SOC 2 FIVE-STEP READINESS PROCESS

Preparing for a SOC 2 audit can be strenuous and time-consuming, depending on the scope and level of complexity in a corporate environment. GoldSky Security begins this process by understanding what is driving the need for a SOC 2 audit and assessing the systems that are pertinent to those drivers. The following is our proven Five Step Approach towards achieving SOC 2 accreditation:

STEP ONE — DETERMINE TRUST SERVICES CRITERIA IN SCOPE FOR EXAMINATION

The trust services criteria are classified into the following five categories:

1. SECURITY: Information and systems are protected against unauthorized access, unauthorized disclosure of information and damage to systems that could compromise the availability, integrity, confidentiality and privacy of information or systems and affect the entity’s ability to meet its objectives.

2. AVAILABILITY: Information and systems are available for operation and use to meet the entity’s ability to meet its objectives.

3. PROCESSING INTEGRITY: System processing is complete, valid, accurate, timely, and authorized to meet the entity’s objectives.

4. CONFIDENTIALITY: Information designated as confidential is protected to meet the entity’s objectives.

5. PRIVACY: Personal information is collected, used, retained, disclosed, and disposed of to meet the entity’s objectives.

STEP TWO — PERFORM A NIST SP 800-53 SECURITY RISK ASSESSMENT & SOC 2 GAP ANALYSIS

GoldSky performs a NIST based security risk assessment, examines the controls effectiveness and identifies gaps and vulnerabilities that exist within the organization. This assessment serves as a baseline for determining the starting point on the journey towards SOC 2 accreditation.

- **INTERVIEWS** with key stakeholders
- **REVIEW** of policies & procedures
- **INTERNAL/EXTERNAL** vulnerability assessments
- **IDENTIFICATION** of gaps
- **DETAILED** Gap Analysis report
- **THREAT** out brief with key stakeholders

STEP THREE — DESIGN OF CONTROLS

Evaluate the control environment using the SOC 2 criteria customized to the chosen Trust Services Criteria to identify gaps that require remediation.

The assessment consists of the following steps:

- **MAPPING** of existing controls to the framework
- **DOCUMENTATION** of gaps and "future state" controls
- **IDENTIFICATION** of remediation plans

STEP FOUR — REMEDIATION

The Remediation plan serves as a detailed Roadmap in preparation for the SOC 2 report and addresses the following:

- **DETAILED** steps and deliverables to satisfy the control standards
- **ACHIEVABLE** timelines to meet goals
- **DETERMINE** Remediation stakeholders to drive and track progress

Some gaps are easily remedied. Others will require more time and cost investment to implement. Regular meetings should be scheduled for key stakeholders involved in the SOC 2 remediation activities. It is critical to meet with all stakeholders and solicit their subject matter expertise on remediation and process improvements. These meetings will also begin the process of fostering a culture of SOC 2 compliance, which is imperative, especially for companies carrying out the assessment for the first time.

STEP FIVE — SOC 2 READINESS TESTING

GoldSky will perform readiness testing to ensure the company's controls work as intended. This should be done before engaging the auditor. Readiness testing reduces the risk of exceptions that could result in qualified opinions and serves to validate management's assertions made during documentation and remediation phases. Only when a company has performed readiness testing and addresses its operating effectiveness issues should management feel confident to move forward with the SOC 2 audit.

CONCLUSION

SOC 2 Readiness requires guidance from experienced IT Security and Compliance professional to ensure the controls will meet the AICPA standards. SOC 2 Readiness should be viewed as a company wide transformation for your business to gain a competitive advantage in the marketplace. GoldSky Security's proven process has helped small-midsize businesses achieve SOC 2 accreditation.

TESTIMONIAL

"We've come a long distance in improving our security measures and GoldSky has helped us get there. Not only are we able to get bigger clients that see our SOC 2 certification status, but we also have better processes from which to run our business. It feels great to know that we're continuously developing into a really stable and secure company."

— Dan Barber
CIO, COMPLIANCE SOLUTIONS

Scan to learn more about GoldSky's **SOC 2 Readiness Program**

GOLDSKY
CYBER SECURITY SOLUTIONS