SUNHAWK CONSULTING

Getting a Thumbs Up from the Agency CISO

A Case Study in Security Focus and Execution

Learn how to align activities for FedRAMP, CMMC, NIST 171, SOC, HIPAA, StateRAMP, TXRAMP, etc.

- Know your limitations!
  - Assess your internal staffing capabilities.
    - How do they align with your compliance needs?
    - Just being aware of requirements is grossly inefficient and ineffective.
  - Experience is directly proportional to success.

SUNHAWK CONSULTING

Learn how to align activities for FedRAMP, CMMC, NIST 171, SOC, HIPAA, StateRAMP, TXRAMP, etc.

- What resources do you have that can accomplish and maintain compliance activities?
  - Do you have qualified staff that can handle the design, implementation, and documentation requirements for the target authorization?
    - Security Frameworks have varying levels of difficulty and complexity.
    - Expertise in the specific framework is critical to success.

SUNHAWK CONSULTING

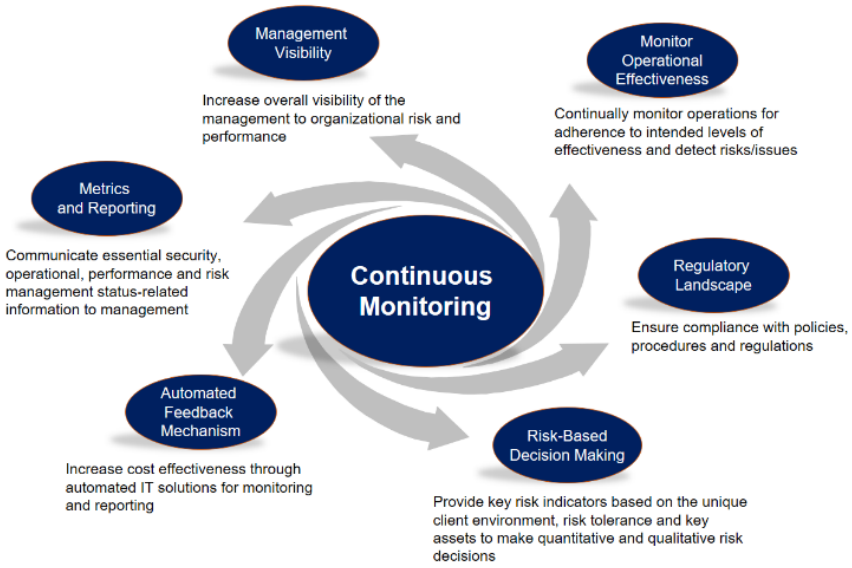
Learn how to align activities for FedRAMP, CMMC, NIST 171, SOC, HIPAA, StateRAMP, TXRAMP, etc.

- Be Organized
- LEVERAGE the work already completed for other frameworks? (YES, there are a significant number of redundancies.)
  - All frameworks have similarities
    - Policies and Procedures
    - Security documentation
    - Reporting mechanisms

SUNHAWK CONSULTING

Learn how to align activities for FedRAMP, CMMC, NIST 171, SOC, HIPAA, StateRAMP, TXRAMP, etc.

- Sync your continuous monitoring and reporting activities
- No need to constantly “re-invent the wheel”.
- Stop the constant rush to get out reports for agencies and governing bodies.
- Focus on the activities required (again, a lot of redundancies) and have them scheduled with a similar cadence.



SUNHAWK CONSULTING

Learn how to align activities for FedRAMP, CMMC, NIST 171, SOC, HIPAA, StateRAMP, TXRAMP, etc.

- Vulnerability scans, POAM updates, inventory changes, and infrastructure updates can be synchronized across all framework platforms and applications.
- It is very common to have the same compliance team performing these actions. Having a routine cadence can prevent mistakes, burnout, and oversights.

SUNHAWK CONSULTING

Understand how to navigate the administrative, regulatory, and political aspects of agency approval.

- KNOW YOUR CLIENT!!
  - Identify ***ALL*** Stakeholders. This includes not just the Senior management levels, but also the program teams, ISSOs, GRC staff, and the contracting officer.
    - Understand "Who" the players are and "What" they are going to focus on when you meet.

SUNHAWK CONSULTING

Understand how to navigate the administrative, regulatory, and political aspects of agency approval.

- Make sure your team is prepared for the onslaught of questions, concerns, “land mines”, and data categories (YES, they vary between agencies and program offices.)
  - No two agencies are alike.
  - Specific requirements or “overlays” that must be addressed by the vendor.
    - These can include Privacy, Critical system, and Supply Chain security control “overlays”. (Additional Controls)

SUNHAWK CONSULTING

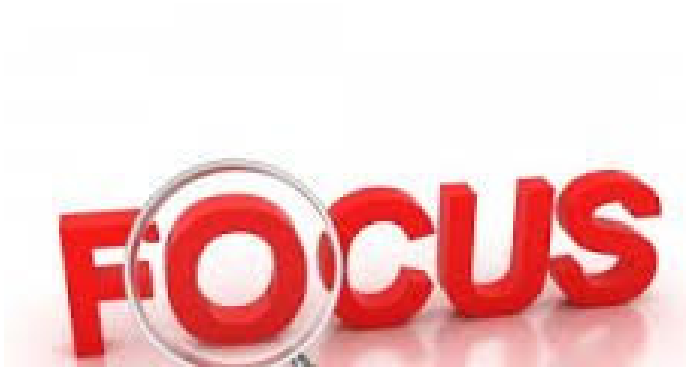
Understand how to navigate the administrative, regulatory, and political aspects of agency approval.

- Engage experts who have *already been successful* in achieving compliance with multiple frameworks and agencies.
  - The experience of ***knowing*** (not just reading about) the likely pitfalls attributed to politics, regulatory overlaps, and the administrative demands will be your saving grace.

SUNHAWK CONSULTING

Understand how to navigate the administrative, regulatory, and political aspects of agency approval.

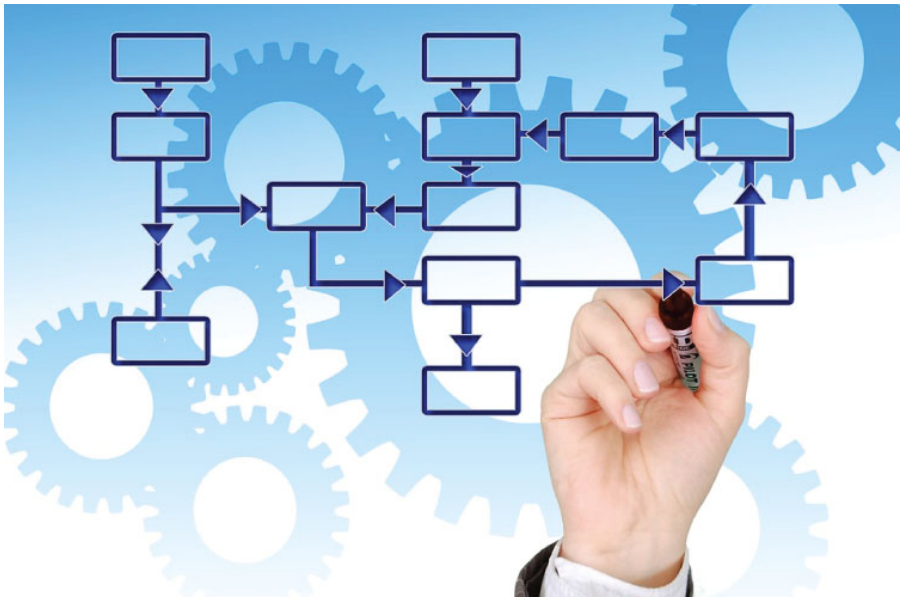
- Understand and be prepared for differing agencies having different "agency specific" security requirements. (GRC platforms, approval processes, data categorizations, and critical infrastructure definitions)
- Keep your *<u>focus on your client requirements</u>*!



SUNHAWK CONSULTING

Assess the level of planning and oversight needed to achieve and maintain compliance.

- *COMPLETELY UNDERSTAND THE REQUIRED PROCESSES AND STAKEHOLDER RESPONSIBILITIES!*
  - You can't plan the trip if you don't know where you are going.



SUNHAWK CONSULTING

Assess the level of planning and oversight needed to achieve and maintain compliance.

- Appoint a ***STRONG Project Manager*** who will be responsible and accountable for compliance success.
    - They will drive the effort so that milestones are met, resources are assigned, and communication with the Agency is consistent.

SUNHAWK CONSULTING

PLAN THE WORK. WORK THE PLAN.

- Ensure, as much as one can, that your teams are not trying to accomplish too much too fast. The mistakes occurring in the compliance process will ***COST*** you significantly regarding time to completion, missing compliance review windows established by agencies and compliance governing bodies (CMMCAB, FedRAMP PMO, StateRAMP PMO, federal agencies, etc.), and the complication of Continuous Monitoring activities

SUNHAWK CONSULTING

Questions

SUNHAWK CONSULTING