THE SOC 2 HANDBOOK

A COMPLETE GUIDE TO DESIGNING, IMPLEMENTING, AND AUDITING A SOC 2 COMPLIANCE PROGRAM

PRACTICAL GUIDANCE • REAL-WORLD EXAMPLES • PROVEN RESULTS

FRANKLIN GRAYSON

COMPLIANCE. ASSURANCE. TRUST.

The Definitive Guide to SOC 2

A Complete Guide to Designing, Implementing, and Auditing a SOC 2 Compliance Program

Steve Publications

This book is available at https://leanpub.com/thedefinitiveguidetosoc2

This version was published on 2026-08-12

This is a Leanpub book. Leanpub empowers authors and publishers with the Lean Publishing process. Lean Publishing is the act of publishing an in-progress ebook using lightweight tools and many iterations to get reader feedback, pivot until you have the right book and build traction once you do.

Contents

A Complete Guide to Designing, Implementing, and Auditing a SOC 2 Compliance Program

This book takes you from zero knowledge to professional-level competence in SOC 2 compliance. Whether you are a startup founder needing your first report, a security leader building a compliance program, an engineer implementing controls, or an auditor evaluating systems, this guide provides the end-to-end knowledge you need. You will learn what SOC 2 is and why it matters, how to design and document your system, how to select and implement effective controls, how to collect audit-ready evidence, how to prepare for and pass your examination, and how to maintain continuous compliance as part of ongoing governance rather than a one-time project. Every chapter includes practical implementation guidance, realistic examples, templates, checklists, and decision frameworks you can apply immediately.

Introduction: Trust in the Age of Cloud Services

In 2017, Equifax disclosed that hackers had stolen personal data from approximately 147 million people through an unpatched vulnerability in its web application infrastructure. The breach cost the company billions in fines, settlements, and remediation expenses, but the most enduring damage was to trust. Customers questioned whether their sensitive financial data was safe. Regulators demanded answers. And for years afterward, Equifax had to prove it could be trusted again [1].

That incident illustrates something fundamental about modern business: trust is not optional, and it cannot be assumed. In an era where organizations increasingly rely on cloud services, SaaS platforms, third-party vendors, and interconnected systems, customers need assurance that the companies handling their data are doing so responsibly. They need proof.

SOC 2 is one of the most widely recognized forms of that proof.

What This Book Is About

SOC 2 (System and Organization Controls 2) is a framework for evaluating how service organizations manage customer data based on five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. It was developed by the American Institute of Certified Public Accountants (AICPA) and has become a de facto standard in technology, cloud computing, SaaS, fintech, healthcare IT, and many other industries [2].

But here is what most people get wrong about SOC 2: it is not a checklist you complete to get a certificate. It is not a one-time audit you survive and then forget. And it is not something only large enterprises with dedicated security teams can achieve. SOC 2 is a structured approach to building trustworthy systems, backed by independent verification. When done right, it strengthens your security posture, improves your operational discipline, accelerates your sales cycles, and gives customers real confidence in your services [3].

This book explains everything you need to know to design, implement, operate, and maintain a SOC 2 compliance program from the ground up. It is written for multiple audiences:

- **Complete beginners** who have never heard of SOC 2 but now need it because a customer asked for it or a vendor requested it
- **Security and IT professionals** building their organization first compliance program
- **Engineering leaders** who need to understand how development practices relate to control requirements
- **Compliance officers and risk managers** seeking a comprehensive reference
- **Auditors and consultants** looking for practical implementation patterns
- **Startup founders and executives** making strategic decisions about when and how to pursue SOC 2

The book assumes no prior knowledge. It starts with the fundamentals and progressively builds toward professional-level understanding. By the time you finish, you will be able to scope a SOC 2 engagement, design controls that match your actual operations, implement technical and administrative safeguards, collect reliable evidence, prepare for auditors, respond to findings, and maintain continuous compliance as part of normal business operations.

What SOC 2 Is and Is Not

Before we dive into the details, let me clarify some common misconceptions.

SOC 2 is not a law or regulation. Unlike HIPAA, PCI-DSS, GDPR, or SOX, there is no government agency that requires you to have SOC 2 compliance. You pursue it because your customers expect it, your industry norms demand it, or you want the competitive advantage of demonstrating trustworthiness independently.

SOC 2 is not a certification. There is no such thing as being certified for SOC 2. What you receive is an attestation report issued by a licensed CPA firm after examining your controls. The report carries one of four opinions: unqualified (clean), qualified (passed with exceptions), adverse (failed), or disclaimer of opinion (insufficient evidence) [4].

SOC 2 is not prescriptive about specific technologies. The framework does not say you must use a particular firewall, password manager, vulnerability scanner, or encryption tool. It specifies objectives and criteria that your controls must achieve. How you achieve them is up to you, based on your environment, risk profile, and operational constraints [5].

SOC 2 is not the same as SOC 1 or SOC 3. These are related but distinct reports within the AICPA SOC suite. SOC 1 focuses on controls relevant to financial reporting. SOC 2 focuses on security, availability, processing integrity, confidentiality, and privacy. SOC 3 is a simplified, public-facing version of a SOC 2 report [6].

SOC 2 is not a substitute for good security. If your organization has no security practices and you implement controls solely to pass an audit, you will likely fail the audit anyway. Auditors test whether controls actually operate effectively. They interview people, review evidence, sample transactions, and verify that what is documented matches what happens in reality [7].

Why Organizations Pursue SOC 2

Despite not being legally required, SOC 2 has become one of the most sought-after compliance attestations in technology and professional services. Here are the primary reasons:

Customer requirements. Enterprise buyers routinely require SOC 2 reports from their vendors as part of procurement and vendor risk management processes. If you want to sell to large organizations, a SOC 2 report is often a gatekeeper requirement [8].

Accelerated sales cycles. Instead of answering dozens of security questionnaires from different prospects, you can share your SOC 2 report as evidence of your security posture. This reduces friction and speeds up deals [9].

Competitive differentiation. In crowded markets, a clean SOC 2 report signals maturity and trustworthiness that smaller competitors may lack. It is a tangible credential that customers recognize and value [10].

Regulatory alignment. While SOC 2 itself is not a regulation, its controls often map to requirements in GDPR, HIPAA, CCPA, and other frameworks. Organizations pursuing multiple compliance objectives can use SOC 2 as a foundation [11].

Operational improvement. The process of designing and implementing SOC 2 controls forces organizations to document their practices, identify gaps, standardize procedures, and establish governance structures that improve overall operations [12].

How This Book Is Organized

The book is structured to take you on a logical journey from understanding the framework to implementing it in practice.

Part I: Foundations covers what SOC 2 is, its governing standards, the Trust Services Criteria, examination types, and how SOC 2 relates to other frameworks. These chapters establish the conceptual foundation you need before implementation begins.

Part II: Planning and Scoping explains how to determine whether SOC 2 is appropriate for your organization, define system boundaries, document architecture and data flows, perform risk assessments, and build an implementation roadmap.

Part III: Control Design and Implementation provides detailed guidance for all major control domains, including identity and access management, change management, secure development, vulnerability management, logging and monitoring, incident response, data protection, availability and disaster recovery, vendor management, training, governance, and more. Each domain is explained with the purpose of controls, the risks they address, implementation steps, evidence requirements, and common pitfalls.

Part IV: Evidence and Audit Preparation covers how to build an evidence management program, prepare for auditors, respond to testing and sampling, handle walkthroughs and interviews, and manage the examination process.

Part V: Findings, Remediation, and Continuous Compliance explains how to understand audit findings, remediate deficiencies, maintain compliance after the report, avoid common failures, and build a sustainable program.

Throughout the book, you will find:

- **Realistic examples** labeled as illustrative templates rather than universal requirements
- **Tables and matrices** for control mapping, risk registers, evidence catalogs, and decision frameworks

- **Checklists** for implementation steps and audit preparation
- **Callouts** distinguishing formal AICPA requirements from recommendations and best practices

How to Use This Book

You can read this book sequentially from beginning to end if you want a comprehensive understanding. If you need specific information quickly, here are some shortcuts:

- **Deciding whether SOC 2 is right for you:** Read Chapters 1 and 4
- **Planning your first SOC 2 engagement:** Read Chapters 3, 4, and 5
- **Implementing specific controls:** Use the domain chapters in Part III as reference guides
- **Preparing for an audit:** Read Chapters 14 and 15
- **Understanding audit findings:** Read Chapter 15
- **Building continuous compliance:** Read Chapter 16

The book is designed so that each chapter stands on its own while building on previous material. Cross-references point you to related topics when needed.

By the end of this journey, you will understand SOC 2 not as an abstract compliance exercise but as a practical framework for building trustworthy systems that protect customer data, maintain operational reliability, and earn the confidence of your stakeholders. Let us begin.

Chapter 1: Understanding SOC 2 — Foundations and Framework

Before you can implement SOC 2, you need to understand what it is, who created it, how it fits into the broader compliance landscape, and why organizations choose it over other frameworks. This chapter establishes the foundational knowledge that underpins everything else in this book.

The AICPA and the SOC Reporting Frameworks

SOC 2 was created by the American Institute of Certified Public Accountants (AICPA), a professional organization representing more than 400,000 CPAs in the United States [13]. The AICPA develops and maintains the auditing standards that govern how SOC reports are conducted, ensuring they follow rigorous attestation procedures rather than informal checklists.

The SOC framework evolved over decades. It began with SAS 70 (Statement on Auditing Standards No. 70), issued in 1992, which provided guidance for auditors examining service organization controls. SAS 70 served the industry well but had limitations: it was not internationally aligned, its scope was narrow, and it did not adequately address the growing complexity of cloud computing and SaaS services [14].

In 2011, the AICPA replaced SAS 70 with SSAE 16 (Statement on Standards for Attestation Engagements No. 16), introducing the SOC suite of reports we know today: SOC 1, SOC 2, and SOC 3. This was coordinated with international standard-setting bodies to align with ISAE 3402, ensuring global consistency [15].

SSAE 18 replaced SSAE 16 in 2016 as part of a broader codification of attestation standards. SSAE 18 includes AT-C Section 205 (Examination Engagements), which governs how SOC reports are performed, and AT-C Section 101 (General Principles and Responsibilities for Attestation Engagements), which establishes the foundational requirements for auditors [16].

The key takeaway: SOC 2 is not a casual framework. It is governed by formal attestation standards maintained by a recognized professional body, and only licensed CPA firms with appropriate qualifications can perform SOC 2 examinations and issue reports [17].

The Three SOC Reports

The AICPA SOC suite includes three distinct report types, each serving different purposes:

SOC 1 (SOC for Service Organizations: Internal Control over Financial Reporting) focuses on controls that could affect a user entity's financial statements. It is primarily relevant to organizations providing services that impact financial reporting, such as payroll processors, claims administrators, or billing platforms. SOC 1 reports use criteria defined by the service organization and its users rather than a standard set of criteria [18].

SOC 2 (SOC for Service Organizations: Trust Services Criteria) focuses on controls related to security, availability, processing integrity, confidentiality, and privacy. It is designed for technology companies, data centers, SaaS providers, cloud platforms, managed service providers, and any organization that stores or processes customer data in ways that customers care about from a security and operational perspective [19].

SOC 3 (SOC for Service Organizations: Trust Services Criteria for General Use Report) is essentially a simplified, public-facing version of a SOC 2 report. It covers the same Trust Services Criteria but contains less detail and can be freely distributed without confidentiality restrictions. SOC 3 reports are useful for marketing purposes when an organization wants to demonstrate trustworthiness publicly but does not want to share the detailed information in a SOC 2 report [20].

The table below summarizes the key differences:

Feature	SOC 1	SOC 2	SOC 3
Focus	Financial reporting controls	Security, availability, integrity, confidentiality, privacy	Same as SOC 2
Audience	Users and their auditors	User entities, regulators, specific stakeholders	General public
Criteria	Defined by users/service org	AICPA Trust Services Criteria	AICPA Trust Services Criteria
Detail level	Detailed	Detailed	Summary only
Distribution	Restricted (confidential)	Restricted (confidential)	Unrestricted (public)
Type I/II options	Yes	Yes	No (single type)

What SOC 2 Is and What It Is Not

Understanding what SOC 2 is not is almost as important as understanding what it is. Misconceptions about SOC 2 lead to poor implementation decisions, wasted resources, and failed audits.

What SOC 2 Is

SOC 2 is:

- **An attestation framework:** A structured approach for independent auditors to evaluate whether an organization's controls meet established criteria
- **Based on the Trust Services Criteria:** A defined set of principles and requirements published by the AICPA that specify what good controls look like [21]

- **Principles-based, not prescriptive:** SOC 2 defines objectives and outcomes but does not mandate specific technologies, tools, or processes. Organizations choose how to meet the criteria based on their environment and risk profile [22]
- **Flexible in scope:** Organizations select which Trust Services Categories apply to their services and define system boundaries that match what they actually do
- **Backed by independent verification:** Only licensed CPA firms can perform SOC 2 examinations, ensuring objectivity and professional standards

What SOC 2 Is Not

SOC 2 is not:

- **A law or regulation:** No government agency mandates SOC 2 compliance. It is a voluntary framework pursued for business reasons [23]
- **A certification:** There is no SOC 2 certificate. You receive an attestation report with an auditor's opinion, which is fundamentally different from a pass/fail certification
- **A one-time achievement:** SOC 2 reports cover a specific period and must be renewed annually. Maintaining compliance requires ongoing effort [24]
- **A guarantee of security:** A clean SOC 2 report means your controls were suitably designed and operating effectively during the audit period. It does not mean you are immune to breaches or that no vulnerabilities exist
- **Applicable to all organizations:** SOC 2 is designed for service organizations – entities that provide products or services to other organizations (user entities). If you do not handle customer data or provide services to other businesses, SOC 2 may not be relevant [25]

How SOC 2 Differs from ISO 27001, SOC 1, SOC 3, HIPAA, PCI-DSS

Organizations often face multiple compliance requirements and need to understand how SOC 2 relates to other frameworks. Here is a practical comparison:

SOC 2 vs ISO 27001

ISO 27001 is an international standard for Information Security Management Systems (ISMS) published by the International Organization for Standardization. It is the most widely recognized security certification globally [26].

Key differences:

- **Geographic relevance:** SOC 2 is primarily recognized in North America, particularly among U.S. technology companies and their customers. ISO 27001 has global recognition and is often preferred outside the United States [27]
- **Format:** SOC 2 produces an attestation report with an auditor's opinion. ISO 27001 produces a formal certificate valid for three years with annual surveillance audits [28]
- **Prescriptiveness:** ISO 27001 has more prescriptive requirements, including mandatory documentation of an ISMS, risk treatment plans, and specific control implementation. SOC 2 is more flexible about how you achieve the objectives [29]
- **Scope:** ISO 27001 focuses on information security broadly. SOC 2 can cover security plus availability, processing integrity, confidentiality, and privacy depending on scope [30]
- **Timeline:** SOC 2 Type I can be completed in weeks to months. ISO 27001 certification typically takes six months to a year for first-time certification [31]

Many organizations pursue both: SOC 2 for U.S. enterprise customers and ISO 27001 for international markets and broader recognition. The control overlap is significant, so implementing one framework provides a strong foundation for the other [32].

SOC 2 vs HIPAA

HIPAA (Health Insurance Portability and Accountability Act) is a U.S. federal law that sets requirements for protecting health information. It applies to covered entities (healthcare providers, health plans, healthcare clearinghouses) and their business associates [33].

Key differences:

- **Legal status:** HIPAA is legally mandatory for covered organizations. SOC 2 is voluntary
- **Scope:** HIPAA focuses specifically on protected health information (PHI). SOC 2 can cover any type of customer data depending on the organization's services
- **Criteria:** HIPAA has specific regulatory requirements (Security Rule, Privacy Rule, Breach Notification Rule). SOC 2 uses the Trust Services Criteria
- **Enforcement:** HIPAA violations can result in fines from the Department of Health and Human Services. SOC 2 failures result in audit findings but no government penalties

Healthcare IT companies often need both: HIPAA compliance because they handle PHI, and SOC 2 because their customers expect it as evidence of security maturity [34].

SOC 2 vs PCI-DSS

PCI-DSS (Payment Card Industry Data Security Standard) is a set of security requirements for organizations that process, store, or transmit credit card data. It is mandated by payment card brands (Visa, Mastercard, American Express, etc.) [35].

Key differences:

- **Scope:** PCI-DSS applies specifically to cardholder data environments. SOC 2 can cover any system handling customer data
- **Requirements:** PCI-DSS is highly prescriptive with specific technical requirements (encryption standards, network segmentation rules, logging requirements). SOC 2 defines outcomes but not specific implementations
- **Assessment:** PCI-DSS requires annual assessments by Qualified Security Assessors (QSAs) or self-assessment questionnaires. SOC 2 requires examination by licensed CPAs

Organizations processing payment data may need both frameworks depending on their business model [36].

SOC 2 vs GDPR

GDPR (General Data Protection Regulation) is the European Union's comprehensive privacy regulation. It applies to any organization processing personal data of EU residents, regardless of where the organization is located [37].

Key differences:

- **Nature:** GDPR is a legal regulation with specific rights and obligations. SOC 2 is a voluntary attestation framework
- **Focus:** GDPR focuses on individual privacy rights (consent, access, deletion, portability). SOC 2's Privacy criterion addresses some of these but within a broader control framework
- **Enforcement:** GDPR violations can result in fines up to 4% of global annual revenue or 20 million euros. SOC 2 findings affect audit opinions but carry no government penalties

SOC 2 does not replace GDPR compliance, but SOC 2 controls can support GDPR obligations around security, data handling, and accountability [38].

The Trust Services Criteria Overview

The heart of SOC 2 is the Trust Services Criteria (TSC), published by the AICPA in TSP Section 100 as the 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (with Revised Points of Focus – 2022) [39].

The criteria define what auditors evaluate during a SOC 2 examination. They are organized into five categories:

1. **Security** – Also called Common Criteria because it applies to every SOC 2 report. Covers protection against unauthorized access, both physical and logical.
2. **Availability** – System accessibility per commitments made to users (SLAs, service level objectives).
3. **Processing Integrity** – Accuracy, completeness, timeliness, and authorization of system processing.
4. **Confidentiality** – Protection of information designated as confidential throughout its lifecycle.

5. **Privacy** – Collection, use, retention, disclosure, and disposal of personal data in accordance with the AICPA's Generally Accepted Privacy Principles (GAPP).

Security is mandatory for all SOC 2 reports. The other four categories are optional and should be selected based on the organization's service commitments and what matters most to its users [40].

Structure of the Criteria

The Trust Services Criteria are built on the COSO Internal Control – Integrated Framework (2013), which defines five components of internal control: control environment, risk assessment, control activities, information and communication, and monitoring activities [41].

For the Security criterion, the AICPA developed Common Criteria (CC) numbered CC1 through CC9, organized as follows:

- **CC1:** Control Environment – Governance, ethics, tone at the top
- **CC2:** Communication and Information – Internal and external communication of objectives and responsibilities
- **CC3:** Risk Assessment – Identification and analysis of risks to objectives
- **CC4:** Monitoring Activities – Ongoing and separate evaluations of controls
- **CC5:** Control Activities – Policies and procedures that help ensure management directives are carried out
- **CC6:** Logical and Physical Access Controls – Restricting access to assets, data, and systems
- **CC7:** System Operations – Day-to-day operations, monitoring, vulnerability management, incident response
- **CC8:** Change Management – Authorization, design, development, testing, and implementation of changes
- **CC9:** Risk Mitigation – Managing risks from third parties, vendors, and business partners

Each criterion has sub-criteria (e.g., CC6.1, CC6.2) that specify particular aspects. The AICPA also publishes Points of Focus for each criterion, which provide implementation guidance and examples but are not mandatory requirements [42].

The other Trust Services Categories have their own criteria series:

- **Availability:** A1 through A3
- **Processing Integrity:** PI1 through PI3
- **Confidentiality:** C1 through C3
- **Privacy:** P1 through P7 (aligned with GAPP)

In total, there are 61 Trust Services Criteria across all categories [43]. Chapter 2 provides a detailed breakdown of each criterion and what it requires.

Management vs Auditor Responsibilities

SOC 2 examinations involve two parties with distinct responsibilities: management of the service organization and the independent auditor (service auditor). Understanding these roles is essential for successful implementation.

Management Responsibilities

Management is responsible for:

- **Defining scope:** Deciding which systems, services, and Trust Services Categories are included in the SOC 2 examination [44]
- **Designing controls:** Creating policies, procedures, technical safeguards, and operational practices that address the applicable criteria
- **Implementing controls:** Putting designed controls into practice across the organization
- **Operating controls consistently:** Running controls as designed throughout the audit period (especially critical for Type II examinations)
- **Documenting the system:** Preparing a system description that accurately represents the in-scope environment, including infrastructure, data flows, service commitments, and risk factors [45]
- **Making management assertions:** Issuing a formal statement asserting that the system description is fair and that controls are suitably designed (Type I) or operating effectively (Type II) [46]
- **Providing evidence:** Supplying the auditor with documentation, logs, records, and other evidence to support their testing
- **Remediating deficiencies:** Addressing any control gaps identified during the examination

Management cannot delegate these responsibilities to the auditor. The auditor evaluates what management has done but does not design or implement controls on management's behalf [47].

Auditor Responsibilities

The service auditor is responsible for:

- **Planning the engagement:** Understanding the system, assessing risks, and designing audit procedures appropriate to the scope and criteria
- **Evaluating the system description:** Determining whether it fairly presents the in-scope system in accordance with AICPA description criteria [48]
- **Testing controls:** Examining evidence through inspection, observation, inquiry, and reperformance to assess design suitability (Type I) and operating effectiveness (Type II)
- **Forming an opinion:** Issuing a report with one of four opinions based on the audit findings: unqualified, qualified, adverse, or disclaimer
- **Maintaining independence:** Ensuring no conflicts of interest that would impair objectivity
- **Following attestation standards:** Conducting the examination in accordance with SSAE 18 and applicable AICPA professional standards [49]

The auditor does not guarantee security, certify compliance, or provide advice on how to fix deficiencies (unless a separate consulting engagement is arranged). Their role is to examine and report based on evidence gathered during the engagement [50].

The SOC 2 Report as a Communication Tool

At its core, SOC 2 is about communication. Service organizations use SOC 2 reports to communicate their control environment to user entities – the customers, partners, and stakeholders who rely on their services. This is especially important when user entities cannot directly observe or evaluate the service organization's controls [51].

A SOC 2 report typically includes:

- **Auditor's opinion:** The auditor's conclusion about whether controls are suitably designed (Type I) or operating effectively (Type II) relative to the Trust Services Criteria

- **Management assertion:** Management's formal statement about their system and controls
- **System description:** A detailed narrative of the in-scope system, including infrastructure, data flows, service commitments, control environment, and risks [52]
- **Trust Services Criteria:** The specific criteria used for the examination
- **Tests of controls and results (Type II only):** Description of audit procedures performed and findings
- **Complementary user entity controls (CUECs):** Controls that user entities need to implement for the service organization's controls to be effective [53]
- **Subservice organization information:** How third-party providers are handled in the report scope

The report is distributed under a confidentiality agreement, which protects sensitive details while allowing recipients to evaluate the service organization's trustworthiness. Organizations can share redacted versions or summaries when full disclosure is not appropriate [54].

Summary

SOC 2 is a framework developed by the AICPA for evaluating how service organizations manage customer data based on five Trust Services Criteria: Security, Availability, Processing Integrity, Confidentiality, and Privacy. It is governed by formal attestation standards (SSAE 18), requires examination by licensed CPA firms, and produces an independent report that organizations use to demonstrate trustworthiness to customers and stakeholders.

SOC 2 is not a law, not a certification, and not prescriptive about specific technologies. It is principles-based and flexible in scope, allowing organizations to tailor their implementation to their actual operations while still meeting rigorous evaluation standards. Security is mandatory for all SOC 2 reports; other categories are selected based on service commitments.

Management bears responsibility for designing, implementing, operating, and documenting controls. The auditor evaluates those controls and issues an opinion. The resulting report serves as a communication tool that helps user entities assess risk and make informed decisions about their relationships with the service organization.

With this foundation in place, we can now dive into the specifics of how SOC 2 works: the Trust Services Criteria in detail, examination types, scope definition, and the practical steps for implementation.

Chapter 2: Trust Services Criteria Deep Dive

The Trust Services Criteria are the foundation of every SOC 2 examination. They define what auditors evaluate and against what standards they form their opinions. This chapter explains each criterion in detail, including its structure, purpose, specific requirements, and practical implementation guidance. Understanding these criteria is essential because every control you design, implement, and document ultimately maps back to one or more of them.

The Security Criterion — Common Criteria for All SOC 2 Reports

Security is the only mandatory Trust Services Category in SOC 2. Every SOC 2 report must include an evaluation of controls related to security, regardless of whether other categories are selected. This is why the Security criteria are also called Common Criteria (CC) – they apply universally [55].

The Common Criteria are organized into nine series (CC1 through CC9), each addressing a different component of the control environment. They are derived from the COSO Internal Control – Integrated Framework and supplemented with technology-specific guidance by the AICPA [56].

CC1: Control Environment

CC1 addresses the foundation of all controls: governance, ethics, tone at the top, and organizational culture. It asks whether management has established an environment that supports effective internal control.

Key sub-criteria:

- **CC1.1:** The entity demonstrates a commitment to integrity and ethical values by establishing and communicating organizational values and codes of conduct and acting consistently with them

- **CC1.2:** The board of directors exercises oversight responsibility over the design, operation, and monitoring of internal controls, or this responsibility is assigned to a management committee or individual designated by the board
- **CC1.3:** In establishing and communicating the responsibilities for designing, operating, and monitoring internal controls, management under the supervision of the board of directors establishes structures, reporting lines, and appropriate authorities and responsibilities

What this means in practice: You need documented governance structures that show who is responsible for security and compliance decisions. This typically includes:

- A code of conduct or ethics policy that employees acknowledge
- Evidence that leadership (board, executive team) reviews security matters periodically
- Defined roles and responsibilities for security management
- Clear reporting lines so people know who to escalate issues to

Common implementation: Most organizations satisfy CC1 through an Information Security Policy approved by senior leadership, a code of conduct with annual employee acknowledgment, documented security committee meetings or executive review sessions, and an org chart showing security responsibilities [57].

CC2: Communication and Information

CC2 addresses how information flows within the organization and externally. Effective controls depend on people having the right information to do their jobs and report issues.

Key sub-criteria:

- **CC2.1:** The entity obtains or generates and uses relevant, quality information to support the functioning of internal control
- **CC2.2:** The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control

- **CC2.3:** The entity communicates with external parties regarding matters affecting the operation of internal control

What this means in practice: You need evidence that security policies are communicated to employees, that people know their responsibilities, that incidents can be reported, and that relevant information reaches the right stakeholders. This includes:

- Policy distribution and acknowledgment processes
- Security awareness training that communicates expectations
- Incident reporting channels accessible to all employees
- Communication with customers about security incidents when required

Common implementation: Security policies published on an internal wiki or document management system, mandatory annual policy acknowledgments, regular security communications (newsletters, alerts), documented incident reporting procedures, and a public-facing privacy policy [58].

CC3: Risk Assessment

CC3 addresses how the organization identifies and analyzes risks to achieving its objectives. You cannot design effective controls without understanding what you are trying to protect against.

Key sub-criteria:

- **CC3.1:** The entity specifies objectives with sufficient clarity to identify and assess risks relating to them
- **CC3.2:** The entity identifies risks relevant to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed
- **CC3.3:** The entity considers the potential for fraud in assessing risks to the achievement of objectives
- **CC3.4:** The entity identifies and assesses changes that could significantly impact the system of internal control

What this means in practice: You need a documented risk assessment process that:

- Identifies assets, threats, and vulnerabilities relevant to your services
- Assesses likelihood and impact of potential incidents
- Considers fraud risks (internal and external)
- Is updated periodically or when significant changes occur

The AICPA does not prescribe a specific risk assessment methodology. Organizations commonly use qualitative approaches (low/medium/high ratings), quantitative methods (financial impact estimates), or hybrid frameworks aligned with NIST, ISO 27005, or FAIR [59].

Common implementation: An annual risk assessment documented in a risk register, threat modeling for new systems, periodic reassessments when major changes occur, and evidence that identified risks drive control decisions [60].

CC4: Monitoring Activities

CC4 addresses how the organization monitors whether controls are operating effectively over time. Controls that are designed well but not monitored may degrade silently.

Key sub-criteria:

- **CC4.1:** The entity selects, develops, and performs ongoing and/or separate evaluations, or a combination thereof, to ascertain whether each of the components of internal control is present and functioning
- **CC4.2:** The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate

What this means in practice: You need evidence that controls are tested or reviewed periodically, not just implemented and forgotten. This includes:

- Regular access reviews to verify permissions are appropriate
- Periodic control testing (internal audits or self-assessments)
- Monitoring dashboards that track control performance
- Processes for identifying and escalating control failures

Common implementation: Quarterly access reviews, annual internal control assessments, continuous monitoring tools that alert on policy violations, documented remediation of identified issues [61].

CC5: Control Activities

CC5 is the broadest criterion. It addresses the policies and procedures that help ensure management directives are carried out to mitigate risks to acceptable levels.

Key sub-criteria:

- **CC5.1:** The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels
- **CC5.2:** The entity also selects and develops general control activities relevant to system operations, including programs to address the risk associated with noncompliance with applicable laws and regulations

What this means in practice: This criterion is satisfied by implementing specific controls across all domains: access management, change management, incident response, training, vendor management, and more. CC5 essentially asks: have you designed controls that address your identified risks, and are those controls aligned with applicable legal requirements?

Common implementation: Every control policy and procedure in your program contributes to CC5. The key is demonstrating that controls were selected based on risk assessment results rather than arbitrarily [62].

CC6: Logical and Physical Access Controls

CC6 addresses how access to systems, data, and facilities is restricted to authorized individuals. This is typically one of the most heavily tested areas in SOC 2 audits because unauthorized access is a primary security risk [63].

Key sub-criteria:

- **CC6.1:** The entity implements logical access security software, infrastructure, and architectures over protected information assets to meet its objectives
- **CC6.2:** The entity restricts logical access to software, data, and other assets based on job function or other relationship to the entity, while preventing unauthorized individuals from associating with authorized individuals to gain access

- **CC6.3:** Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity
- **CC6.4:** The entity restricts the assignment of rights or privileges in accordance with management-defined policies based on a user's need to know and job function
- **CC6.5:** The entity identifies and authenticates internal and external users prior to allowing access to data, software, functions, and other system components
- **CC6.6:** The entity restricts the download and upload of protected information assets through interfaces with external parties
- **CC6.7:** The entity manages security credentials, including timely issuance, modification, and removal consistent with an individual's access authorizations throughout the credential lifecycle
- **CC6.8:** The entity modifies or removes individuals' logical access to data, software, functions, and other system components promptly upon changes to or at the end of the individual's employment, engagement, or when management-defined indicators are present
- **CC6.9:** The entity limits physical access to facilities and equipment by authorized personnel through the use of [physical] access controls
- **CC6.10:** The entity authorizes, monitors, and restricts physical access of internal and external users and visitors

What this means in practice: CC6 requires comprehensive identity and access management:

- Multi-factor authentication for accessing systems containing sensitive data
- Role-based access control so employees only have permissions needed for their jobs
- Formal provisioning process with approval before access is granted
- Timely deprovisioning when employees leave or change roles
- Physical access controls for facilities (badges, locks, visitor logs)
- Secure credential management (password policies, key rotation)

Common implementation: Identity provider (Okta, Azure AD, Google Workspace) with MFA enforcement, SSO for all in-scope applications, quarterly access reviews, automated joiner-mover-leaver workflows triggered by HR system changes, documented offboarding checklists [64].

CC7: System Operations

CC7 addresses day-to-day system operations, including monitoring, vulnerability management, and incident response. It ensures systems run securely and issues are detected and addressed promptly [65].

Key sub-criteria:

- **CC7.1:** To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities; and responds to such vulnerabilities appropriately
- **CC7.2:** The entity monitors system components and the operation of those components for anomalies, assessing the security impact of identified anomalies, and taking actions that include determining their cause, responding to them, and reporting them to appropriate personnel within the entity, external parties, or both as required by law, regulation, or contract
- **CC7.3:** The entity implements operational procedures, consistent with control policies, designed to achieve its objectives regarding the security of information and proper processing of data

What this means in practice: You need:

- Regular vulnerability scanning (internal and external) with documented remediation timelines
- Security monitoring (SIEM, log analysis, intrusion detection) that alerts on suspicious activity
- Defined incident response procedures for handling security events
- Operational runbooks that document how systems are managed securely

Common implementation: Monthly or quarterly vulnerability scans using tools like Nessus, Qualys, or cloud-native scanners, centralized logging to a SIEM or log management platform, an Incident Response Plan tested at least annually, documented operational procedures for key systems [66].

CC8: Change Management

CC8 addresses how changes to systems and software are authorized, tested, and implemented. Poor change management is one of the leading causes of security incidents and system outages [67].

Key sub-criteria:

- **CC8.1:** The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, software, systems, and processes to meet its objectives
- **CC8.2:** The entity evaluates and documents the potential security impact of changes to infrastructure, software, systems, and processes prior to implementation to prevent unintended impact on security

What this means in practice: You need a formal change management process that:

- Requires approval before production changes are made
- Includes testing in non-production environments
- Documents what changed, why, who approved it, and when
- Evaluates security implications of changes
- Has rollback procedures for failed changes

For software development organizations, this typically means version control with branch protection rules, required code reviews, automated testing in CI/CD pipelines, and separation between development, staging, and production environments [68].

Common implementation: Git-based workflows requiring pull request approvals before merging to main branches, CI/CD pipelines that run tests automatically, change tickets in a ticketing system for infrastructure changes, documented emergency change procedures with post-implementation review [69].

CC9: Risk Mitigation (Third-Party and Vendor Management)

CC9 addresses how the organization manages risks from third parties, vendors, and business partners. Modern organizations depend heavily on external providers, creating supply chain risks that must be managed [70].

Key sub-criteria:

- **CC9.1:** The entity identifies risks arising from the use of its products or services by user entities, and from the relationship with third parties that directly impact the entity's processing on behalf of user entities
- **CC9.2:** The entity assesses and manages risks associated with vendors and business partners in a manner that supports its objectives

What this means in practice: You need:

- A vendor inventory identifying all third parties with access to your systems or data
- Risk assessments for critical vendors
- Security evaluations during vendor onboarding (questionnaires, SOC report reviews)
- Contracts with security and privacy provisions
- Ongoing monitoring of high-risk vendors

Common implementation: Vendor risk management program with tiered assessment based on risk level, standard security questionnaires for new vendors, review of vendor SOC 2 reports where available, annual reassessments for critical vendors [71].

Availability — Uptime, Performance, and Service Continuity

The Availability criterion applies when the organization has made commitments about system accessibility, such as service level agreements (SLAs) or uptime guarantees. Many SaaS companies, cloud providers, and managed services include Availability in their SOC 2 scope [72].

Availability is organized into three criteria series:

A1: Commitments to Provide Access to the System

- **A1.1:** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors the system's infrastructure, software, data, and procedures to meet its commitments about providing access to the system

What this means in practice: You need evidence that your infrastructure is designed for availability: redundant systems, load balancing, geographic distribution, capacity planning, and monitoring. This includes documented SLAs or service level objectives that define expected uptime and performance [73].

A2: Environmental Protections and Data Backups

- **A2.1:** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives

What this means in practice: You need:

- Environmental controls for facilities (power, cooling, fire suppression) – often inherited from cloud providers
- Regular backups of critical data and systems
- Secure storage of backups separate from production
- Documented backup procedures with defined frequency and retention periods [74]

A3: Recovery Planning and Testing

- **A3.1:** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors recovery plan procedures supporting system recovery to meet its objectives
- **A3.2:** The entity tests recovery plan procedures supporting system recovery to meet its objectives

What this means in practice: You need:

- A disaster recovery plan that defines how systems are restored after major incidents
- Regular testing of backup restoration and failover procedures
- Documented recovery time objectives (RTO) and recovery point objectives (RPO)

- Evidence that tests were performed and results evaluated [75]

When to include Availability: Include this criterion if you have SLAs with uptime commitments, if your customers depend on continuous access to your service, or if downtime would significantly impact their operations. Most SaaS companies and cloud platforms include Availability in their SOC 2 scope [76].

Processing Integrity — Accuracy, Completeness, Timeliness

Processing Integrity applies when the organization processes data and accuracy, completeness, timeliness, or authorization are part of its service commitments. This is common for payment processors, trading platforms, logistics systems, and any service where incorrect processing directly impacts customers [77].

PI1: System Processing Objectives

- **PI1.1:** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors the system's infrastructure, software, data, and procedures to meet its commitments about the accuracy, completeness, timeliness, and authorization of system processing

What this means in practice: You need controls that ensure data is processed correctly: input validation, error handling, reconciliation processes, audit trails for transactions, and monitoring for anomalies in processing outcomes [78].

PI2: Detection and Monitoring of Processing Failures

- **PI2.1:** The entity uses detection and monitoring procedures to identify failures in system processing; assesses the impact of identified failures; and takes actions that include determining their cause, responding to them, and reporting them to appropriate personnel within the entity, external parties, or both as required by law, regulation, or contract

What this means in practice: You need automated monitoring that detects processing errors, alerts on anomalies, triggers remediation workflows, and reports failures to customers when required [79].

PI3: Corrective Action

- **PI3.1:** The entity corrects failed processing and takes action to prevent recurrence of such failures

What this means in practice: You need documented procedures for investigating processing failures, correcting affected data or transactions, implementing fixes, and conducting root cause analysis to prevent recurrence [80].

When to include Processing Integrity: Include this criterion if your service involves processing transactions or data where accuracy matters to customers – payment processing, financial calculations, order fulfillment, medical billing, trading systems, or any scenario where incorrect output directly impacts customer outcomes. If you primarily store and protect data without complex transformation logic, Processing Integrity may not be necessary [81].

Confidentiality — Protecting Sensitive Information

Confidentiality applies when the organization has commitments to protect information designated as confidential throughout its lifecycle. This is common for organizations handling intellectual property, business secrets, legal documents, or other sensitive non-public information [82].

C1: Commitments About Protecting Confidential Information

- **C1.1:** The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors the system's infrastructure, software, data, and procedures to meet its commitments about protecting designated information as confidential during its specified retention period

What this means in practice: You need:

- A data classification policy that identifies what information is confidential
- Access controls restricting confidential data to authorized personnel
- Encryption for confidential data at rest and in transit
- Secure disposal procedures when data reaches end of retention period [83]

C2: Detection and Monitoring of Breaches of Confidentiality

- **C2.1:** The entity uses detection and monitoring procedures to identify breaches of confidentiality; assesses the security impact of identified breaches; and takes actions that include determining their cause, responding to them, and reporting them to appropriate personnel within the entity, external parties, or both as required by law, regulation, or contract

What this means in practice: You need monitoring for unauthorized access to confidential information, alerts on anomalous data access patterns, and incident response procedures for confidentiality breaches [84].

C3: Corrective Action

- **C3.1:** The entity corrects failures of controls related to confidentiality and takes action to prevent recurrence of such failures

What this means in practice: You need documented remediation processes for confidentiality incidents, including root cause analysis and control improvements [85].

When to include Confidentiality: Include this criterion if you handle sensitive business information beyond personal data – trade secrets, proprietary algorithms, financial forecasts, legal documents, merger/acquisition information, or any data where unauthorized disclosure would harm the organization or its customers. Note that if you are already including Privacy (which covers personal data), Confidentiality may overlap significantly unless you also protect non-personal confidential information [86].

Privacy — Personal Data Protection Principles

Privacy applies when the organization collects, uses, retains, discloses, or disposes of personal data. It is based on the AICPA's Generally Accepted Privacy Principles (GAPP), which align with major privacy regulations including GDPR and CCPA [87].

Privacy has seven principle categories:

P1: Management

- **P1.1:** The entity demonstrates accountability for the personal data it controls
- **P1.2:** The entity maps, documents, and monitors its compliance with its published privacy policies and applicable privacy laws and regulations

What this means in practice: You need a designated privacy owner, documented privacy policies, data mapping that shows where personal data flows, and regular monitoring of privacy compliance [88].

P2: Notice

- **P2.1:** The entity notifies individuals regarding the purposes for which personal data is collected, used, retained, and disclosed; the choices and means the entity offers individuals for limiting use and disclosure; and how an individual may contact the entity with questions or concerns about its privacy practices

What this means in practice: You need a clear privacy notice (privacy policy) that explains what data you collect, why, how it is used, and how individuals can exercise their rights [89].

P3: Choice and Consent

- **P3.1:** The entity provides choices and obtains consent regarding the collection, use, and disclosure of personal data for specified purposes as appropriate under law, regulation, or contract

What this means in practice: For sensitive data or marketing uses, you may need explicit consent mechanisms (opt-in checkboxes, preference centers) [90].

P4: Collection

- **P4.1:** The entity limits collection of personal data to that which is relevant for the purposes identified in its privacy notice

What this means in practice: Data minimization – collect only what you need and document why each data element is necessary [91].

P5: Use, Retention, and Disposal

- **P5.1:** The entity uses, retains, and disposes of personal data in a manner that is relevant to the purposes identified in its privacy notice and consistent with applicable laws, regulations, or contracts
- **P5.2:** The entity establishes retention periods for personal data based on business needs and legal requirements

What this means in practice: Defined retention schedules, secure deletion procedures, and controls preventing use of data beyond stated purposes [92].

P6: Access

- **P6.1:** The entity provides individuals with reasonable access to their personal data for the purpose of reviewing and contesting its completeness, accuracy, and timeliness
- **P6.2:** The entity establishes procedures for responding to individual requests regarding their personal data

What this means in practice: Processes for handling data subject access requests (DSARs), including identity verification, response timeframes, and mechanisms for correction or deletion [93].

P7: Quality

- **P7.1:** The entity takes reasonable steps to ensure that personal data is relevant, accurate, complete, and current for the purposes identified in its privacy notice

What this means in practice: Data quality controls, validation at point of entry, processes for updating information, and mechanisms for individuals to correct their data [94].

P8: Security for Privacy (Cross-Cutting)

- **P8.1:** The entity implements security measures consistent with its privacy notice to protect personal data from loss, misuse, and unauthorized access, use, modification, or disclosure

What this means in practice: This overlaps significantly with Security criteria but focuses specifically on protecting personal data [95].

P9: Monitoring and Enforcement

- **P9.1:** The entity monitors compliance with its privacy policies and procedures and takes steps to address any noncompliance

What this means in practice: Regular privacy audits, employee training on privacy obligations, documented remediation of privacy issues [96].

When to include Privacy: Include this criterion if you collect or process personal data (names, email addresses, identification numbers, health information, financial data, etc.) and want formal attestation that your privacy practices meet recognized standards. Many organizations serving EU customers include Privacy to demonstrate GDPR alignment, though SOC 2 Privacy does not replace legal compliance obligations [97].

Selecting Applicable Trust Services Categories

Choosing which Trust Services Categories to include in your SOC 2 report is a strategic decision. Security is mandatory; the others should be selected based on your service commitments and what matters most to your customers [98].

Decision Framework

Use this framework to decide:

1. **Security:** Always included. Required for every SOC 2 report.
2. **Availability:** Include if you have uptime SLAs, if customers depend on continuous access, or if downtime significantly impacts their operations. Most SaaS and cloud services include this.
3. **Processing Integrity:** Include if your service processes transactions or data where accuracy is a core commitment – payments, trading, calculations, order processing. Exclude if you primarily store and protect data without complex transformation.
4. **Confidentiality:** Include if you protect sensitive non-public business information beyond personal data – IP, trade secrets, proprietary documents. Consider excluding if Privacy covers your primary confidentiality obligations.
5. **Privacy:** Include if you handle personal data and want formal attestation of privacy practices. Often included by organizations serving consumers or EU customers.

Practical Considerations

- **Cost impact:** Each additional category increases audit scope and cost by approximately 20-30% [99]
- **Customer expectations:** Ask your largest prospects what they expect. Many enterprise buyers primarily care about Security and Availability
- **Implementation effort:** More categories mean more controls to design, implement, operate, and evidence
- **Overlap:** Controls often satisfy multiple criteria. Encryption protects security, confidentiality, and privacy simultaneously [100]

Common Combinations

- **Security only:** Minimal scope for organizations with basic data protection needs and no uptime commitments
- **Security + Availability:** Most common combination for SaaS companies
- **Security + Availability + Privacy:** Common for consumer-facing services handling personal data
- **Security + Availability + Confidentiality:** Common for B2B services handling sensitive business information
- **All five categories:** Typically only necessary for complex services with broad commitments (e.g., payment processors, healthcare IT platforms)

Summary

The Trust Services Criteria define what auditors evaluate during a SOC 2 examination. Security (Common Criteria CC1-CC9) is mandatory and covers governance, risk assessment, access controls, change management, system operations, monitoring, and third-party risk. Availability addresses uptime and recovery commitments. Processing Integrity covers accuracy and completeness of data processing. Confidentiality protects designated sensitive information. Privacy ensures responsible handling of personal data aligned with GAPP.

Each criterion has specific sub-criteria that define particular aspects of control expectations. Points of Focus provide implementation guidance but are

not mandatory requirements. Organizations select which optional categories to include based on their service commitments and customer expectations, with Security always required.

Understanding these criteria is essential because every control you implement ultimately maps to one or more of them. The next chapters will show how to translate these criteria into practical controls that match your organization's operations.

Chapter 3: Type I vs Type II — Examination Types and Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

SOC 2 Type I — Design Effectiveness at a Point in Time

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Type I Tests

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Type I Timeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Type I Cost

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

When Type I Makes Sense

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Limitations of Type I

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

SOC 2 Type II — Operating Effectiveness Over Time

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Type II Tests

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Type II Timeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Type II Cost

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

When Type II Makes Sense

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

The Observation Period

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Defining System Boundaries and Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Is In Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Is Out of Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Scoping Principles

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Scope Documentation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

The System Description and Management Assertion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

System Description Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative System Description Outline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Management Assertion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Management Assertion

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Inclusion of Subservice Organizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Carve-In vs Include Method

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Using Cloud Provider SOC Reports

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Complementary User Entity Controls (CUECs)

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Typical Examination Timelines and Costs

Type I Timeline Breakdown

Type II Timeline Breakdown

Cost Factors

Cost Breakdown Example (Mid-size SaaS, Type II)

Summary

Chapter 4: Getting Started — Deciding, Scoping, and Planning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Is SOC 2 Right for Your Organization?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

When SOC 2 Makes Sense

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

When SOC 2 May Not Be Appropriate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Decision Checklist

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Defining Organizational and System Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Organizational Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

System Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Scope Documentation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Identifying In-Scope Services and Environments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Service Inventory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Environment Inventory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Infrastructure Inventory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

People Inventory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Documenting Architecture and Data Flows

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

System Architecture Diagrams

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Data Flow Diagrams

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Data Flow Description

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Identifying Stakeholders

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Key Stakeholder Roles

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Establishing Accountability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Building an Implementation Roadmap and Timeline

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Phase-Based Approach

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline Adjustments by Organization Type

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Resource Planning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Budget Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 5: Risk Assessment and Control Mapping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Understanding Risk in the SOC 2 Context

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risk vs Threat vs Vulnerability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risk Appetite and Tolerance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Performing a SOC 2-Aligned Risk Assessment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Step-by-Step Risk Assessment Process

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Risk Register Example

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Identifying Threats, Vulnerabilities, and Impact Scenarios

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Threat Categories for SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Impact Assessment Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Mapping Risks to Controls and Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control-to-Risk Mapping Process

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Risk-to-Control Mapping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Establishing Control Objectives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Good Control Objectives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Examples of Control Objectives

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Building a Control Matrix

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Matrix Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Control Matrix Excerpt

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Using the Control Matrix

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 6: Control Design — Principles and Domains

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principles of Effective Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 1: Align with Risk

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 2: Match Reality

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 3: Be Specific and Testable

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 4: Automate Where Possible

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 5: Generate Evidence Naturally

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 6: Assign Clear Ownership

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Principle 7: Design for Sustainability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Administrative Controls — Policies, Procedures, Governance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Administrative Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Key Administrative Controls for SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Designing Effective Policies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Policy Structure

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Logical and Technical Controls — Systems and Technology

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Technical Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Key Technical Controls for SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Designing Effective Technical Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Physical Controls — Facilities and Access

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Physical Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Key Physical Controls for SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Cloud Provider Physical Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Organizing Controls by Domain for SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Identity and Access Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Change Management and Secure Development

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Vulnerability Management and System Operations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Incident Response

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Data Protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Availability and Business Continuity

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Third-Party Risk Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

People and Culture

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Governance and Oversight

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 7: Identity and Access Management Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

User Provisioning and Deprovisioning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Authentication and Multi-Factor Authentication

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Privileged Access Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Access Reviews and Recertification

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Password Management and Credential Security

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Logical Access Controls and Segregation of Duties

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 8: Change Management and Secure Development Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Change Management Policies and Procedures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Development Environment Separation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Code Review and Approval Processes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Deployment Controls and Release Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Secure Software Development Practices

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Infrastructure as Code and Configuration Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 9: Vulnerability Management, Monitoring, and Incident Response

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Vulnerability Assessment and Scanning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Patch Management Processes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Logging and Audit Trail Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Security Event Detection and Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Incident Response Planning and Procedures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Post-Incident Review and Improvement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 10: Data Protection, Privacy, and Confidentiality Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Data Classification and Handling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Encryption in Transit and at Rest

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Secrets Management and Key Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Data Retention and Disposal

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Privacy Controls and Personal Data Protection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Confidentiality Agreements and Information Sharing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 11: Availability, Business Continuity, and Disaster Recovery

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Availability Monitoring and Alerting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Capacity Planning and Management

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Backup Strategies and Restoration Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Business Continuity Planning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Disaster Recovery Planning and Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Service Level Objectives and Commitments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 12: Vendor Management, Third-Party Risk, and Subservice Organizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Understanding Subservice Organizations in SOC 2

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Carve-In vs Include Method

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Using Cloud Provider SOC Reports

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Third-Party Risk Assessment and Due Diligence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Vendor Security Questionnaires and Assessments

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Contracts, SLAs, and Complementary Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Ongoing Vendor Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Using SOC Reports from Service Providers

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

How to Review Vendor SOC Reports

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 13: People, Training, and Governance Controls

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Security Awareness Training Programs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Employee Onboarding and Offboarding Procedures

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Asset Management and Inventory

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Policy Development and Maintenance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Management Oversight and Review

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Relevant Trust Services Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Governance Structure and Accountability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Design

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 14: Evidence Management and Audit Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Building an Evidence Management Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of the Control

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Risks Addressed

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Program Components

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Guidance

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Requirements

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Weaknesses

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Good Evidence Looks Like

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Strong Evidence

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Evidence Types by Control Category

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Evidence Mistakes to Avoid

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Manual vs Automated Evidence Collection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Automated Evidence Collection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Manual Evidence Collection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Hybrid Approach

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Preparing for the SOC 2 Engagement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Readiness Assessment

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline for Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Auditor Selection

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Engagement Letter

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Auditor Walkthroughs and Interviews

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Purpose of Walkthroughs

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What to Expect

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Preparation Tips

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Responding to Requests and Managing Sampling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Information Request Lists

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Auditor Sampling

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Managing Sampling Effectively

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 15: The Examination, Findings, and Remediation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Happens During the SOC 2 Examination

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Phase 1: Planning and Scoping

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Phase 2: Fieldwork

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Phase 3: Testing and Evaluation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Phase 4: Reporting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

What Auditors Actually Test

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Understanding Exceptions and Deficiencies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Exception vs Deficiency

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Are Exceptions Always Bad?

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Deficiency Severity Levels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Control Deficiency

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Significant Deficiency

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Material Weakness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Opinion Types and Their Meaning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Management Responses to Findings

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

During the Examination

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Management Response in the Report

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Remediation Planning and Execution

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Remediation Planning Steps

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Types of Remediation Actions

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Illustrative Remediation Plan

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Verifying Remediation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Report Review and Post-Audit Activities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Reviewing the Final Report

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Distributing the Report

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Post-Audit Improvement

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Bridge Letters

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 16: Continuous Compliance and Program Sustainability

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Moving from Project to Program

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Project Mode

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Characteristics of Program Mode

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Transition Steps

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Continuous Monitoring and Control Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Automated Monitoring

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Internal Control Testing

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Metrics, Dashboards, and Reporting

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Key Compliance Metrics

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Dashboard Implementation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Annual Planning and Recertification Readiness

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Annual Compliance Calendar

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Recertification Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Managing Changes to Systems, Vendors, and Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

System Changes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Vendor Changes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Scope Changes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Implementation Failures and How to Avoid Them

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Failure 1: Poorly Defined Scope

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Failure 2: Weak Control Ownership

Failure 3: Policies That Do Not Match Actual Practices

Failure 4: Inadequate Evidence

Failure 5: Ineffective Access Reviews

Failure 6: Incomplete Risk Assessments

Failure 7: Weak Change Management

Failure 8: Insufficient Vendor Oversight

Failure 9: Excessive Manual Processes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Failure 10: Last-Minute Audit Preparation

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Chapter 17: Implementation Roadmaps by Organization Type

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Startups and Early-Stage Companies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Strategic Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Priorities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Staffing Recommendations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Tooling Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline and Budget

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Startup Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Small to Mid-Sized SaaS Companies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Strategic Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Priorities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Staffing Recommendations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Tooling Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline and Budget

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Mid-Sized Company Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Growing Technology Companies

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Strategic Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Priorities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Staffing Recommendations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Tooling Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline and Budget

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Growing Company Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Enterprise Organizations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Strategic Considerations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Implementation Priorities

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Staffing Recommendations

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Tooling Strategy

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Timeline and Budget

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Common Enterprise Mistakes

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Choosing Tools and Automation Levels

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Automation Decision Framework

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Compliance Platform Selection Criteria

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

When Automation Is Not Appropriate

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Budget, Staffing, and Resource Planning

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Cost Categories

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Staffing Time Estimates

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Resource Planning Tips

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

Summary

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.

References

This content is not available in the sample book. The book can be purchased on Leanpub at https://leanpub.com/thedefinitiveguidetosoc2.