Simplify, CMMC, DFARS[NIST 800-171], ITAR Compliance on AWS Gov Cloud

COMPLYUP
Assessment Platform

aws

PreVeil

PC-WARRIORS

Agenda

Preparing for Assessment

AWS Gov Cloud Platform

Ted Steffan, AWS

Platform to Store, Share CUI, Documentation

PreVeil

Platform to build SSP, Compute SPRS Score

Matt Majot, ComplyUp

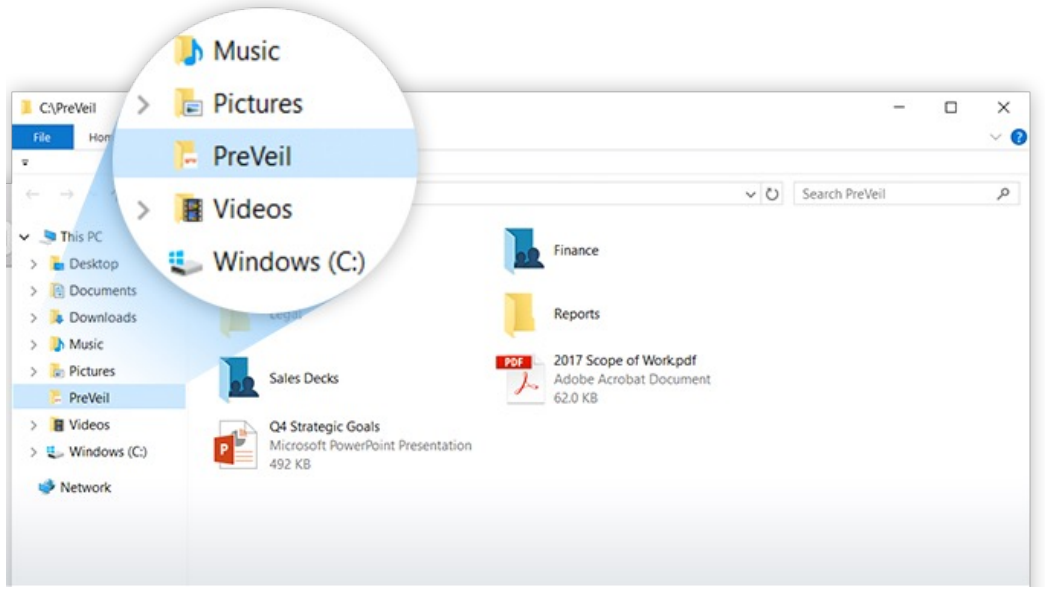
Getting Organization Fully Ready for Assessment

Jose Neto PC Warriors

The focus of CMMC, DFARS, ITAR is Protecting CUI

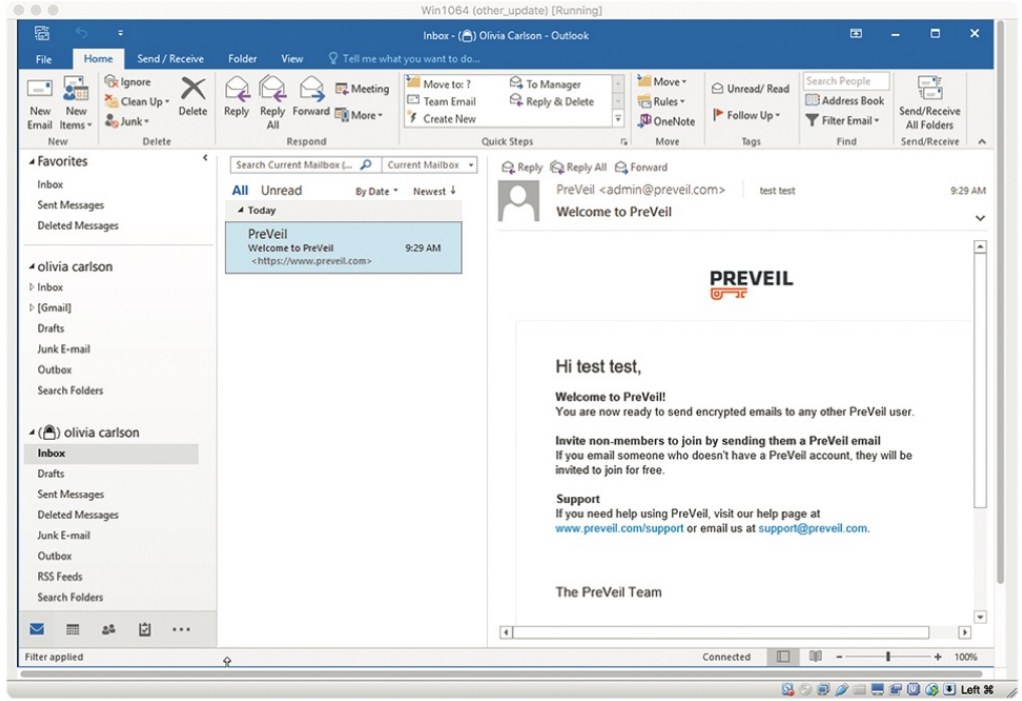
PreVeil Encrypted Cloud Drive & Mail

Encrypted Document Collaboration



Encrypted Cloud File Storage, Sync, and Collaboration
Ransomware Proof

Encrypted Messaging



Works with Outlook & Gmail, **using existing email address**

NIST 800-171, CMMC Compliance

Achieved 110/110 NIST 800-171 in DIBCAC Audit

Demonstrates CMMC Level 2 (Advanced)
PreVeil Addresses 84/110 Controls

Cloud Platform on AWS Gov Cloud

FedRAMP Baseline Moderate Equivalent
FIPS 140-2 Validated Encryption
DFARS 7012 (c-g) Compliant

PreVeil CMMC Documentation for SSP

Simplifies 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

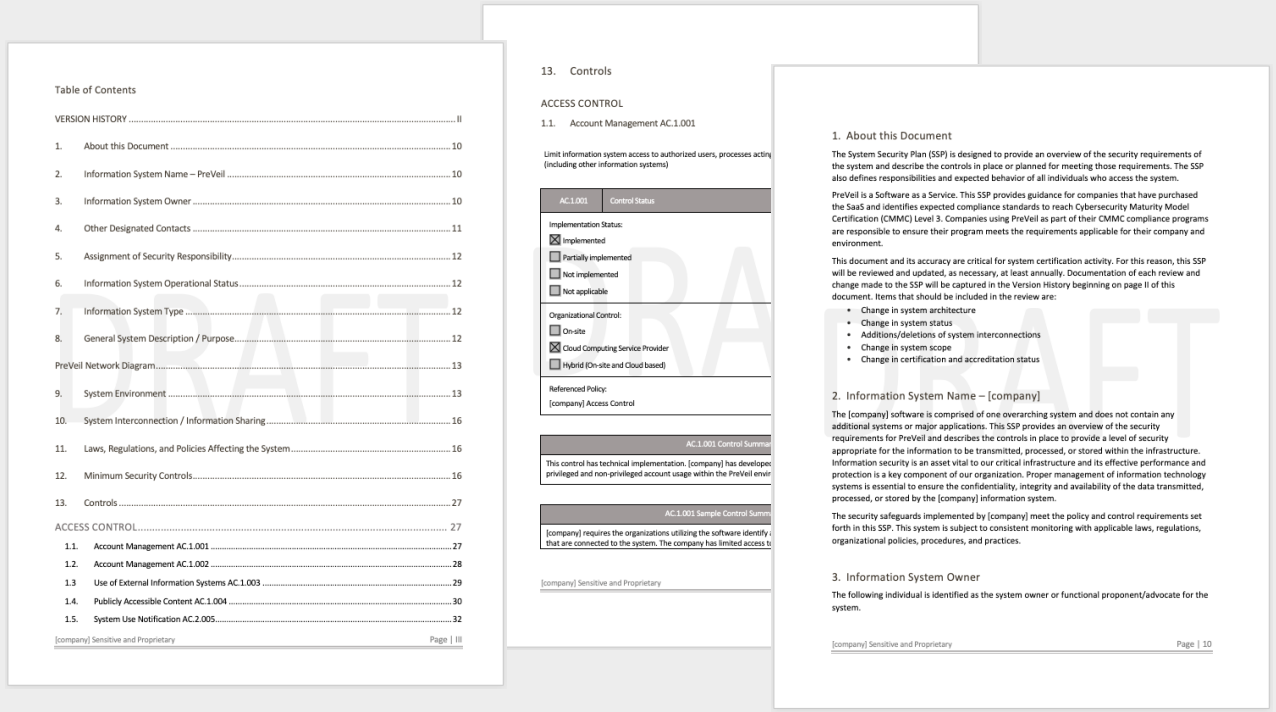


Table of Contents

VERSION HISTORY II

1. About this Document 10
2. Information System Name – PreVeil 10
3. Information System Owner 10
4. Other Designated Contacts 11
5. Assignment of Security Responsibility 12
6. Information System Operational Status 12
7. Information System Type 12
8. General System Description / Purpose 12

PreVeil Network Diagram 13

9. System Environment 13
10. System Interconnection / Information Sharing 16
11. Laws, Regulations, and Policies Affecting the System 16
12. Minimum Security Controls 16
13. Controls 27

ACCESS CONTROL 27

1.1. Account Management AC.1.001 27
1.2. Account Management AC.1.002 28
1.3 Use of External Information Systems AC.1.003 29
1.4. Publicly Accessible Content AC.1.004 30
1.5. System Use Notification AC.2.005 32

[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

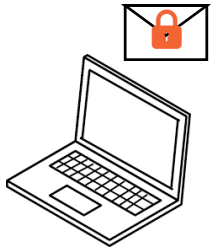
The following individual is identified as the system owner or functional proponent/advocate for the system.

[company] Sensitive and Proprietary Page | 10

Zero Trust Server: End-to-end Encryption

In PreVeil all Files and Emails are encrypted at the sender's device and can only be decrypted by the recipient
The Servers (AWS Gov Cloud by Default) can never decrypt the data, neither can attacker., PreVeil or AWS

Encrypt



Company A

AWS GovCloud

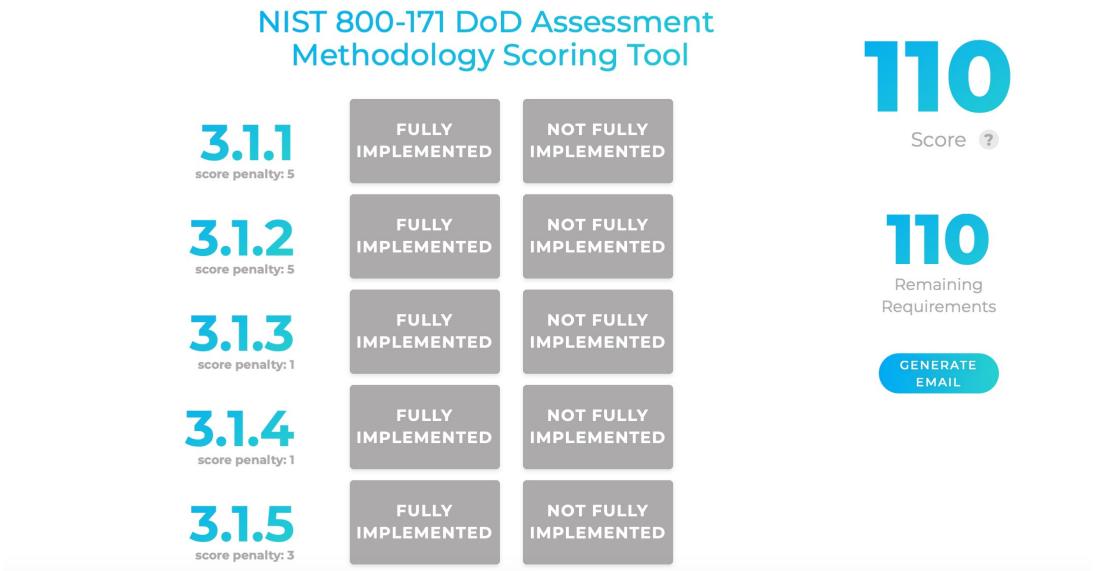
Company B

Decrypt

Company C

Company D

Integrated with GRC > ComplyUP



- Automatically Loads PreVeil Documentation
- Generates SPRS Score
- Monitors POAM Completion
- Creates System Security Plan