Sensiba

SOC 2 Items to Keep in Mind

Disclaimer*: These are commonly requested items. There can be additional requests that fall outside of this listing, depending on the in-scope environment and completeness of the GRC tool.*

SOC 2 Type 1:

Security, Availability, and Confidentiality

1. For a sample new hire: (HRS-3, HRS-1, GOV-11, and IAC-9)
   a. Policy acceptance, background verification (can be de-scoped if not applicable), and onboarding ticket upon hire.
2. For a sample current/existing employee: (SAT-1, IAC-1, IAC-12, CRY-3, and END-1)
   a. Security awareness training completion, unique ID, MFA enabled, HD encryption, and malware detection software installed for those accessing systems and the production environment.
3. For a sample terminated user: (IAC-8)
   a. An offboarding ticket to show access was revoked in a timely manner.
4. A sample job description related to system, engineering, IT, etc. (GOV-10)
5. Evidence of infrastructure logging (MON-1/MON-2), monitoring (MON-4), and redundancy configurations (BCD-6); network access restrictions (NET-4); encryption in transit (NET-1); customer data encryption at rest (CRY-4); and daily database backups (BCD-4/BCD-5).
6. A sample code change that was recently completed showing approval and testing prior to implementation in the production environment. (CHG-1)
7. Recent vulnerability scan export. (VPM-2)
   a. Sample remediation for any high or critical findings within the scan.
8. Screenshot that shows role-based access is implemented. (IAC-2)
9. Screenshot of the security incident tracking tool in place. (IRO-3)
10. Optional: Evidence of an intrusion detection system in place to provide continuous monitoring of the company's network and early detection of potential security breaches. (MON-1)

Processing Integrity

11. A screenshot of the application configurations showing that application edits limit input to acceptable value ranges and that system edits require mandatory fields to be complete before record entry is accepted. (MON -3)

Privacy

12. Screenshot or evidence that management reviewed privacy practices from the company's website. (PRI-16)
13. Screenshot that shows users are required to explicitly accept the notice of privacy practices prior to entering information into the application, system, etc. (PRI-9)
14. For a sample of data deletion request, provide evidence that shows data was deleted in accordance with the Privacy Policy. (DCH-6)
15. Screenshot that shows users accessing their personal information through the entity's application/system must be authenticated with a username and password. (DCH-8)
16. Evidence of the user settings to show users can access all of their personal information through the application by navigating to their settings and profile. (PRI-2)

17. Evidence of user access logs demonstrating attempts to correct, amend, or append personal information, as well as documentation on system configuration settings allowing users to manage their personal information. (PRI-2)
18. Evidence of the customer portal to show that data subjects can submit inquiries, complaints, and disputes via the customer portal. (PRI-7)

SOC 2 Type 2:

Security, Availability, and Confidentiality

1. For a sample of new hires that occur during the period: (HRS-3, HRS-1, GOV-11, and IAC-9)
    a. Policy acceptance, background verification (can be de-scoped if not applicable), and onboarding ticket upon hire.
2. For a sample of current/existing employees that occur during the period: (SAT-1, IAC-1, IAC-12, CRY-3, and END-1)
    a. Security awareness training, unique ID, MFA enabled, HD encryption, and malware detection software installed for those accessing systems and the production environment.
3. For a sample of terminated users that occur during the period: (IAC-8)
    a. An offboarding ticket to show access was revoked in a timely manner.
4. A sample job description related to system, engineering, IT, etc. (GOV-10)
5. Evidence of infrastructure logging (MON-1/MON-2), monitoring (MON-4), and redundancy configurations (BCD-6); network access restrictions (NET-4); encryption in transit (NET-1); customer data encryption at rest (CRY-4); and daily database backups (BCD-4/BCD-5).
6. Population of security incidents that occur during the period. IRO-3)
    a. If there is a non-occurrence, we will ask to see a screenshot of the security incident tracking tool in place.
7. Population of completed production changes that occurred during the period. (CHG-1)
    a. After the period ends, we will select a sample to see the individual tickets to confirm that code changes are tested and approved prior to implementation.
    b. Make sure that code changes are approved and merged by different people to show a segregation of duties.
8. A sample of vulnerability scans performed during the period. Sensiba will select a sample of scans based on the frequency stated within policy and procedure. (VPM-2)
    a. Furthermore, evidence of ongoing remediation for any high or critical findings.
9. Screenshot that shows role-based access is implemented. (IAC-2)
10. Optional: Evidence of an intrusion detection system in place to provide continuous monitoring of the company's network and early detection of potential security breaches. (MON-1)

Processing Integrity

11. A screenshot of the application configurations showing that application edits limit input to acceptable value ranges and that system edits require mandatory fields to be complete before record entry is accepted. (MON-3)

Privacy

12. Screenshot or evidence that management reviewed privacy practices from the company's website. (PRI-16)
13. Screenshot that shows users are required to explicitly accept the notice of privacy practices prior to entering information into the application, system, etc. (PRI-9)

14. Population of data deletion requests that occurred during the period. (DCH-6)
    a. For a sample of data deletion request, provide evidence that shows data was deleted in accordance with the Privacy Policy
15. Screenshot that shows users accessing their personal information through the entity's application/system must be authenticated with a username and password. (DCH-8)
16. Evidence of the user settings to show users can access all of their personal information through the application by navigating to their settings and profile. (PRI – 2)
17. Evidence of user access logs demonstrating attempts to correct, amend, or append personal information, as well as documentation on system configuration settings allowing users to manage their personal information. (PRI – 2)
18. Evidence of the customer portal to show that data subjects can submit inquiries, complaints, and disputes via the customer portal. (PRI -7)

Annual Items:

***Disclaimer**: Frequency within policy should clearly state how often these controls occur (annual, bi-annual, quarterly, etc.)*

- *If any annual tests occur outside of a shortened period (3, 6, 9- month duration); Sensiba will note a non-occurrence, if applicable, within the 'Results': "N/A - An annual ________ did not occur during XX/XX/XXXX- XX/XX/XXXX…".*
- *If a control does not occur naturally during the audit period (example: if no new hires occur), there is no testable evidence of that control's operation. In such cases, a non-occurrence statement would be used in the SOC 2 Type 2 report to explain this to the end users reading the report. This is a very standard and accepted practice, and it does not indicate a deficiency or impact the overall opinion, provided the control is designed appropriately and the surrounding control environment is effective.*

Security

1. Annual access review performed by management during the period. (IAC-7)
2. Annual Penetration Test completed during the period. (IAO-2)
3. Risk Assessment completed/ reaffirmed during the period. (RSK-1/RSK-2)
4. Risk Treatment Plan completed/ reaffirmed during the period. (RSK-2)
5. An annual 'SOC Report Review' completed within the 'Vendors' tab for the primary infrastructure provider during the period. (TPM-2)
6. Annual review of Organization Chart. (GOV-8)
7. Annual review of policies done by management within the 'Policy Center'.
8. Annual Disaster Recovery Exercise performed. (BCD-2)
9. Optional: Annual Incident Response Exercise performed. (IRO-1)

Privacy

10. Annual review of Privacy Policy. (PRI-16)