FAQs

Version 3 (2021)

1. When is contract compliance due?
   a. Effective Immediately – as contracts are renewed.
2. Do all existing contracts need to be re-negotiated to become compliant?
   a. If additional protections are needed, the expectation would be that there would be a re-negotiation.
3. Where are the contract "requirements" located?
   a. *Business Procedures Manual, Section 3.4.4*
4. What is the contract submission process?
   a. This will vary by organization. Contracts should be submitted in the same manner as before; this will add additional levels of review.
5. Who is responsible for determining the contract's cybersecurity risk?
   a. The Contract Owner – see *Contract Renewal Checklist* and *Cybersecurity Contract Checklist* for additional information.
6. Where do I learn more about how to define "Risk Levels" as described in the checklists?
   a. Reference the *Business Procedures Manual, Section 3.4.4* and the *Cybersecurity Standard* to learn more.
7. Do all contracts require a cybersecurity review?
   a. Depends – the Contract Owner shall review the contract routing form (cover sheet) to determine if the contract's "Risk Level" is rated "High."
      i. If "YES" – send contract to Intuitional cybersecurity teams for review. Contact USG Cybersecurity at cybersecurity@usg.edu for further assistance.
      ii. If "NO" – no cybersecurity review is required.
8. What is a "Security Plan?"
   a. A written, reviewable, and implemented cyber risk management plan that clearly defines how USG's data and resources are protected. Suppliers must keep this plan up-to-date and operating effectively. Moreover, suppliers should also manage risks that stem from their (fourth party) suppliers.
9. What should we be looking for when reviewing a supplier's security plan?
   a. Review the *Cybersecurity Contract Checklist*, items designated as "High" are required within the supplier's security plan.
10. What should we be requesting from the supplier in addition to the security plan?
    a. Evidence the plan is working: A method to demonstrate that the plan is implemented and working effectively. Examples include:
       i. Completed and reviewed HECVAT (used by over 100 universities);

ii. SOC Type 2 Report using an appropriate set of controls;

iii. ISO 27001 certification using an appropriate set of controls;

iv. PCI Report on Compliance;

v. A Health Information Trust Alliance (HITRUST) Common Security Framework Certification;

vi. A Statement on Standards for Attestation Engagements (SSAE) No. 18, Reporting on Controls at a Service Organization;

vii. FedRAMP Certification;

viii. 3rd party audit demonstrating effective cyber risk management; or

ix. Some combination of the above.

11. Who are the governing body responsible for SOC and SSAE statements?

    a. The Association of International Certified Professional Accountants (AICPA) is the body providing governance of the criteria for Statement on Standards for Attestation Engagements (SSAE) 18 and Service Organization Control (SOC) reports.

12. Can I freely share my SOC2 report with vendors that request an example copy?

    a. Because each firm's report may contain sensitive information, they are ordinarily shared with partners who have a legitimate business need. Caution must be considered when sharing the SOC 2 report obtained from one supplier with another without permission. The supplier asking for an example should obtain answers to questions from their CPA.

13. What are SOC's five trust criteria?

    a. Because SOC engagements are work products of independent auditors, most accounting or audit firms performing SOC 2 reviews use consistent formatting to address these five trust criteria in a SOC 2 report:

       i. Security
       ii. Availability
       iii. Processing Integrity
       iv. Confidentiality
       v. Privacy

14. What are the standard deliverables of a SOC 2 engagement?

    a. The common deliverables provide by a SOC assessor are:

       i. An opinion letter;
       ii. Management assertion;
       iii. A detailed description of the system or service;
       iv. Details of the selected trust services categories;
       v. Tests of controls and the results of testing; and
       vi. Optional additional information.

15. Can you provide an example of the Table of Contents for a SOC report?

    a. Yes, this is a typical table of contents from a SOC 2 report:

       i. Section I: Management's Assertion

ii. Section II: Independent Service Auditor’s Report

iii. Section III: Description of Services during the Examination Period

iv. Section IV: Description of Control Objectives, Controls, Tests, and Test Results

1. CC1.0 Control Environment
2. CC2.0 Communication and Information
3. CC3.0 Risk Assessment
4. CC4.0 Monitoring Activities
5. CC5.0 Control Activities
6. CC6.0 Logical and Physical Access Controls
7. CC7.0 System Operations
8. CC8.0 Change Management
9. CC9.0 Risk Mitigation
10. A.0 Availability Criteria
11. C.0 Confidentiality Criteria

v. Section V: Other Information Provided by Company

vi. Management Response(s) to items of note

16. What is an Incident Response Plan?

a. An incident response plan establishes and maintains processes to identify and report cybersecurity incidents affecting USG information and data assets.

17. What incident response roles does suppliers have?

a. Suppliers must promptly report all cybersecurity incidents or events of interest affecting systems or data for any of the cybersecurity objectives of confidentiality, integrity or availability to USG Cybersecurity through the Enterprise Service Desk (helpdesk@usg.edu) at 706-583-2001, or 1 888-875-3697 (Toll free within Georgia). Further, suppliers should also notify the USG point of contact as identified in their contract.

18. How quickly should suppliers report an incident?

a. All cybersecurity incidents affecting the operation of mission-critical systems and categorized as “High” shall be reported to USG Cybersecurity **within one hour** of identification.

19. Are there specific types of incidents suppliers must report?

a. Yes – the incidents that suppliers must report to USG Cybersecurity include “type of cyber-attack, data breach, or use of malware” if these criteria are met:

i. Creates a life-safety event, or
ii. Substantially impacts the security of data and information systems, or
iii. Affects mission-critical systems, equipment, or service delivery.