QUANTUM EVOLVE

Business & Cybersecurity Resilience Consultancy

System and Organisation Controls

White Paper

www.quantum-evolve.com

Introduction

System and Organisation Controls (SOC) (also sometimes referred to as Service Organisations Controls) as defined by the American Institute of Certified Public Accountants (AICPA) is the collective name of a suite of reports produced during an audit.

SOC is intended for use by Service Organisations (organisations that provide information systems as a service to other organisations) to issue validated reports of internal controls over those information systems to the users of those services.

The reports focus on controls grouped into five categories called Trust Services Criteria. The Trust Services Criteria were established by the AICPA through its Assurance Services Executive Committee (ASEC) in 2017 (2017 TSC).

The AICPA auditing standard Statement on Standards for Attestation Engagements no. 18 (SSAE 18), section 320, *"Reporting on an Examination of Controls at a Service organisation Relevant to User Entities' Internal Control Over Financial Reporting"*, defines two levels of reporting, type 1 and type 2. Additional AICPA guidance materials specify three types of reporting:

SOC 1, SOC 2 & SOC 3.

When Did SOC Audits Start?

The roots of SOC 2 are in the early 1970s when the AICPA released the Statement on Auditing Standards (SAS) 1. The SAS 1 document officially outlined an independent auditor’s role and responsibilities.

Decades passed and new SASs were created, all the way up to SAS 70 in 1992. Throughout the early 1990s, CPAs used SAS 70 to determine how effective a company’s internal financial controls were and, over time, to report on how companies treated information security in general.

Over the next 20 years, companies began to outsource services like payroll processing and cloud computing. These services could directly affect financial reporting or data security. As a result, the need arose for companies to validate their level of security, ideally through a trusted third party.

There are two levels of SOC reports specified by SSAE 18:

Type 1

Describes a Service Organisation's systems and whether the design of specified controls meet the relevant trust principles.

Type 2

Also addresses the operational effectiveness of the specified controls over a period (usually 9 to 12 months).

There are three types of SOC reports.

SOC 1	Internal Control over Financial Reporting (ICFR)
SOC 2	Trust Services Criteria
SOC 3	Trust Services Criteria for General Use Report

Additionally, there are specialised SOC reports for Cybersecurity and Supply Chain.

SOC 1 and SOC 2 reports are intended for a limited audience – specifically, users with a sufficient understanding of the system in question. SOC 3 reports contain less specific information and can be distributed to the public.

Who Needs a SOC 2 Report?

If you are a Service Organisation that stores, processes or transmits any kind of customer data, you will likely need to be SOC 2 compliant. SOC 2 requirements help your company establish airtight internal security controls. This lays a foundation of security policies and processes that can help your company scale its activities securely.

It also builds trust with your customers. Often, Service Organisations pursue a SOC 2 report because their customers are asking for it. Your clients need to know that you will keep their sensitive data safe. A SOC 2 report is the gold standard for providing that assurance.

A SOC 2 report can also be the key to unlocking sales and moving upmarket. It can signal to customers a level of sophistication within your organisation and a commitment to security. Achieving a successful SOC 2 report needs significant amounts of planning, work, and money. The benefits of SOC 2 compliance extend far beyond having the actual report in hand.

Here are some of the many advantages from complying with the SOC 2 framework.

- Protect your company reputation.
- Distinguish your company from its competition.
- Earn more customer trust, win new clients and gain access to more markets.

- Better understand your internal operating processes.
- Gain efficiencies, risk mitigations and overall improvements across internal processes.
- Strengthen security over processing, compliance and controls.

Without a SOC 2 report in hand, you may need to fill out lengthy security questionnaires for every enterprise customer. These questionnaires can be incredibly detailed, specific and difficult to fill out if you do not already have processes and documents in place. Having a SOC 2 report helps you sell to larger companies and gives you a set of solid best practices for protecting sensitive data.

SOC 2 compliant policies, procedures, and controls make it easier to achieve other security certifications. For example, SOC 2 compliance shares many requirements with ISO 27001 guidelines. Getting a SOC 2 report makes getting your ISO 27001 certification faster and less expensive.

Trust Services Criteria

Trust Services Criteria were designed to provide flexibility in application to better suit the unique controls implemented by each organisation to address its unique risks and threats it faces. This contrasts with other control frameworks that mandate specific controls whether applicable or not.

These Trust Services Criteria are the basic elements of cybersecurity posture and assess organisation controls, risk assessment, risk mitigation, risk management, and change management. The SOC 2 framework consists of 5 Trust Services Criteria made up of 64 individual requirements.

Controls are the security measures in place to satisfy these requirements. For SOC 2, there are five Trust Services Criteria to evaluate. Out of the five, only Security is required for a SOC 2 report.

Availability

Ensuring employees and clients can rely on your systems to do their work

Processing Integrity

Verifying that company systems operate as intended

Confidentiality

Protecting confidential information by limiting its access, storage, and use

Privacy

Safeguarding sensitive personal information against unauthorized users

The Trust Services Criteria were modelled in conformity to The Committee of Sponsoring organisations of the Treadway Commission (COSO) Internal Control - Integrated Framework (COSO Framework). In addition, the Trust Services Criteria can be mapped to NIST SP 800 - 53 criteria and to EU General Data Protection Regulation (GDPR) Articles.

organisation of the Trust Services Criteria is aligned to the COSO framework's 17 principles with additional supplemental criteria organized into logical and physical access controls, system operations, change management and risk mitigation. Further, the additional supplemental criteria are shared among the Trust Services Criteria - Common Criteria (CC) and additional specific criteria for availability, processing integrity, confidentiality and privacy.

Common criteria are labelled as:

- Control environment (CC1.x).
- Information and communication (CC2.x).
- Risk assessment (CC3.x).
- Monitoring of controls (CC4.x).
- Control activities related to the design and implementation of controls (CC5.x).

Common criteria are suitable and complete for evaluation security criteria. However, there are additional category specific criteria for Availability (A.x), Processing integrity (PI.x), Confidentiality (C.x) and Privacy (P.x).

Criteria for each trust services category addressed in an engagement are considered complete when all criteria associated with that category are addressed.

When Did SOC 2 Start?

In April 2010, the AICPA announced a new auditing standard: the Statement on Standards for Attestation Engagement (SSAE 16). Under SSAE 16, the AICPA released three new reports. This resulted in the SOC and the ever-popular SOC 2:

SOC 1	Internal Controls for Financial Statements & Reporting
SOC 2	Internal controls for the five Trust Services Criteria. (These are Security, Confidentiality, Processing Integrity, Privacy and Availability of customer data.)
SOC 3	SOC 2 results, tailored for a public audience

In May 2017, the AICPA replaced SSAE 16 with SSAE 18 to update and simplify some confusing aspects of SSAE 16. SSAE 18 is now used for all SOC 1, SOC 2, and SOC 3 reports.

What are the 5 AICPA Trust Services Criteria?

① Security

The Security Trust Criteria are all about protecting information from unauthorized disclosure. The Security Criteria are often known as the Common Criteria. They prove that a service organisation's systems and control environment are protected against unauthorized access and other risks.

Security is the only Trust Services Criteria category required for every SOC 2 audit. Other criteria can be added to the scope if an organisation chooses but are not required to achieve SOC 2 compliance.

② Availability

The Availability Criteria determine whether your employees and clients can rely on your systems to do their work. Some examples are data backups, disaster recovery, and business continuity planning. Each of these examples minimizes downtime in the event of an outage.

Consider adding to your SOC 2 if:

- You offer a continuous delivery or deployment platform.
- An outage would prevent your clients from building or deploying changes to their services, e.g. cloud computing or cloud data storage providers.

③ Processing Integrity

The Processing Integrity Criteria determine whether a system works properly and without delay, error, omission, or accidental manipulation. This is not the same as data integrity — a system can work properly with incorrect data.

Consider adding to your SOC 2 if:

- You provide financial reporting services, or you are an e-commerce company.
- You need to ensure your transaction processing is accurate to combat fraud.

④ Confidentiality

The Confidentiality Criteria evaluate how organisations protect confidential information by limiting its access, storage, and use. It can help organisations define which individuals can access what data and how that data can be shared. This ensures that only authorized people can view sensitive information, like legal documents or intellectual property.

Consider adding to your SOC 2 if:

- Your organisation handles confidential information. Examples include financial reports, passwords, business strategies, and intellectual property.

⑤ Privacy

This Trust Security Criteria looks at how an organisation's control activities protect customers’ personally identifiable information (PII). It also ensures that a system that uses personal data complies with the AICPA’s Generally Accepted Privacy Principles.

Name, physical address, email address, and Social Security number are a few examples of information that falls under this privacy category. Data like health, race and sexuality may be pertinent to privacy for some companies and service providers, too.

Consider adding to your SOC 2 if:

- Your organisation gathers, stores, uses, preserves, reveals or disposes of personal information.

What is the SOC 2 Common Criteria List?

The Security Trust Security Criteria is all about protecting information and systems.

Is data secure during its collection or creation? Is it secure during its use, processing, transmission, and/or storage? How does a company prevent and monitor any vulnerabilities in its systems?

The SOC 2 Common Criteria list, also known as the CC-series, includes nine subcategories:

CC1 — Control environment

Does the organisation value integrity and security?

CC2 — Communication & Information

Are policies and procedures in place to ensure security? Are they communicated well to both internal and external partners?

CC3 — Risk Assessment

Does the organisation analyse risk and monitor how changes impact that risk?

CC4 — Monitoring Controls

Does the organisation monitor, evaluate and communicate the effectiveness of its controls?

CC5 — Control Activities

Are the proper controls, processes, and technologies in place to reduce risk?

CC6 — Logical & Physical Access Controls

Does the organisation encrypt data? Does it control who can access data and restrict physical access to servers?

CC7 — System Operations

Are systems monitored to ensure they function properly? Are incident response and disaster recovery plans in place?

CC8 — Change Management

Are material changes to systems properly tested and approved beforehand?

CC9 — Risk Mitigation

Does the organisation mitigate risk through proper business processes and vendor management?

SOC 2 Common Criteria Mapping

Many organisations choose to pursue compliance with multiple security standards. The AICPA helps map the Common Criteria onto requirements for frameworks including ISO 27001 and GDPR.

Mapping SOC 2 Common Criteria to ISO 27001

ISO 27001 specifies requirements for establishing, implementing, maintaining and improving an information security management system (ISMS). It includes 114 controls across 14 groups, the majority of which map to SOC 2 Trust Services Criteria.

The AICPA ISO 27001 mapping spreadsheet breaks down the overlap with the Trust Services Criteria.

Mapping SOC 2 Common Criteria to GDPR

The European Union’s General Data Protection Regulation (GDPR) is designed to protect EU citizens’ personal data rights. It applies to any company that handles these protected individuals’ data. It includes 99 articles across 11 chapters.

Nearly all of Chapters 2 and 3 and most of Chapter 4 of GDPR map onto SOC 2’s Trust Services Criteria. The AICPA also provides an EU GDPR mapping spreadsheet to help cross-reference criteria and controls.

SOC 1 vs SOC 2 vs SOC 3

System and organisation Controls, better known as the SOC framework, was developed by the American Institute of CPAs (AICPA). The AICPA defines three different types of SOC reports. Understanding the differences between SOC 1 vs SOC 2 vs SOC 3 is important when deciding which type of compliance you need for your business.

SOC 1, 2 and 3 all have different purposes. SOC 1 focuses on financial reporting, SOC 2 focuses on a broader range of data management practices, and SOC 3 provides a summary of the SOC 2 attestation report that is suitable for the public.

Here is the difference between SOC 1, SOC 2 and SOC 3:

	What does it cover?	Who needs one?
SOC 1	Internal controls for financial statements and reporting.	organisations providing a service that can impact a client’s financial statements, e.g. collections agencies, payroll providers and payment processing companies.
SOC 2	Internal controls for security, confidentiality, processing integrity, privacy and availability of customer data.	organisations that store, process or transmit client data, e.g. SaaS companies, cloud storage services and data hosting or processing providers.
SOC 3	SOC 2 results tailored for a general audience.	organisations that require a SOC 2 who want to use compliance for marketing to the public.

The numbers do not indicate a particular sequence or a higher set of standards. A SOC 3 is not harder to get or more prestigious than a SOC 2. You do not need a SOC 1 before starting a SOC 2 audit. SOC 1, 2 and 3 are simply different reporting types.

SOC 1 vs SOC 2

A SOC 1 report is for organisations whose internal security controls can impact a customer’s financial statements. Think payroll, claims, or payment processing companies. SOC 1 reports can assure customers that their financial information is being handled securely.

SOC 2 reports help organisations demonstrate their cloud and data centre security controls. This security framework is based on the Trust Services Criteria (more on that in a bit).

Both SOC 1 and SOC 2 are attestation reports, where management attests that certain security controls are in place. An independent CPA firm is brought in to verify those claims and either agree or disagree.

Both SOC 1 and SOC 2 also offer Type I and Type II reports.

What is the difference between SOC Type I vs Type II?

There are two types of SOC 2 reports:

SOC 2 Type I Reports

Evaluate a company's controls at a single point in time. It answers the question: are the security controls designed properly?

SOC 2 Type II Reports

Assess how those controls function over a period, generally 3-12 months. It answers the question: do the security controls a company has in place function as intended?

Type I reports evaluate an organisation's controls at a single point in time. Essentially, the goal is to determine whether the controls put in place are designed correctly. A Type II report examines how well those controls perform over a period (typically 3-12 months).

To choose between the two report types, consider your goals, cost, and timeline constraints. A Type I report can be faster to achieve but a Type II report offers greater assurance to your customers.

Many customers are increasingly rejecting Type I reports so a company may need a Type II report at some point and, by going straight for a Type II, will save time and money by doing a single audit.

If you need a SOC 2 report ASAP, a Type II report that covers a shorter 3-month review period can be an alternate solution. This shorter period may not be acceptable for complex risk assessments.

SOC 3 Reports vs SOC 2 Reports

Both SOC 2 and SOC 3 reports are conducted according to SSAE 18 standards, as outlined by the AICPA. Both reports involve a CPA audit and rigorous testing of an organisation’s security controls.

There are a few key differences:

Reporting Type

As mentioned above, SOC 2 offers both Type I and Type II reports. SOC 3 reports are always Type II reports.

Level of Detail

SOC 3 Type 2 reports do not include detailed descriptions of the auditor’s control tests, test procedures, or test results. They do contain the auditor’s opinion, management assertion, and system description. Because the report does not go into as much detail as a SOC 2, SOC 3 reports usually will not satisfy customer needs.

Level of Privacy

SOC 2 reports are private, which means they are typically shared only with customers and prospective customers under a non-disclosure agreement (NDA). SOC 3 reports are general use reports that can be distributed freely or posted to the public on an organisation’s website.

Why Do Customers Often Ask For a SOC 2?

The most referenced report is the SOC 2. SaaS vendors are commonly asked by their customers' legal, security, and procurement departments to provide a copy of their SOC 2 report.

SOC 2 is not motivated by compliance with legal regulations unlike many other frameworks such as HIPAA, GDPR, and CCPA. Instead, it helps organisations prove that their internal controls protect customer data.

Deciding which SOC report makes the most sense for your company depends on the type of information you are processing for your customers. Some organisations need both a SOC 1 and SOC 2 report. This will depend on the services you provide and your customers.

For example, if you are providing payroll processing services, you will most likely need a SOC 1.If you are hosting or processing customer data, you will need a SOC 2 report. SOC 3 reports are less formal and are best used as marketing material.

www.quantum-evolve.com

Safeguard your Reputation

Without a clear and complete understanding of your IT estate, it is not possible to secure a business.

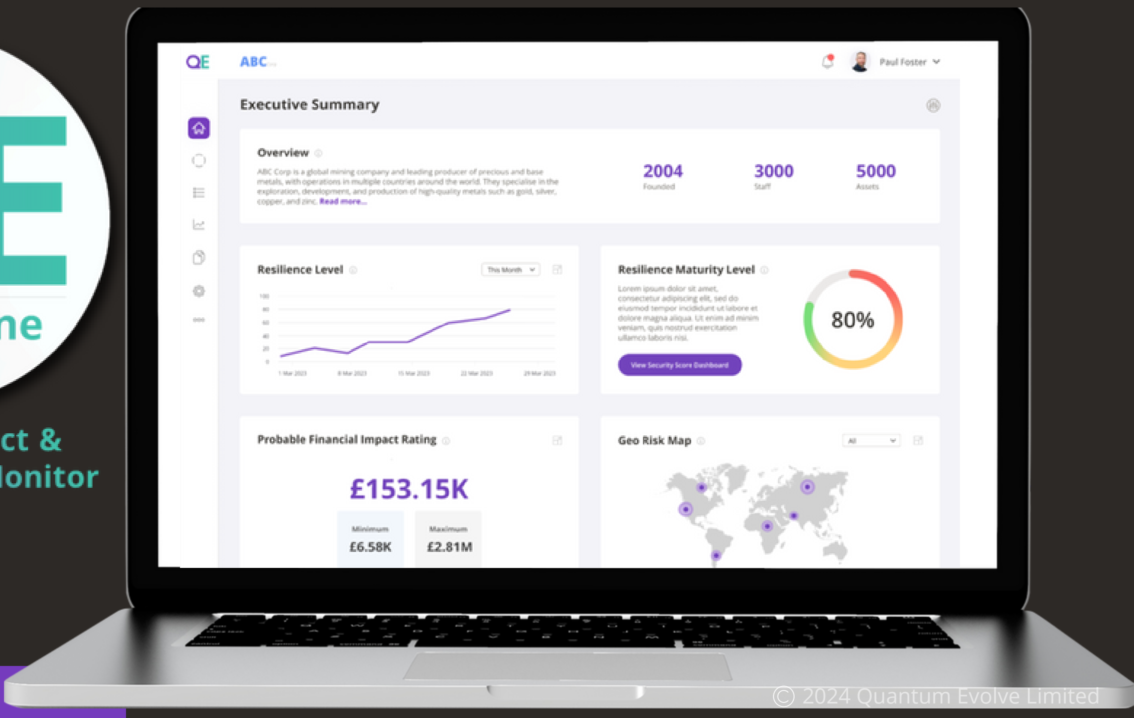
Quantum Evolve's innovative approach to Cyber Resilience & Posture provides your business with a comprehensive understanding of the risks within its digital ecosystem.

QE Touchstone, our extensive 360-degree, "single plane of glass" view of your security controls and capabilities, identifies emerging threats, existing vulnerabilities and cyber risks.

It quickly and efficiently benchmarks your compliance against globally recognised standards and frameworks e.g. NIST, ISO, GDPR, PCI DSS, HIPAA, thereby safeguarding your network, brand and reputation.

Touchstone

Assess, Protect & Continuously Monitor



Executive Summary

Overview

ABC Corp is a global mining company and leading producer of precious and base metals, with operations in multiple countries around the world. They specialise in the exploration, development, and production of high-quality metals such as gold, silver, copper, and zinc. Read more...

2004 Founded

3000 Staff

5000 Assets

Resilience Level

Resilience Maturity Level

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi.

Probable Financial Impact Rating

£153.15K

Minimum £6.58K

Maximum £2.81M

Geo Risk Map

Resilient Security Posture

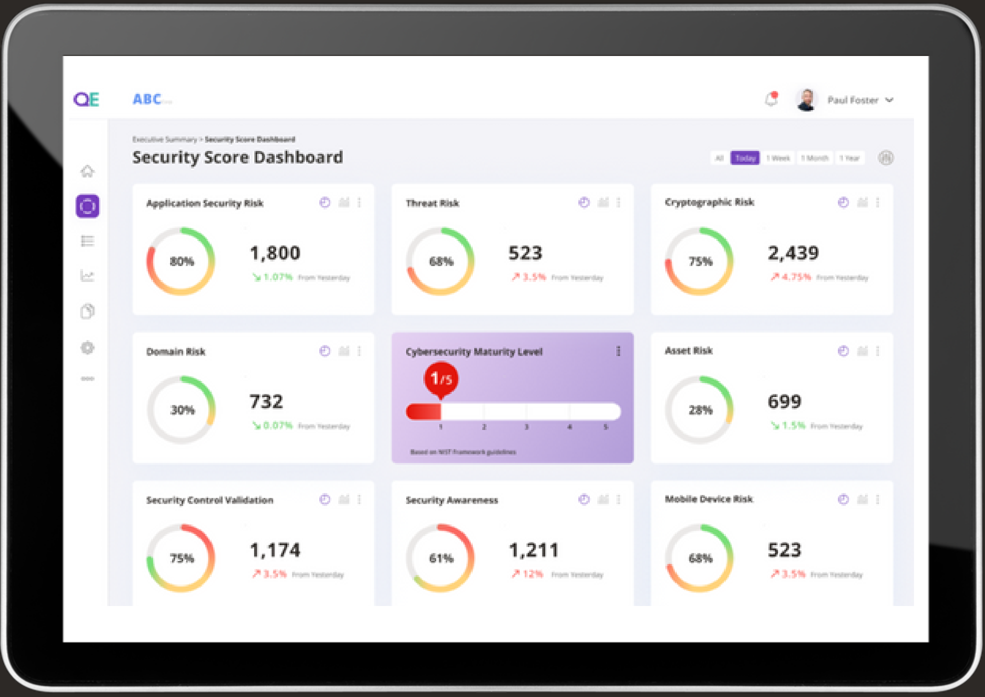
We can easily interpret your business' true risk from financial quantification to technical detail.

QE Touchstone allows us to capture and prioritise your risks, stating the required remediation and allowing you to develop a clear roadmap to ensure you can modernise, whilst consecutively and effectively mitigating / managing your risks.

Assessment Outsourcing

Assessments can be selected from QE Touchstone's wide-ranging services and, where necessary, tailored to meet exact requirements. Reports will be supplied directly on completion – either in hard copy, soft copy or via a secure, online portal.

Should you wish to find out more information on the solutions and services Quantum Evolve can provide, please contact one of our experts.



ABC

Paul Foster

Executive Summary > Security Score Dashboard

Security Score Dashboard

All | Today | 1 Week | 1 Month | 1 Year

Application Security Risk: 80% — 1,800 — ↘ 1.07% From Yesterday

Threat Risk: 68% — 523 — ↗ 3.5% From Yesterday

Cryptographic Risk: 75% — 2,439 — ↗ 4.75% From Yesterday

Domain Risk: 30% — 732 — ↘ 0.07% From Yesterday

Cybersecurity Maturity Level: 1/5 (1 2 3 4 5) — Based on NIST Framework guidelines

Asset Risk: 28% — 699 — ↘ 1.5% From Yesterday

Security Control Validation: 75% — 1,174 — ↗ 3.5% From Yesterday

Security Awareness: 61% — 1,211 — ↗ 12% From Yesterday

Mobile Device Risk: 68% — 523 — ↗ 3.5% From Yesterday

Touchstone

Assess, Protect & Continuously Monitor

QUANTUM EVOLVE

Business & Cybersecurity Resilience Consultancy

QE Touchstone

Assess, Protect & Continuously Monitor

Michael (Mo) Stevens, Chairperson
+44 (0)7801 712582
michael.stevens@quantum-evolve.com
michael-mo-stevens-b42b61

Mark Child, CEO
+44 (0)7515 107005
mark.child@quantum-evolve.com
mark-child-8859451

Paul Foster, CTO
+44 (0)7450 872368
paul.foster@quantum-evolve.com
paulfosterconsultancy

www.quantum-evolve.com

quantum-evolve-business-enablement

CYBER ESSENTIALS CERTIFIED PLUS

MSDUK CERTIFIED ETHNIC MINORITY BUSINESS