# Prospective Senior GRC Employee: FedRAMP Writing Assignment

Dear Prospective Employee,

As a Veris Group employee, you will be responsible for creating client deliverables that document our assessment work. Our FedRAMP projects require write ups that are clear, concise, and defendable. This writing assignment is your first opportunity to demonstrate your technical writing abilities.

## FedRAMP Client Scenario

You have been working on a project team serving as a third-party assessment organization (3PAO) for a small cloud security provider (CSP) named Veris Group. This is the initial assessment for the CSP. The CSP has a small SaaS environment by the name of Sky Solutions. Fortunately, the SSP is well-documented. Its FIPS 199 security categorization is Moderate.

Your manager has assigned you to assess the AC-11, IA-2(1), IR-2, and SI-16 controls. During your time onsite, you have worked alongside the system administrator for the client as well as your project team and have collected a multitude of artifacts and interview notes to help support you as begin to draft your write-ups. This assessment took place during 2017.

**Directions:**

1. Read the sample Veris Group SSP
2. Analyze provided artifacts
3. Complete the (abbreviated) FedRAMP SRTM workbook write-ups for AC-11, IA-2(1), IR-2, and SI-16 controls
4. Submit write-ups to recruiting.

**Resources:**

1. Sky Solutions SSP (in Appendix)
2. FedRAMP SRTM (Security Requirement Traceability Matrix) workbook (in Appendix)
3. Sky Solutions artifacts (in Appendix)

\*Save and extract the files in the Appendix to work with the artifacts

Expectations and Caveats

As a member of the Veris Group team, you’re expected to be able to effectively analyze and interpret customer documentation as well as management, operational, and technical artifacts. As part of this assignment, you are provided an abbreviated SSP containing the security controls to which you have been assigned as well as a series of artifacts to support the implementation of those security controls. It is your job to analyze the associated artifacts and documentation, while identifying the pertinent information which validates the implementation of each security control.

## Appendix

