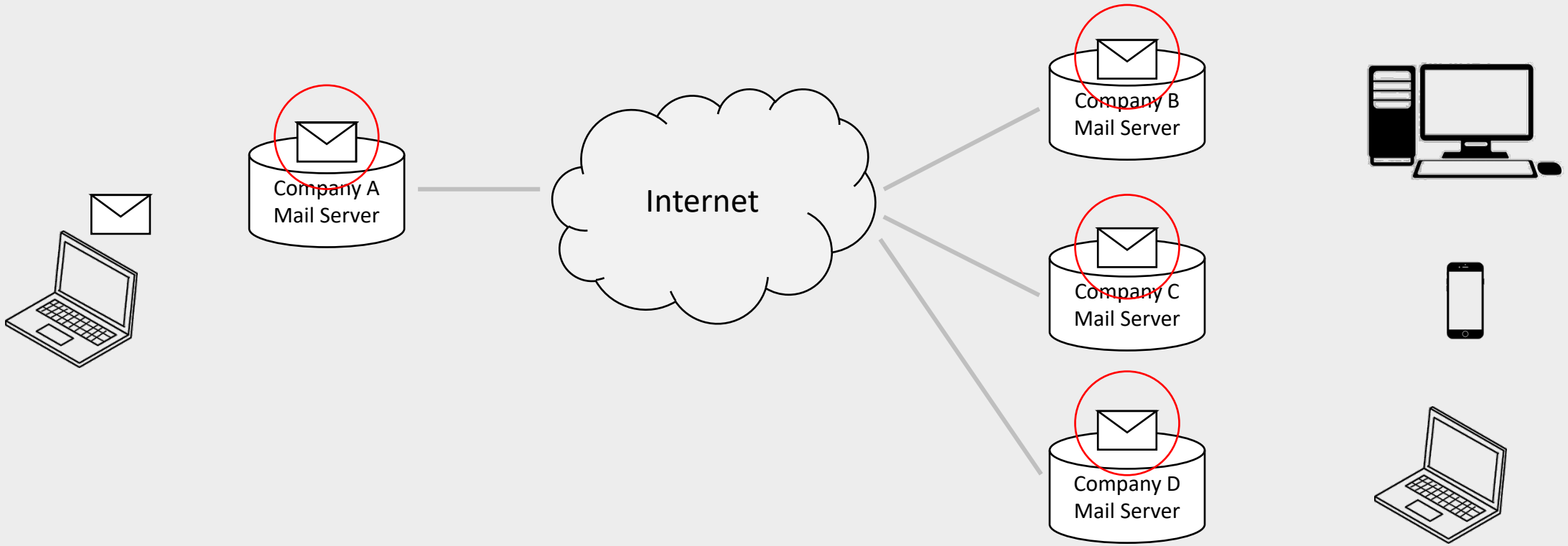
3. Information System Owner

The following individual is identified as the system owner or functional proponent/advocate for the system.

[company] Sensitive and Proprietary Page | 10

Zero Trust Data Security for CUI

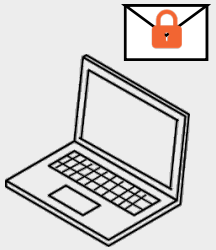
CUI on Traditional Mail Servers



In Traditional Systems, like GCC High, O365, GSuite the Server can see Unencrypted data
So can the attacker

End-to-end Encryption

Encrypt



Company A

AWS GovCloud

Company B

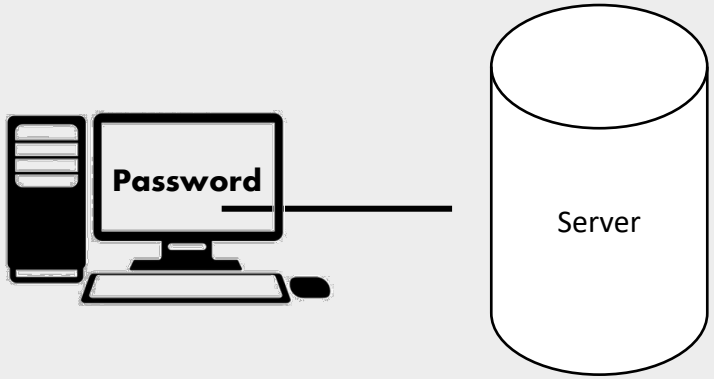
Decrypt

Company C

Company D

Eliminate Password Vulnerabilities with Keys

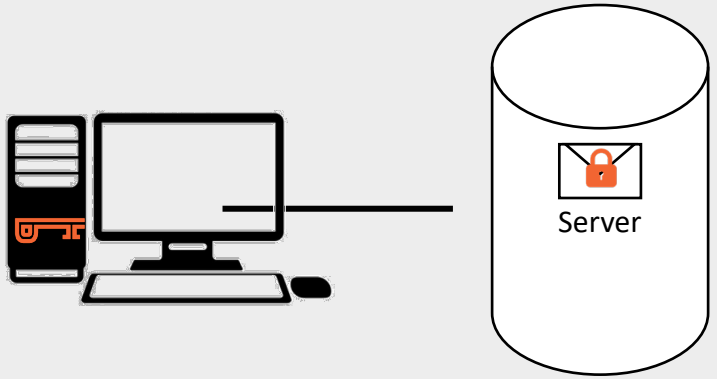
Traditional System



Attacker obtaining password can log in remotely

Attacker

PreVeil



Unguessable Key stored on device required for decryption and user authentication

Attacker can not log in remotely

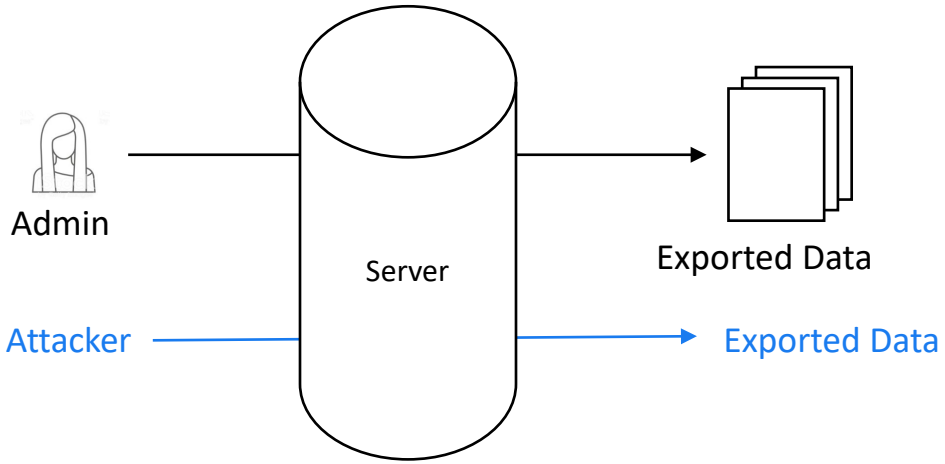
Reduce Administrative Vulnerabilities

Traditional System

Any admin can perform sensitive operations:

- Reset passwords
- Export data
- Delete users

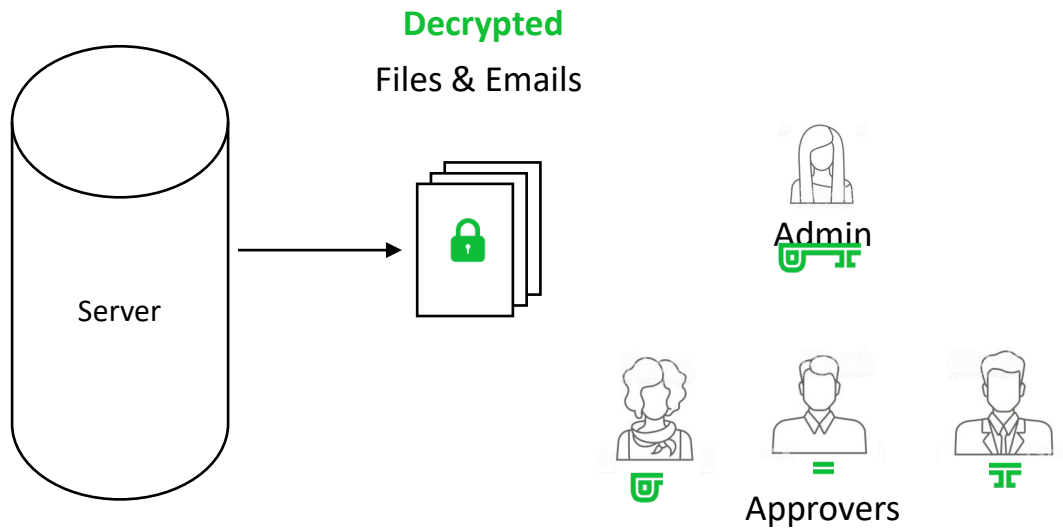
And so can an attacker



PreVeil

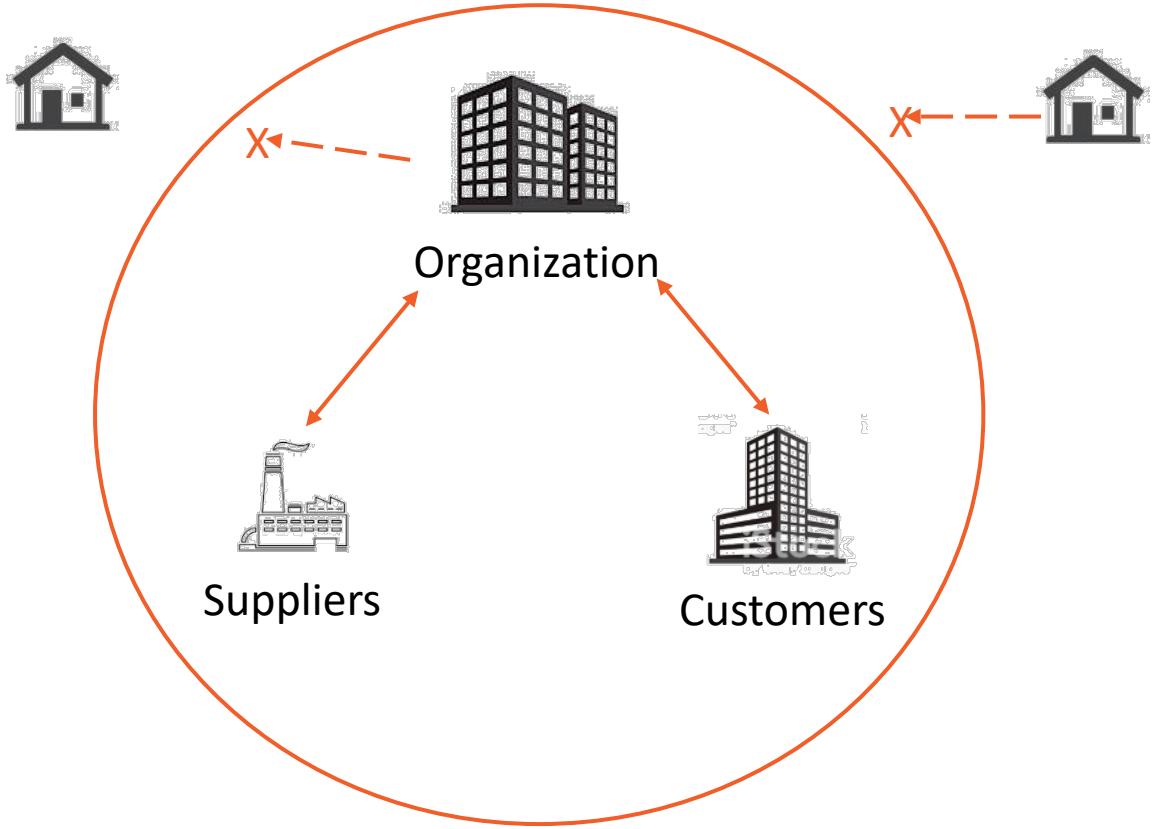
Admins can perform sensitive functions only with after being authorized by an “approval group.”

Example — Exporting Data:



COALFIRE FEDERAL aws PREVEIL

Restrict CUI Access to Trusted Communities



Simple to Deploy and Use

Leverages power of AWS GovCloud (US)

Retain your O365 and GSuite

Simple, Quick Deployment

- No Rip and Replace
- No Changes to Existing

Q&A

COALFIRE FEDERAL

coalfirefederal.com

Stuart.itkin@coalfirefederal.com

603-892-0538

aws

aws.com

steffat@amazon.com

239.470.5187

PREVEIL

preveil.com

sanjeev@preveil.com

857-353-6480