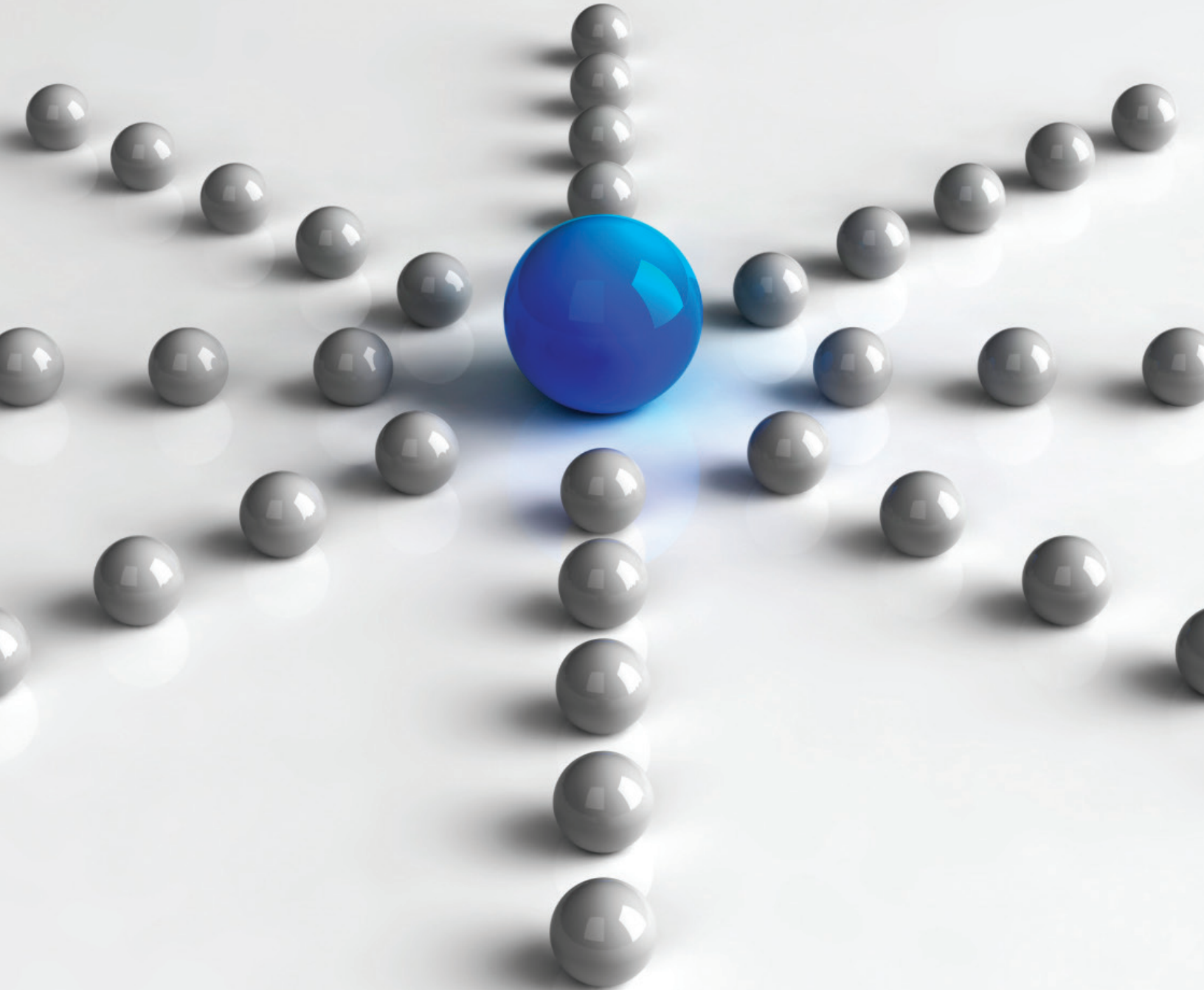


SYSTEM AND ORGANIZATION CONTROLS (SOC)

SOC Suite of Services (SOC 1[®], SOC 2[®], SOC 3[®], SOC for Cybersecurity
and SOC for Supply Chain)





Schneider Downs—SOC Examinations

Your clients and prospects want assurance that you will process their transactions and maintain their data with the utmost integrity and care. How do you respond?

A System and Organization Controls (SOC) Report May Be Your Answer

For your service organization or entity, a cost-effective option is to have Schneider Downs perform a SOC examination. The SOC engagement focuses on the design and operating effectiveness of your organization's control activities. At the conclusion of the engagement, we issue a SOC report that attests to the design and operating effectiveness of your organization's controls, which can be given to your clients.

A SOC examination is often requested by organizations (user entities) that receive significant services from a service organization (organization that provides services critical to the client) and their auditors (user auditors).

Examples of service organizations include:

- Application service providers
- Bank trust departments
- Claims processing centers
- Data centers or other data processing service bureaus
- Investment management firms
- Payroll and billing service providers
- Mortgage, title, closing and appraisal services
- Inventory management
- Software-as-a-Service (SaaS) providers
- Cloud services
- Managed IT services
- Facilities management

Receiving a clean (unqualified) SOC opinion demonstrates to clients that your organization has effective internal controls and related safeguards in place. In addition, the examination may uncover process and control efficiency opportunities. In today's marketplace, an organization's ability to furnish its clients with a SOC report is rapidly becoming requisite.

Organizations are also facing increased pressure from regulators to demonstrate that adequate controls are in place with respect to the processing and safeguarding of their data at remote locations. Regulations, including, but not limited to, Section 404 of the Sarbanes-Oxley Act of 2002 (SOX 404), Gramm-Leach-Bliley (GLBA) Act and Health Insurance Portability and Accountability Act (HIPAA), stress the need for effective internal controls like never before. In response to these and other pressures, user organizations expect strict compliance standards and strong controls to be in place.

Types of Reports

SOC reports provide valuable information regarding an organization's controls and the effectiveness of those controls, which may also satisfy the user auditor's needs.

The following types of SOC examinations aid in assessing an organization's controls:

- **SOC 1 - Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting** - This report type is specifically designed to meet the needs of user entities and user auditors to evaluate the effect of the controls at the service organization on user entities' financial statements. Use of this report is restricted.
- **SOC 2 - Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality and/or Privacy** - This report is intended to meet the broad range of users that need information and assurance about the controls at a service organization that affect the security, availability and processing integrity of the systems processing users' data and the confidentiality and privacy over the data. Use of this report is generally restricted to parties that have knowledge of a service organization's services and IT environment.

- SOC 2+ - Same as the SOC 2 report, but contains additional criteria to address other compliance requirements. Examples include:
 - » HITRUST CSF
 - » ISO 27001
 - » ALTA
 - » HIPAA
 - » PCI
 - » NIST (FISMA)
 - » COBIT 5
 - » DEA Final Rule on Electronic Fulfillment of Controlled Substances
 - » Cloud Security Alliance

Two types of reports are available for SOC 1 and SOC 2 engagements: Type 1 and Type 2. A Type 1 report assesses the design of controls within the environment at a specific date in time. A Type 2 report is issued covering a period of time, and assesses both the design and operating effectiveness of controls to conclude if the controls are suitably designed and operating effectively.

- SOC 3 – This report is designed to meet the needs of users who desire assurance about the controls at a service organization that cover the same five categories as the SOC 2, but do not have the need for or the knowledge necessary to make effective use of the details contained in a SOC 2 report. Because they are general use reports, SOC 3 reports can be freely distributed or posted on a website.
- SOC for Cybersecurity – This report provides stakeholders with information regarding an organization’s cybersecurity risk management program. The report provides a means for organizations to demonstrate that they are effectively managing cybersecurity threats.
- SOC for Supply Chain – This is an internal controls report on an entity’s system and controls for producing, manufacturing or distributing goods to better understand and manage the risks arising from business relationships with their supplier and distribution networks.

Our Approach

At Schneider Downs, our approach leverages the knowledge and project management expertise of our professionals from various disciplines, including information technology and internal and external audit. The engagement begins with a pre-assessment of the organization’s controls in order to gain a high-level understanding of the significant controls in place

over essential processes. Next, we work with your management team to develop a project management plan and an approach that will ensure that your expectations are met and the engagement is completed within the specified time frame. We then evaluate the test results to determine the operating effectiveness of the controls and report our results.

Trust Our Experience

Schneider Downs provides an experienced and proven group of professionals who specialize in SOC examinations. This team is composed of multidisciplinary professionals experienced in providing audit and attest services, internal audit and risk advisory services, IT audit and cybersecurity services. By integrating a diverse group of experienced individuals within the SOC process, Schneider Downs is able to provide unique and value-added insight to clients. Our team works with clients across the country and is well recognized for its experience and service model.

For more information, please contact:

Eric M. Wright, Shareholder
(412) 697-5328 or ewright@schneiderdowns.com

Heather A. Haemer, Practice Co-Director
(412) 697-5433 or hhaemer@schneiderdowns.com

Holly L. Russo, Practice Co-Director
(412) 697-5337 or hrusso@schneiderdowns.com



From the start, Schneider Downs was an extremely thorough, knowledgeable and valuable partner. Schneider Downs took the time to understand our specific goals and prepared us well, ensuring that the audit process was seamless and efficient.



Elizabeth Sullivan
President and CEO, Integrated Health 21

ONE OF THE
60 LARGEST
ACCOUNTING AND
BUSINESS ADVISORY
FIRMS IN THE
UNITED STATES

FOUNDING MEMBER OF
PRIMEGLOBAL
INTERNATIONAL
ASSOCIATION
OF ACCOUNTING
FIRMS, WITH
REPRESENTATION ON
THE ASSOCIATION
BOARDS,
COMMITTEES AND
MANAGEMENT

REGISTERED WITH
PCAOB
TO AUDIT PUBLIC
COMPANIES

60+
YEARS OF STABILITY

Established in 1956, Schneider Downs has grown to be the largest regional independent registered public accounting and business advisory firm with nearly 500 personnel. Schneider Downs provides over 80 service offerings from the Schneider Downs group of companies as depicted below:

AUDIT

- Financial Statement Audit
- Review and Compilation
- SEC
- Consulting on New Standard Implementation
- Risk Advisory
- ERISA
- SOC

TAX

- Traditional Compliance
- International
- State and Local Tax
- Tax Accounting
- Employee Benefits
- Cost Segregation
- Co-Sourcing/Outsourcing

CORPORATE FINANCE

- Mergers and Acquisitions
- Buy Side
- Corporate Finance
- Sell Side

WEALTH MANAGEMENT

- 401(k) Plan Management
- High Net Worth

INDUSTRIES SERVED

- | | |
|--------------------------|------------------------------|
| • Automotive | • Government |
| • Construction | • Manufacturing |
| • Higher Education | • Not-for-profit |
| • Employee Benefit Plans | • Real Estate |
| • Energy & Resources | • Retail/consumer |
| • Financial Services | • Transportation & Logistics |



BUSINESS ADVISORS

- Productivity Improvement
- Business Valuation
- Forensic Accounting/ Litigation Support
- Transaction Advisory Services

TECHNOLOGY

- Software Solutions
- Process Reengineering
- Security Vulnerability Testing
- Software Selection
- Internal Control Assessment
- Review of Ongoing Technology Operations
- Cybersecurity
- Robotic Process Automation

GLOBAL REACH

Schneider Downs' global service delivery model incorporates the PrimeGlobal association of over 300 highly successful independent public accounting firms with a combined annual revenue of more than US\$2.5 billion. PrimeGlobal's independent member firms house a combined total of 2,500 partners, 16,300 employees, and 900 offices in 80 countries around the globe.

Our Risk Advisory practice works with member firms throughout the United States and in Canada, Europe, Asia Pacific, Central America, South America and Australia to coordinate our clients' international business needs.

