schellman

Quality, above all.

Portfolio Cybersecurity Assessments for Private Equity & Venture Capital Firms

Protect all of your investments continuously.

Not only are small and medium size businesses (SMBs) attractive to private equity and venture capital firms, but these same companies are also prime targets for cybersecurity attacks. SMBs focus on growth and can have gaps in security resources and expertise. Lack of sufficient protections and investment in good cybersecurity hygiene can cost SMBs their livelihood and negatively affect investor returns.

Increase visibility to threats and monitor portfolio for cybersecurity hygiene.

As a national leader in attestation, compliance, and certification services, Schellman is uniquely positioned to assist private equity, venture capital, and other firms that manage companies as part of a portfolio of investments, partnerships, and other strategic relationships. With Schellman's Portfolio Cybersecurity Assessments, PE/VC firms are armed with KPIs and performance criteria related to the security posture of each of their portfolio companies. These assessments provide a comprehensive perspective on cybersecurity threats by using a consistent assessment framework and presenting the findings in a clear and actionable manner. This approach of continued due diligence helps to protect and create value for your investments.

Service Offerings

Level of oversight is important and should be tailored to your portfolio. Schellman has different assessments based on specific operating needs. We have created a three-tiered assessment approach:

	LEVEL 1 **Baseline Assessment**	**LEVEL 2** **Additional Controls and Requirements Assessment**	**LEVEL 3** **Advanced Controls Assessment**
Initiation Phase – Portfolio Dashboard	✓	✓	✓
Assessment of 12 Control Areas Using Online Questionnaire for Data Collection and Aggregation	✓	✓	✓
Assessment of Core Cybersecurity Domain Areas Via Remote Interview & Analysis		✓	✓
Assessment in Accordance with Specified Standards (SOC 2, SOC for Cybersecurity, etc.)			✓
Report Designed for Internal Stakeholder Use	✓	✓	✓
Report(s) Designed for External Stakeholder Use			✓
Presentation of Results to Operating Team	✓	✓	✓
Presentation of Results to BoD or Broader Stakeholder Group		✓	✓

Approach & Methodology

INITIAL PORTFOLIO INVENTORY

Regardless of your Portfolio Cybersecurity Assessment service level, the first phase of engagement with Schellman begins with a high-level review of the entire portfolio. Each company is inventoried and categorized. This initiation phase allows Schellman to determine the best places to focus efforts during the assessment. Together with the operating team, Schellman will develop a strategy for the assessments that each portfolio company will undergo.

ASSESSMENT PHASE

Depending on the service level, the assessment approach varies:

Level 1 - Baseline Assessment – Schellman will review baseline information about the compliance maturity of each portfolio company via an online questionnaire. This information allows Schellman to determine if basic cybersecurity controls and/or compliance requirements are in place. Throughout the assessments, a dashboard with metrics and results will be continuously updated. At the conclusion of data collection and aggregation, a summary report is created for the operating team. The data points to be collected as part of this assessment are:

- Available existing security compliance reports (SOC 2, ISO 27001, etc.)
- Penetration testing
- Security Policy
- Protection of data whether at-rest, during processing, or in-transit
- Operating location and/or use of third-party cloud providers
- Incident management and response

Approach & Methodology

ASSESSMENT PHASE (CONT.)

Level 2 - Additional Controls and Requirements Assessment – In addition to the online questionnaire, Schellman will conduct remote interviews and walkthroughs with each portfolio company to gather detailed information related to their cybersecurity controls. These details allow Schellman to perform a robust analysis of the security posture of each company. As with the Level 1 assessment, a dashboard with metrics and results will be updated throughout the assessment phase. At the conclusion of the assessments, a summary report will be created for the operating team as well as a presentation on assessment results to interested parties. In addition to the Level 1 evaluation topics, the following areas will also be covered:

- User identification, authentication, authorization, and credentials management
- Physical and logical access provisioning and de-provisioning
- Remote access
- Privileged account management
- IT asset management
- Patch management
- Software development lifecycle processes
- Scanning and vulnerability management
- Security event management and monitoring
- Data backup and replication
- Business continuity and disaster recovery
- Data retention and deletion

Approach & Methodology

ASSESSMENT PHASE (CONT.)

Level 3 – Advanced Controls Assessment – Schellman will conduct a formal audit, remote or onsite, of all portfolio companies providing formal reports highlighting each organizations' controls against known and relevant standards and frameworks (i.e., SOC 2, SOC for Cybersecurity, NIST, etc.). These audits can be shared both within the PE investor base and/or portfolio company customers.

- System and application change control processes
- Data loss prevention
- Business continuity and disaster recovery testing
- Incident response testing
- Information classification

BLUSTAR

BLUESTAR, INC.
CYBERSECURITY ASSESSMENT
AS OF
MAY 15, 2022

Cybersecurity Assessment Services

schellman
Quality, above all.

Overall Program Management

Expect a high level of professionalism and care when it comes to Schellman's services.

Our dedicated management team model will create a streamlined and consistent experience for your portfolio companies. Assessments from year-to-year will be maintained, which allows your operating team to identify trends, gage maturation of security posture among investment companies, and track KPIs relevant to security risk. Our project management approach includes:

- A Principal and/or Director that manages the overall relationship between your Firm and Schellman.
- A dedicated manager that ensures planning and organization of the assessments is established, directs the completion of each portfolio company assessment, and delivers the results as status updates and formal reports.
- Engagements are staffed by assessors with the appropriate experience and necessary credentials to conduct the assessments.
- Issues are proactively and immediately discussed with the project sponsor and/or designee.
- The PE/VC firm and portfolio companies have constant access to the Schellman team, in particular the management team.

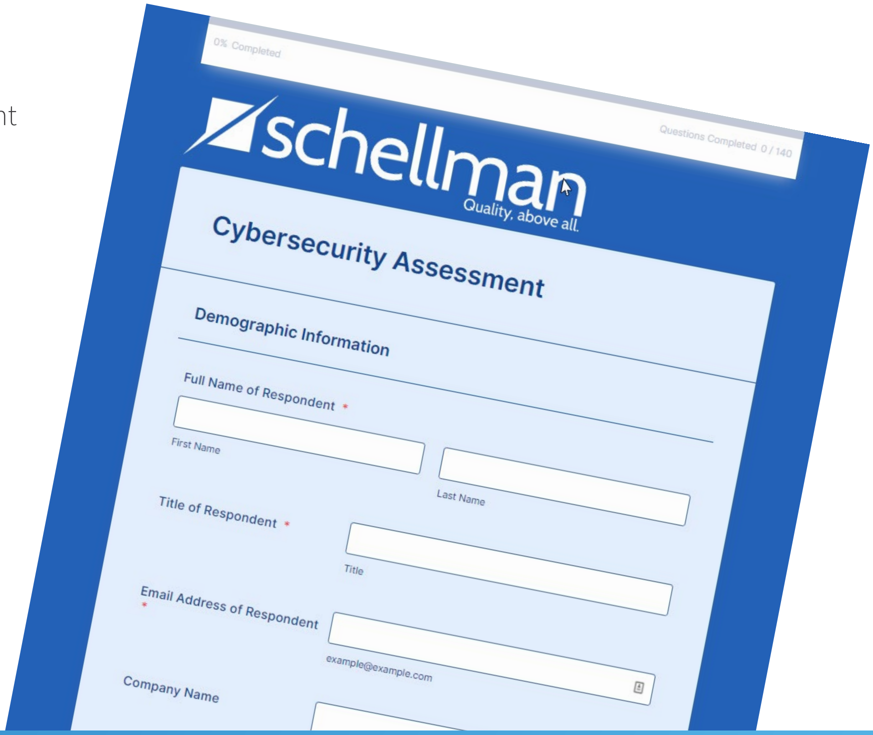
Creating Value Beyond Assessments

Working with Schellman for cybersecurity assessments not only allows your PE/VC firm to gain valuable insight into its investments, but it also establishes a unique opportunity for portfolio companies to take their compliance journey to the next level. Having established a baseline understanding and rapport with these companies, Schellman is able to offer discounted rates for attestation and compliance engagements outside of these standard cybersecurity assessments. Having certifications, attestations, and compliance reports against industry-known standards allows companies to win new business and establish contracts with reputable global organizations.

Fees and timing for Portfolio Cybersecurity Assessments depend on two factors:

- Level of Service:
  - Level 1 - Baseline Assessment
  - Level 2 - Additional Controls and Requirements Assessment
  - Level 3 – Advanced Controls Assessment
- Size of portfolio – number of companies

To learn the fees and timing for your portfolio, a discussion to better understand your specific situation is required.
We then develop a proposal that is tailored to your needs.



Cybersecurity Assessment

Demographic Information

Full Name of Respondent *

First Name

Last Name

Title of Respondent *

Title

Email Address of Respondent *

example@example.com

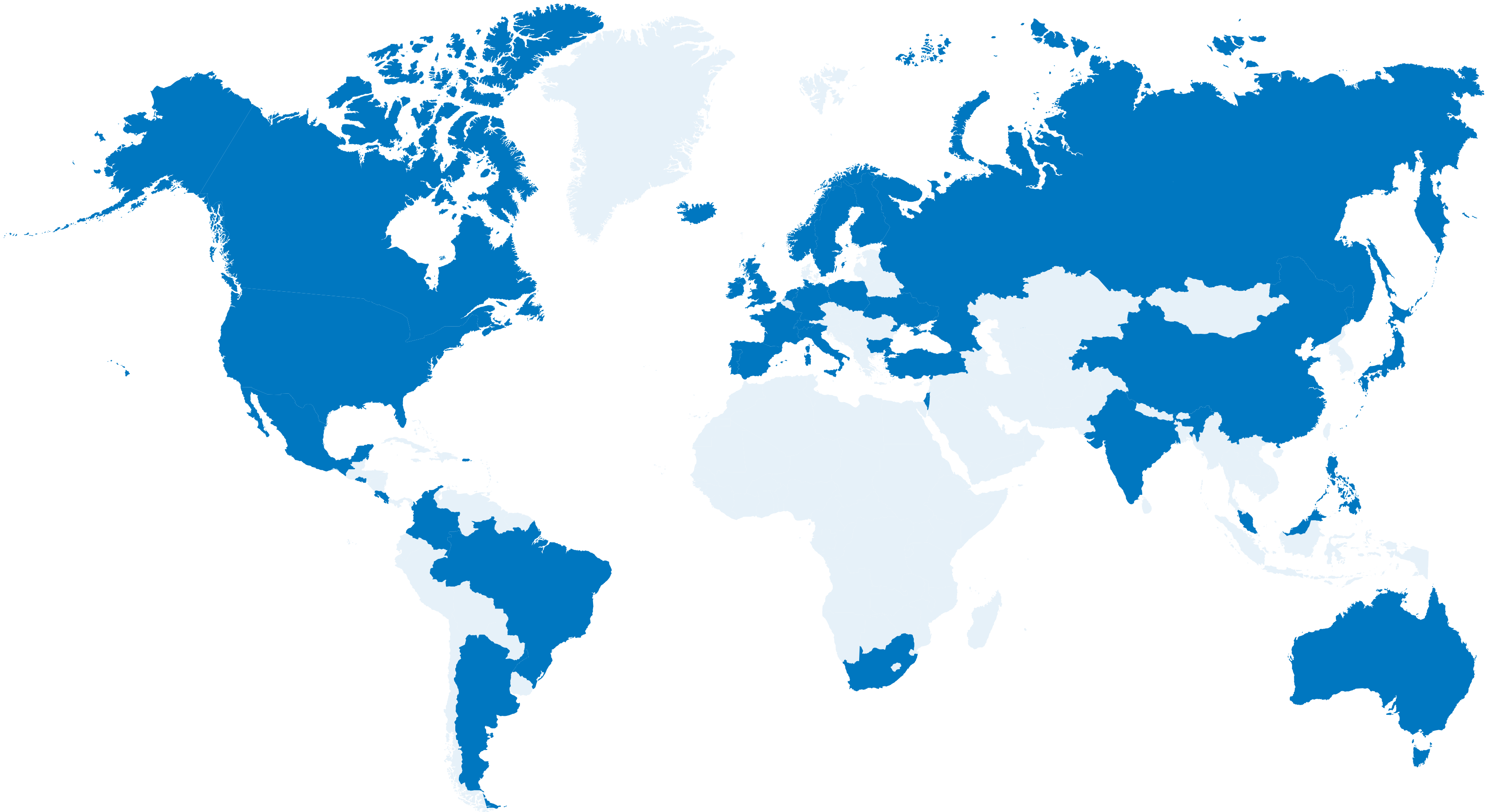
Company Name

The Schellman Advantage

A single team offers clients the unique opportunity to meet multiple compliance requirements. Our examinations are performed by integrated project teams, which drastically reduce duplication of efforts, site visits, and overhead caused by a multi-vendor approach, resulting in significant cost savings.

Our Global Reach

We annually perform over 3,000 projects spanning more than 50 countries



Our People

"I would like to commend the professionalism and thoroughness of the examiners. They were well-prepared, excellent communicators, and worked to understand a complex business and its implications. The experience exceeded my expectations in terms of working with a team of auditors."

- Critical Informatics

Our Process

"The most impact this team had with our team was the willingness to understand the business, the infrastructure and not make assumptions which saved valuable time and resources. Schellman to us will always be recommended as best of class. Thank you."

- Zillow

Our Technology

"The entire IT Security team very much liked working in AuditSource as well, and felt that the organization and communication that AuditSource offered was a huge boon and made evidence gathering much easier and clearer than any system we'd used before. Overall we were very pleased with our SOC2 audit with Schellman."

- On-Line Strategies Services LLC

Trusted By

Microsoft

ORACLE

MCKESSON

facebook

cisco

box

DocuSign

EQUINIX

Dropbox

intuit

IRON MOUNTAIN

slack

THOMSON REUTERS

Canon

Unified Compliance Strategy

SOC Examinations

Healthcare Assessments

ISO Certifications

Cloud Security Assessments

Federal Assessments

CSA STAR Programs

Payment Card Assessments

Privacy Assessments

Cybersecurity Assessments

Financial Services Assessments

Schellman can provide SOC, PCI, ISO, FedRAMP, HITRUST, and Security Assessment services through a single project team.

Breaking Down Inefficiencies

Schellman has a streamlined process to help decrease the touch points that may cause inefficiencies for your company:

- Schellman performed an analysis of the objectives / requirements and supporting control activities to identify overlap and leverage
- Schellman performed a high level overview and has identified controls, testing methods, and evidence that can be consolidated and leveraged across the various assessments.
- Additional controls analysis will be performed for new engagements or engagements with a revised scope to ensure efficiencies can be gained across assessments.
- Client evidence and sample selections will be requested once and leveraged across all reports with corresponding and/or overlapping reporting periods.
- Interviews and documentation will be leveraged across all reports.

Bios

Doug Barbin

Principal

24 Years of Experience

About

Doug Barbin is responsible for the development, growth, and delivery of Schellman's global services portfolio. Since joining in 2009, his primary focus has been to expand our strong foundation in IT audit and assurance to make Schellman a market leading diversified cybersecurity and compliance services provider. He has developed many of Schellman's service offerings, served global clients, and now focuses on leading and supporting the service delivery and practice leaders.

Doug brings more than 25 years' experience in technology focused services. Prior to Schellman, he was the head of product for VeriSign's managed security services business leading to its sale to SecureWorks in 2009. Doug also was a director in VeriSign's consulting practice and separately had roles of CTO/COO for a specialty mortgage insurance company and law firm. He started his career in forensic accounting at Price Waterhouse (then PwC) where he co-started the firm's first computer forensics practice.

Doug holds dual-bachelor's degrees in Accounting and Administration of Justice from Penn State as well as an MBA from Pepperdine. He has also taken post graduate courses on Artificial Intelligence from MIT. He speaks globally on cloud security and compliance, maintains multiple CPA licenses and in addition to most of the major industry certifications including several he helped create.

Certifications

Certified Public Accountant (Multi-State CPA)
Certified Information Privacy Professional (CIPP)
Certificate of Cloud Security Knowledge (CCSK)
ISO 27001 Lead Auditor
Certified Information Systems Security Professional (CISSP)
Payment Application Qualified Security Assessor (PA-QSA)
Payment Card Industry Qualified Security Assessor (PCI QSA)

Education

Master of Business Administration
  Pepperdine University
Bachelor of Science in Administration of Justice
  Penn State University
Bachelor of Science in Accounting
  Penn State University
Executive Program in Artificial Intelligence, MIT

About

Jason Rhoades is a Principal at Schellman, where he oversees multiple compliance and security services including SOC, PCI-DSS, ISO, FISMA and HIPAA services. He helps assist large and complex customers who have multiple compliance needs, strategically aligning their compliance portfolio to maximize cost savings and efficiencies. Jason also leads our Financial Services practice which focuses on cybersecurity and regulatory frameworks such as NIST CSF, SWIFT, NYDFS, FFIEC and many others. In addition, he works with many leading organizations spanning multiple industries such as Fintech, cloud computing (including IaaS and SaaS models), healthcare, cybersecurity and many others.

Jason Rhoades

Principal

21 Years of Experience

Certifications

Certified Public Accountant (CPA)

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Auditor (CISA)

Certified Internal Auditor (CIA)

Certificate of Cloud Security Knowledge (CCSK)

Payment Card Industry Qualified Security Assessor (PCI QSA)

ISO 27001 Lead Auditor

Education

Bachelor of Science in Accounting
Appalachian State University

About

Kristen Wilbur is a Director at Schellman, with over 12 years of experience in providing IT attestation and compliance services. Kristen has evaluated risk and controls for Global 1000, Fortune 500, and regional companies during the course of her career with a strong focus in the technology sector. Kristen currently leads the New York City practice at Schellman where she specializes in SOC 1, SOC 2, ISO 27001, and HIPAA reporting. In her portfolio she also oversees large scale engagements that include assessments around FedRAMP, HITRUST, and Privacy. Kristen has a strong passion for giving back and recently helped to establish the corporate social responsibility program at Schellman called SchellmanCARES.

Kristen Wilbur

Director

12 Years of Experience

Certifications

Certified Public Accountant (CPA)

Certified Information Systems Auditor (CISA)

Certified Information Systems Security Professional (CISSP)

Certificate of Cloud Security Knowledge (CCSK)

ISO 27001 Lead Auditor

AICPA Advanced SOC

Education

MBA

University of Albany

Bachelor of Arts in Criminal Justice & Sociology

University of Albany

About

Bryan Harper is a Manager with Schellman. Prior to joining Schellman, Bryan worked as a Senior IT Auditor, specializing in SOC examinations. Bryan also worked as a staff accountant in a public accounting firm performing financial audits, consulting, and outsourced internal audit engagements for clients in the banking, insurance, and healthcare industries. Bryan is now focused primarily on SOC examinations for organizations across various industries. At Schellman, Bryan is involved with technical training development specific to auditing cloud services and supports Schellman's cybersecurity task force, which is responsible for monitoring developments in and responding to cybersecurity regulations and related cybersecurity compliance frameworks.

Bryan Harper

Manager

9 Years of Experience

Certifications

Certified Public Accountant (CPA)

Certified Information Systems Security Professional (CISSP)

Certified Information Systems Auditor (CISA)

Certificate of Cloud Security Knowledge (CCSK)

AWS Certified Solutions Architect

AICPA Advanced SOC

ISO 27001 Lead Auditor

Education

Master of Science in Accounting
  Texas A&M Commerce

Bachelor of Science in Accounting
  College of New Jersey

About

Brett Hayes is a manager with Schellman based in Los Angeles, California. Prior to joining Schellman in 2016, Brett worked as a senior consultant at big four accounting firm, specializing in Sarbanes-Oxley compliance audits and SOC 1 examinations. Brett also led and support various other projects, including IT advisory engagements. Brett has over nine years of experience comprised of serving various industries including technology, financial services, and healthcare. Brett is now focused primarily on SOC, HIPAA, and ISO services for organizations across various industries.

Brett Hayes

Manager

12 Years of Experience

Certifications

Certified Information Systems Security Professional (CISSP)

Certificate of Cloud Security Knowledge (CCSK)

Certified Information Systems Auditor (CISA)

AICPA Advanced SOC

Education

Bachelor of Science in Business Administration

Kansas State University

About

Jeannette Buttler is a manager with Schellman based in New York, New York. Prior to joining Schellman in 2021, Jeannette worked as a senior manager, for an accounting firm specializing in IT attestation and compliance services. She also led and supported various other projects, including NYDFS compliance, SOX and SOC projects. Jeannette has over 8 years of experience comprised of serving companies of all sizes, including start-ups, Fortune 1000, and publicly traded companies, with a strong focus on technology (including digital currency and blockchain) and financial services sector. Jeannette is now focused primarily on SOC engagements for organizations across various industries.

Jeannette Buttler

Manager

8 Years of Experience

Certifications

Certified Information Systems Security Professional (CISSP)

Certified Public Accountant (CPA)

Certificate of Cloud Security Knowledge (CCSK)

Certified Information Systems Auditor (CISA)

Certified Internal Auditor (CIA)

AICPA Advanced SOC

Education

Bachelor of Science in Accounting
University at Buffalo

Master of Business Administration in Accounting
University at Buffalo

schellman

Quality, above all.

www.schellman.com

4010 W Boy Scout Blvd, Suite 600 / Tampa, FL 33607 / 1.866.254.0000

Outside of the United States, please dial: +1.813.288.8833