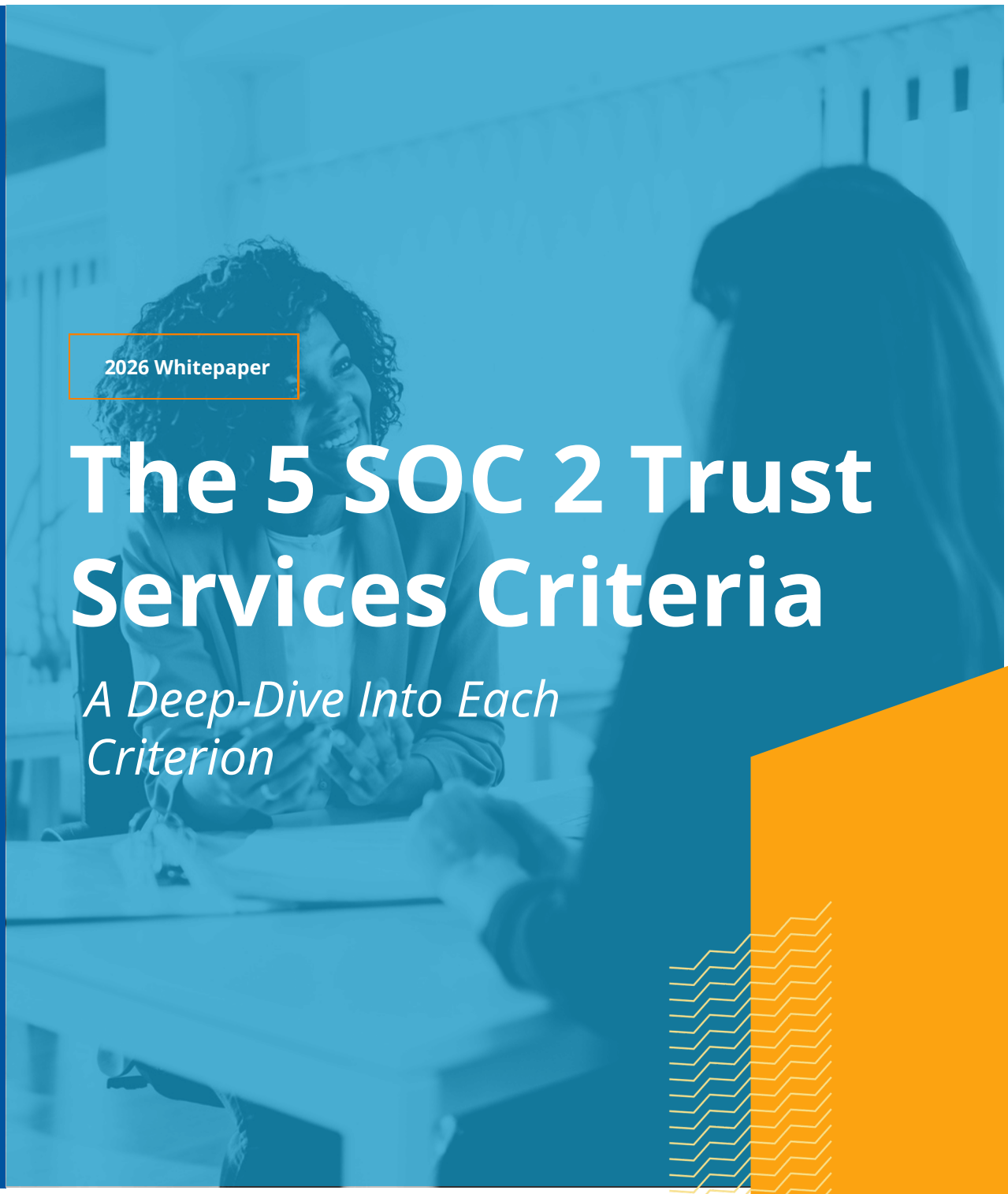
BARR ADVISORY



2026 Whitepaper

The 5 SOC 2 Trust Services Criteria

A Deep-Dive Into Each Criterion

TABLE OF CONTENTS

INTRODUCTION

One of the first steps you'll take when preparing for a SOC 2 audit is selecting which **trust services criteria (TSC)** may be included in the report. Trust services criteria are criteria used to evaluate and report on controls over information and systems. This can be company-wide or specific to a department or division within a company.

What are the trust services criteria?

There are five trust services criteria to consider for a SOC 2 report: security, availability, confidentiality, processing integrity, and privacy.

Every SOC 2 audit includes the security criterion, as it is the required component from which other criteria can be added. But what other criteria are there and how do you know which criterion to include?

Trust Services Criteria Categories

Security
This category looks at how your data and systems are protected against unauthorized access, use, and disclosure to reduce the risk of damage to systems. It is a required category within all SOC 2 reports because it protects data availability, integrity, confidentiality, and privacy issues, which can affect a company's ability to meet security objectives.

Availability
This category demonstrates how information and systems are accessible and maintained to meet the entity's objectives.

Confidentiality
This criterion looks at whether sensitive data or information that is classified as confidential is protected.

Processing Integrity
This shows system processing and data are complete, valid, accurate, timely, and authorized to meet objectives.

Privacy
This demonstrates personal information that is obtained, used, retained, disclosed, and disposed of in accordance with entity objectives and policies.

In short, SOC 2 trust services criteria are used to evaluate the suitability of the design and operating effectiveness of controls.

Let's dive into each criterion.

TRUST SERVICES CRITERION

SECURITY

SECURITY

At the core of every SOC 2 report is one foundational and required element: security.

Here's a quick glance at what you need to know about the security criterion:

- Security is the foundation of every SOC 2 report.
- This criterion is evaluated through nine specific "points of focus."
- Security is the only TSC that is required for all SOC 2 reports.

The Basics

Trust services criteria, which were developed by the American Institute of Certified Public Accountants (ACIPA), are used to evaluate and report on controls over information and systems. These controls may apply across an entire organization or be scoped to a specific system, depending on the SOC 2 report.

According to BARR Advisory Attest Services Manager Amanda Parnigoni, "the objective of the security TSC is to ensure that information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems."

In practice, this means auditors are evaluating whether your organization has designed and implemented controls that help prevent and detect system failures, incorrect processing, theft, or other unauthorized removal or misuse of data.

> ***"The objective of the security TSC is to ensure that information and systems are protected against, unauthorized access, unauthorized disclosure of information, and damage to systems.***
>
> **Amanda Parnigoni**
> Attest Services Manager
> BARR Advisory

Points of Focus

To meet the security criterion, organizations must address nine specific "points of focus." These include:

CC1: Control Environment
CC2: Information and Communication
CC3: Risk Assessment
CC4: Monitoring Activities
CC5: Control Activities
CC6: Logical and Physical Access Controls
CC7: System Operations
CC8: Change Management
CC9: Risk Mitigation

SOC 2 requires organizations to have control activities in place that support each of these points of focus. As a best practice, each point should be backed by two to three controls. This layered approach helps ensure that if one control fails, others are in place to support the criteria and reduce the risk of a qualified audit opinion.

Common Obstacles

One of the most common challenges organizations face during a SOC examination is underestimating the breadth of the security criteria. While many organizations have some security controls in place, those controls may not be formally documented, consistently applied, or monitored in a way that meets audit expectations.

Other common obstacles include unclear ownership of controls, gaps in risk assessment processes, and change management practices that aren't well defined. Addressing these issues early as part of a readiness assessment can significantly reduce friction and the chance of surprises popping up during the audit.

The Bottom Line

Security is the backbone of every SOC 2 report. Getting it right sets the stage for a smoother audit and stronger customer trust.

TRUST SERVICES CRITERION

AVAILABILITY

AVAILABILITY

The availability criterion emphasizes keeping systems and services up and running, accessible, and functioning as promised in service level agreements.

Availability in SOC 2:

- Means reliable, resilient systems achieved through scalability, redundancy, backups, and disaster recovery
- Requires continuous monitoring, quick incident response, and maintenance
- Is measured against service level agreements—strong availability builds trust and reduces downtime impact

What Does "Availability" Really Mean?

Availability in SOC 2 is not simply about uptime—it's about designing, monitoring, and maintaining systems so they consistently meet performance expectations. Organizations must demonstrate their infrastructure can handle expected workloads, recover from disruptions, and minimize downtime.

This is especially critical for cloud service providers, SaaS companies, and any business where customers rely on continuous system access.

Key Controls That Support Availability

To meet the availability criterion, organizations typically implement a range of controls and practices, including:

- Capacity planning to ensure systems can scale with demand
- Redundancy measures like load balancing and failover systems
- Disaster recovery planning to restore services quickly after incidents
- Geographic backups to reduce risk from localized outages

For example, having backup servers in multiple regions ensures if one data center fails, another can take over with minimal disruption.

Monitoring and Incident Response

Monitoring is a critical component of availability. Companies must actively track system performance, uptime, and incident response metrics.

Effective practices include:

- Automated monitoring tools with real-time alerts
- Clearly defined incident response procedures
- Rapid diagnosis and resolution of system issues

These measures help teams address problems before they significantly impact users.

Maintenance and Continuous Improvement

Ongoing maintenance plays a key role in preventing downtime and ensuring reliability. This includes:

- Regular system updates and patch management
- Infrastructure upgrades
- Scheduled maintenance with advance customer communication

Organizations should always aim to minimize disruption during planned downtime.

Measuring Availability Against Commitments

SOC 2 availability is evaluated based on commitments made to customers, typically outlined in service level agreements. These agreements define expected uptime percentages and response and recovery times.

Auditors assess whether controls align with these commitments and whether performance data proves they are consistently met.

Why Availability Matters

Achieving SOC 2 availability builds trust and confidence. It shows a company is prepared to handle both routine operations and unexpected disruptions. In today's digital environment, strong availability practices reduce revenue loss from downtime, protect brand reputation, and improve customer satisfaction.

The Bottom Line

The availability criterion ensures systems are not only secure, but dependable—delivering services when and where users need them most. By investing in resilience, monitoring, and proactive maintenance, organizations can meet SOC 2 requirements while providing a reliable experience that their customers can count on.

TRUST SERVICES CRITERION

CONFIDENTIALITY

CONFIDENTIALITY

Protecting sensitive information from unauthorized access and disclosure is non-negotiable for organizations handling customer data. The SOC 2 confidentiality criterion strengthens your security posture and builds lasting trust. This section will discuss:

- What makes confidentiality different from the other SOC 2 trust services criteria
- Core requirements of confidentiality
- How organizations can demonstrate and practice confidentiality controls
- Gaps and challenges when implementing confidentiality protections

What Makes Confidentiality Different?

Confidentiality specifically addresses how organizations protect information designated as confidential. This is data that requires protection beyond what's provided by the security criteria and encompasses a narrower scope than privacy.

The confidentiality criterion sits between the security and privacy, zeroing in on information that the organization has explicitly committed to keep confidential through contractual agreements, regulatory requirements, or organizational policy.

Confidentiality becomes relevant when organizations handle proprietary information, trade secrets, intellectual property, strategic business plans, or any data subject to non-disclosure agreements. For SaaS providers and cloud service organizations, this often includes customer source code, algorithm details, business strategies, or sensitive configuration data that goes beyond standard security protections. Understanding this distinction helps organizations determine whether confidentiality should be included as additional criteria in their SOC 2 examination alongside security.

Core Requirements of the SOC 2 Confidentiality Criterion

The SOC 2 confidentiality criterion requires organizations to establish and maintain a comprehensive framework for identifying, classifying, and protecting confidential information throughout its lifecycle. At its core, this involves implementing controls that prevent unauthorized disclosure of information designated as confidential, whether that disclosure occurs through system vulnerabilities, human error, or malicious activity.

Organizations must first establish clear policies that define what constitutes confidential information within their environment. This classification process should align with contractual obligations, regulatory requirements, and business needs.

Once classified, the organization needs to implement access controls that restrict confidential information to only those individuals with a legitimate business need. This includes role-based access controls, segregation of duties, and the principle of least privilege applied specifically to confidential data.

Additional requirements include encryption of confidential information both in transit and at rest, secure disposal procedures when confidential data reaches end-of-life, monitoring and logging of access to confidential information, and incident response procedures specifically designed to address confidentiality breaches.

Organizations must also address confidentiality in vendor relationships, ensuring third-party service providers maintain appropriate protections for any confidential information they access or process. Documentation of these controls, along with evidence of their operating effectiveness over the examination period, forms the foundation of a successful SOC 2 confidentiality assessment.

.

How Organizations Demonstrate Confidentiality Controls in Practice

Demonstrating effective confidentiality controls requires both technical implementation and operational discipline. Leading organizations begin with comprehensive data classification programs that inventory all information assets and apply confidentiality labels based on sensitivity and contractual obligations. This classification then drives access decisions, with confidential information segregated into separate repositories, databases, or system environments with enhanced protection measures.

Technical controls typically include encryption key management systems with separation of duties, data loss prevention tools that monitor and block unauthorized transmission of confidential information, and advanced access management systems that enforce multi-factor authentication (MFA) for confidential data access. Organizations often also implement watermarking or digital rights management for confidential documents, network segmentation to isolate confidential information processing, and specialized backup and recovery procedures that maintain confidentiality protections throughout the data lifecycle.

Operational practices are equally important. Effective organizations conduct regular confidentiality awareness training tailored to roles with confidential data access, implement clean desk policies and secure workspace requirements for handling confidential information, and maintain detailed access logs with regular review procedures.

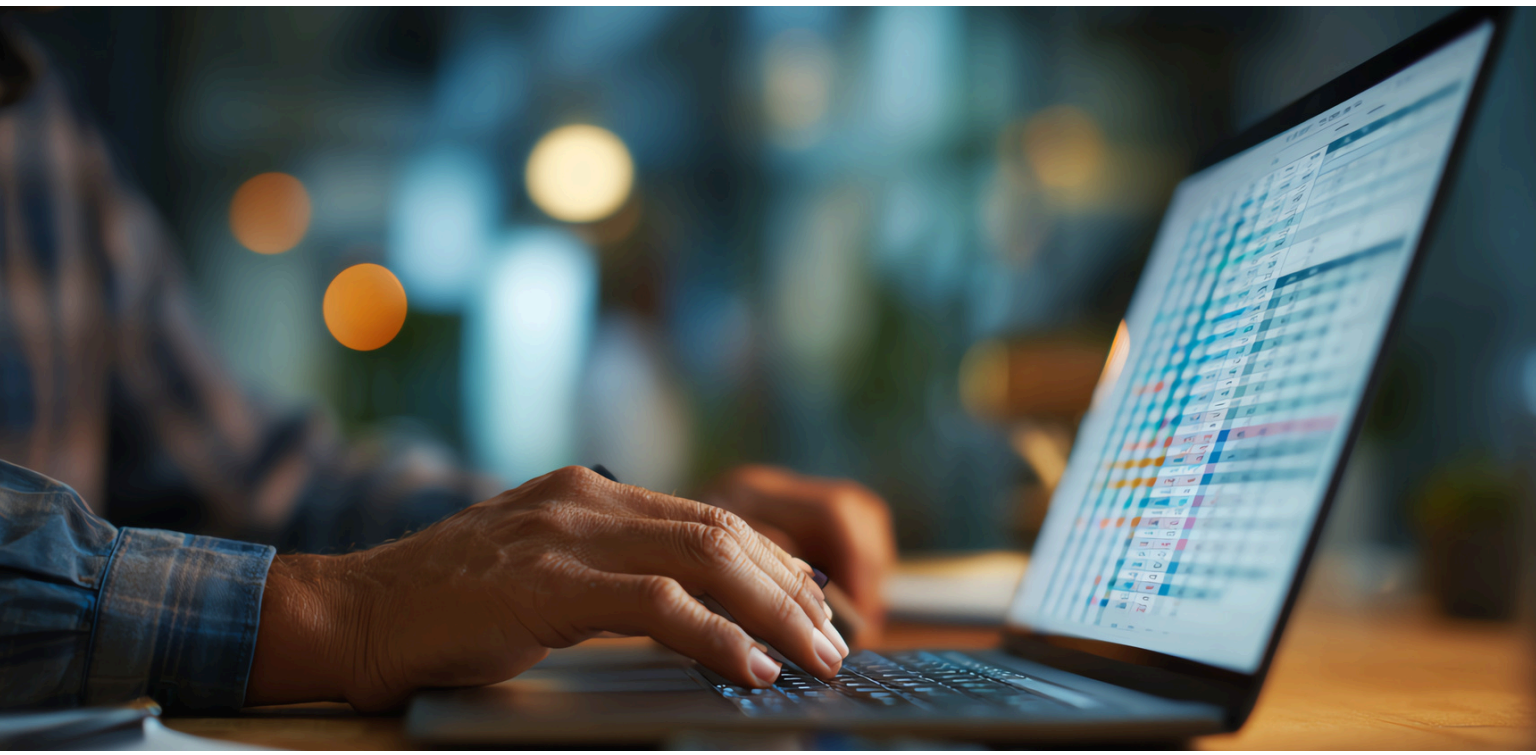
During SOC 2 Type 2 examinations, auditors look for evidence that these controls operate effectively over time—not just that policies exist on paper. This includes reviewing access logs, testing encryption implementation, validating all terminated employees lose confidential data access promptly, and confirming that confidentiality incidents are detected and responded to appropriately.

Common Gaps and Challenges When Implementing Confidentiality Protections

One of the most frequent challenges organizations face is inadequate data classification. Many organizations struggle to identify what information truly qualifies as confidential, leading to either over-classification that creates operational friction or under-classification that leaves sensitive information inadequately protected. Without clear classification criteria aligned to contractual commitments and regulatory requirements, organizations cannot effectively scope their confidentiality controls or demonstrate compliance during examinations.

Access control inconsistencies represent another common gap. Organizations may implement strong controls for production systems while overlooking confidential information in development environments, backup systems, or collaboration platforms. Confidential customer data might be adequately protected in primary databases but inadvertently exposed in troubleshooting logs, email attachments, or employee workstations. This fragmented approach creates vulnerabilities that can surface during SOC 2 testing when auditors trace confidential information across the entire technology ecosystem.

Third-party risk management also presents ongoing challenges. Organizations may implement robust internal confidentiality protections while failing to extend those requirements to vendors, contractors, or business partners who access confidential information. Without appropriate non-disclosure agreements, contractual controls, and regular vendor assessments, confidential information can be exposed through the supply chain. Additionally, many organizations lack mature processes for detecting and responding to confidentiality incidents, making it difficult to demonstrate that breaches are identified and remediated promptly—a key expectation in SOC 2 examinations.



TRUST SERVICES CRITERION

PROCESSING INTEGRITY

PROCESSING INTEGRITY

One of the most critical yet often overlooked trust services criteria is processing integrity.

This criterion focuses on whether systems process data accurately, completely, in a timely manner, and as authorized.

- Processing integrity ensures systems handle data accurately, completely, and as intended, not just securely.
- It differs from other SOC 2 criteria by focusing on correct data processing, rather than access control, uptime, or data protection.
- Demonstrating it requires strong validation, monitoring, and control processes, but organizations often struggle with system complexity and maintaining consistency.

What is Proccessing Integrity?

Processing integrity ensures your systems perform exactly as intended. That means transactions are valid, data isn't lost or altered improperly, and outputs are reliable. For example, if your platform processes financial transactions, processing integrity ensures those transactions are executed correctly—no duplicate charges, missing entries, or calculation errors.

It's not just about preventing malicious activity; it's also about preventing unintentional errors in workflows, integrations, and automation.

How It Differs from Other Criteria

Processing integrity is often confused with the security criterion, but they serve different purposes. Security focuses on protecting systems and data from unauthorized access, while processing integrity is concerned with what happens to the data once it's inside the system. Availability ensures systems are up and running, but not necessarily processing correctly. Confidentiality and privacy deal with data protection and proper handling, not accuracy or completeness of processing.

You can have a highly secure and available system that still produces incorrect results. Processing integrity addresses that gap.

How to Demonstrate Processing Integrity

To meet this criterion, organizations need to implement and document controls that ensure correct processing. Common approaches include:

Input Validation Controls

Ensuring only valid data enters the system.

Processing Checks

Automated controls like reconciliation, error handling, and duplicate detection.

Output Verification

Confirming results are accurate and complete before delivery.

Audit Logs and Monitoring

Tracking system activity to identify anomalies or failures.

Change Management Controls

Ensuring updates don't introduce processing errors.

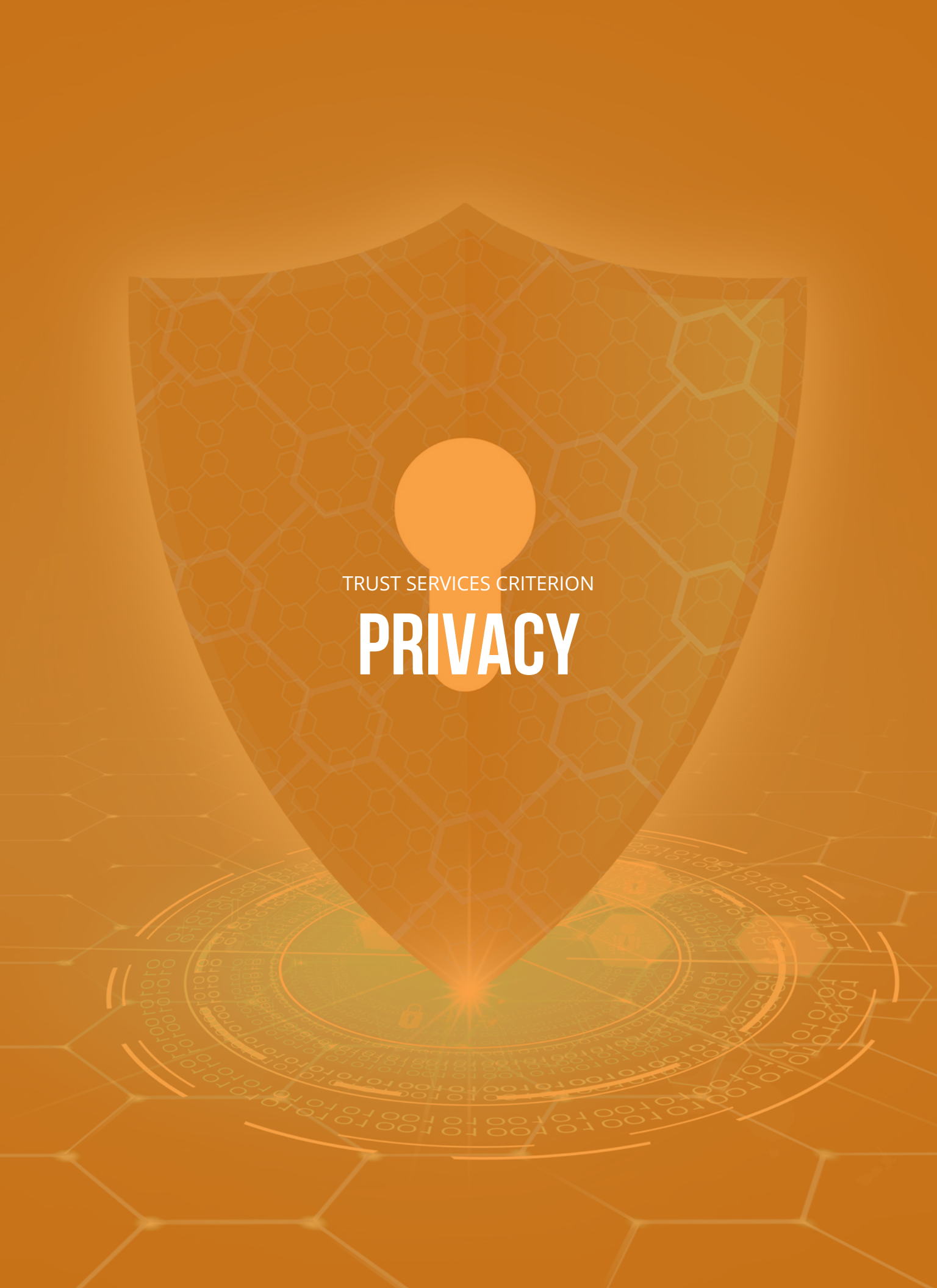
Auditors will look for evidence that these controls are both designed effectively and operating consistently over time.

Common Implementation Challenges

- **Complex system integrations:**
  Data often flows across multiple services, increasing the risk of errors or inconsistencies.
- **Lack of standardized controls:**
  Teams may rely on ad hoc validation instead of consistent, documented processes.
- **Insufficient monitoring:**
  Without robust logging and alerting, processing errors can go unnoticed.
- **Balancing speed and accuracy:**
  High-throughput systems may prioritize performance over thorough validation checks.
- **Evolving systems:**
  Frequent deployments can introduce subtle bugs that impact processing accuracy.

The Bottom Line

Processing integrity is about trust—ensuring your system does what it claims to do, every time. While it may not get as much attention as security, it's just as vital for customer confidence and operational reliability. By investing in strong validation, monitoring, and control frameworks, organizations can confidently demonstrate that their systems aren't just secure—but also dependable.


TRUST SERVICES CRITERION
PRIVACY

PRIVACY

Privacy under SOC 2 is not just about compliance; it's about protecting personally identifiable information (PII) throughout its lifecycle—collection, use, retention, disclosure, and disposal.

For modern organizations, especially those in cloud, SaaS, and regulated industries, demonstrating robust privacy controls is essential to differentiating themselves in the market. It assures clients and partners that data is handled responsibly and in accordance with current best practices and legal requirements. This assurance is critical for maintaining client trust, supporting sales cycles, and enabling global expansion into jurisdictions with strict privacy mandates.

Navigating SOC 2 Privacy Criteria: Key Components and Requirements

The SOC 2 privacy criterion stands apart due to its depth, specificity, and customization required from report to report. There are 18 additional criteria for privacy. Within each of those 18 criteria there are specific points of focus. These include notice and communication of objectives, choice and consent, collection, use, retention and disposal, access, disclosure and notification, quality, and monitoring and enforcement.

Each criterion contains detailed points of focus and requirements. For example, criterion P3.1 states that "Personal information is collected consistent with the entity's objectives related to privacy." Points of focus as it relates to P3.1 include limiting the collection of personal information, collecting information in fair and lawful means, collecting information from reliable sources, and informing data subjects when additional information is required.

The criteria also demand rigorous controls around the retention and secure disposal of PII, timely breach notifications, and ongoing monitoring to ensure policies remain effective and compliant with evolving regulations. These requirements collectively ensure a holistic approach to privacy that aligns with both client expectations and regulatory frameworks such as GDPR and CCPA.

Challenges and Pitfalls: Overcoming Common Privacy Compliance Obstacles

Implementing controls to achieve the SOC 2 privacy criterion is often the most challenging aspect of a SOC 2 engagement. The sheer number of detailed requirements can overwhelm teams, especially those new to privacy frameworks or with limited resources. Common pitfalls include understanding scoping requirements, underestimating the complexity of data inventory and mapping, failing to operationalize user rights management, and overlooking the need for continuous employee training and awareness.

Another significant challenge is harmonizing privacy controls with existing security and operational processes. Privacy is cross-functional, requiring coordination between legal, IT, compliance, and business units. Without a clear governance structure and executive sponsorship, privacy initiatives can stall or become siloed, increasing compliance risk and reducing effectiveness. Organizations must adopt a risk-based approach, prioritize high-impact controls, and leverage expert guidance to navigate these challenges efficiently.

Additionally, understanding if an organization is considered to be a “data processor” or a “data controller” is another large challenge. Scoping will help organizations understand how best to identify. Privacy criteria that are not available are considered a controller.

Integrating Privacy Controls Across Cloud and SaaS Environments

The dynamic nature of cloud and SaaS architectures introduces unique privacy risks and opportunities. Data often moves rapidly between systems, vendors, and geographies, making it critical to embed privacy controls into every aspect of the technology stack. This includes implementing strong access controls, encryption, data minimization, and automated data retention schedules within cloud platforms.

Moreover, organizations must ensure that third-party service providers and sub-processors adhere to the same privacy standards. This requires robust vendor risk management, contractual protections, and continuous monitoring. Leveraging automated compliance tools and centralized evidence management can improve visibility and reduce the operational burden associated with maintaining privacy compliance across complex cloud ecosystems.

Turning Compliance Into Trust: Demonstrating Privacy Excellence to Stakeholders

Achieving the SOC 2 privacy criteria is not just a compliance milestone—it’s a strategic opportunity to build and reinforce trust with customers, partners, and regulators. Demonstrating adherence to privacy best practices through a SOC 2 report can shorten sales cycles, streamline vendor onboarding, and support expansion into new markets. It also provides a transparent, third-party validated assurance that privacy is embedded in the organization’s culture and operations.

To maximize the value of SOC 2 privacy compliance, organizations should communicate their privacy commitments clearly in customer-facing materials, proactively share audit results with stakeholders, and continuously review and enhance their privacy program. By turning privacy into a competitive advantage, organizations not only meet regulatory requirements but also position themselves as trustworthy stewards of sensitive data in a data-driven world.

ABOUT BARR ADVISORY

BARR Advisory is a security and compliance solutions provider specializing in cybersecurity and compliance for organizations with high-value data that serve regulated industries such as healthcare, financial services, and government. A trusted advisor to some of the fastest growing cloud-based organizations around the globe, BARR simplifies compliance across multiple regulatory and customer requirements.

Our Services & Frameworks

SOC Examinations
[SOC 1, SOC 2, SOC 3, SOC for Cybersecurity]

ISO Certification
(27001, 27017, 27018, 27701, 42001, 9001, 22301)

Healthcare Compliance
[HIPAA/HITRUST]

Government Compliance
[FedRAMP, GovRAMP, CMMC, DFARS, NIST]

Privacy & Data Protection
[GDPR, CCPA, GLBA, PCI DSS, CSA STAR, Microsoft DPR]

Advisory & Managed Services

GRC & Engineering

Assessments

Attestation & Certification

CONNECT WITH BARR

Want to learn more about achieving SOC 2 compliance? Contact us today.