

Summary

A large engineering organization attempted to migrate its operations to a Cloud enclave to simplify CMMC compliance; however, a lack of proper preparation resulted in confusion surrounding the location and transmission of CUI.

SP6 was able to significantly:

- ✓ Reduce the cost of compliance by clearly defining and reducing the number of people, processes, and technologies that interact with CUI.
- ✓ Provide data-driven guidance on how to best leverage Cloud technology in conjunction with on-premises software and equipment.
- ✓ Increase the ROI of compliance investments by mapping them to business risk and company objectives.

CASE STUDY

COMPLIANCE ADVISORY CUI DATA MAPPING SERVICE



SYSTEMS MADE
Secure. Compliant. Resilient.

The Problem

This engineering organization historically relied on on-premises solutions to conduct its operations. When it came to achieving compliance, the organization believed that switching to a Cloud enclave would help it better contain and manage CUI.

While this switch could have been successful, the client **failed to fully analyze its environment and needs beforehand** and quickly realized that Cloud enclaves are not as straightforward as they thought – especially given the organization’s reliance on advanced design software and specialized equipment. What resulted was:

- An overwhelming amount of “edge cases” that required inefficient access to in-scope physical endpoints (e.g., cameras, survey instruments, testing equipment) and quickly spiraled out of control
- Confusion surrounding the location and flow of CUI
- High costs of running specialized, high-performant engineering software in the Cloud Service Provider (CSP)

The excess of edge cases made it difficult for the client to identify and track which business functions, teams, and processes stored, processed, and transmitted CUI. **Like many organizations, the client made the mistake of creating an overly large scope that encompassed more of the business than necessary.** This would result in unnecessary compliance investments for business areas that didn’t require them.

Solution

The organization turned to SP6 for guidance on mapping out its CUI, especially when it came to the transmission of CUI from its on-premises endpoints to its Cloud enclave. **SP6’s Certified CMMC Professionals and Assessors performed a CUI Data Mapping exercise that focused on four main goals:**

- Tracing the storage and transmission of CUI across the organization
- Reducing confusion surrounding the flow of CUI between on-premises equipment and the Cloud enclave
- Providing data-backed business justification for different computing approaches (Cloud, hybrid, and on-prem)
- Providing suggestions to limit the scope of CUI to reduce the scope of compliance

SP6 took a **highly individualized approach** to the CUI Data Mapping exercise, interviewing key stakeholders and conducting thorough analysis to identify the following:

- What data does the organization store, receive, or create that is CUI?

Continued

Solution, *continued*

- How does this CUI enter, leave, and flow throughout the organization, and which people, processes, and technology does it touch?
- What percentage of users require access to CUI? What is the threshold allowed for duplicate corporate and enclave licensing costs?
- To what extent is the business capable of working out of an enclave? Specifically examining:
 - Compatibility with printing, 3D printing, testing and survey equipment, cameras, and resource-intensive software
 - The amount of required transmission of CUI outside of controlled areas to perform business functions

Results

After conducting its CUI Data Mapping exercise, SP6 was able to:

- **Significantly reduce the cost of compliance by clearly identifying and reducing the scope of CUI.**
 - SP6 determined over 400 users did not require logical access to CUI within the CSP enclave, saving duplicate Microsoft licensing costs of 130% (corporate and GCC High licenses).
 - SP6 determined over five satellite offices did not store, transmit, or process CUI, resulting in significant savings in physical security and media handling.
 - SP6 reduced the percentage of resource-intensive software and specialized-equipment assets that required additional security controls to meet CMMC compliance to 40%.
- **Reduce the cost of Cloud investments by switching to a more efficient hybrid approach.**
 - By thoroughly detailing the flow of CUI across all on-premises and Cloud locations, SP6 allowed the organization to better understand its Cloud enclave and make an informed decision on whether this was the best way to proceed.
 - After SP6 detailed the compliance, cost, and operational impacts of each approach (Cloud, hybrid, and on-prem), the organization opted for a hybrid approach that better aligned with its business objectives, reduced costs, and centralized CUI.
- **Strengthen the organization's security and compliance posture and provide leadership with confidence in CMMC readiness.**
 - Ensuring that all CUI was accounted for allowed the organization and its leadership to more confidently proceed with compliance decisions and investments.

About SP6

SP6 is a niche services firm with expertise in both Security Analytics and Cybersecurity Compliance. In Security Analytics, SP6 has one of North America's largest and most competent Splunk services teams in North America. SP6 offers both project-based Professional Services and the Value Acceleration Program for Splunk, a fractional co-management model. In the field of Cybersecurity Compliance, SP6 provides consulting expertise with NIST security frameworks such as NIST CSF, 800-171 and 800-53. These services include security and compliance gap assessments, remediation advisement around missing or failed security controls, outsourced Compliance as a Service, and Continuous Controls Monitoring through our ASCERA software product.