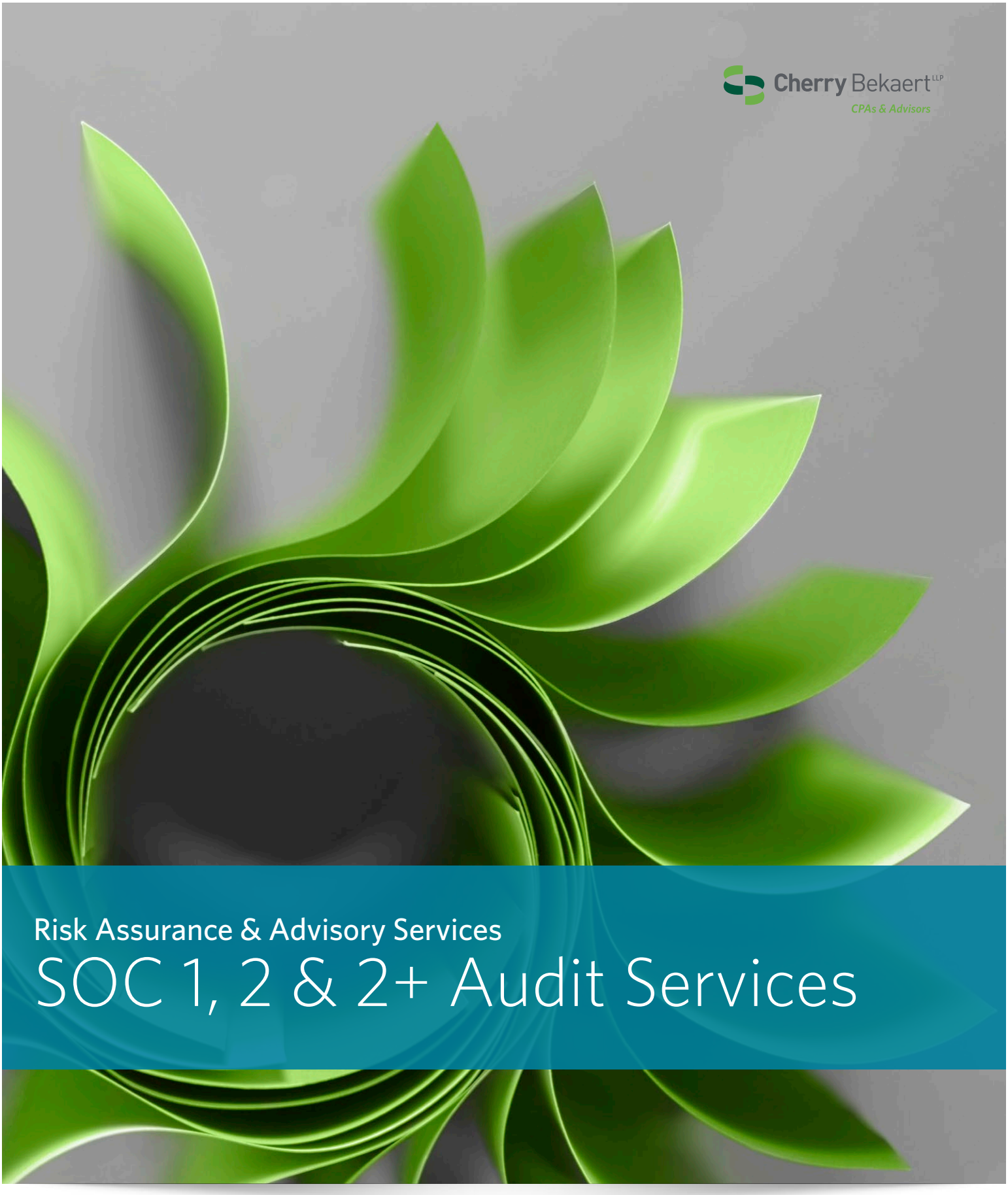


Risk Assurance & Advisory Services

SOC 1, 2 & 2+ Audit Services

Cherry Bekaert's Audit Services

With more companies outsourcing their financially significant and information technology services to third parties, it has become critical for user organizations to understand each service entity and its internal controls.

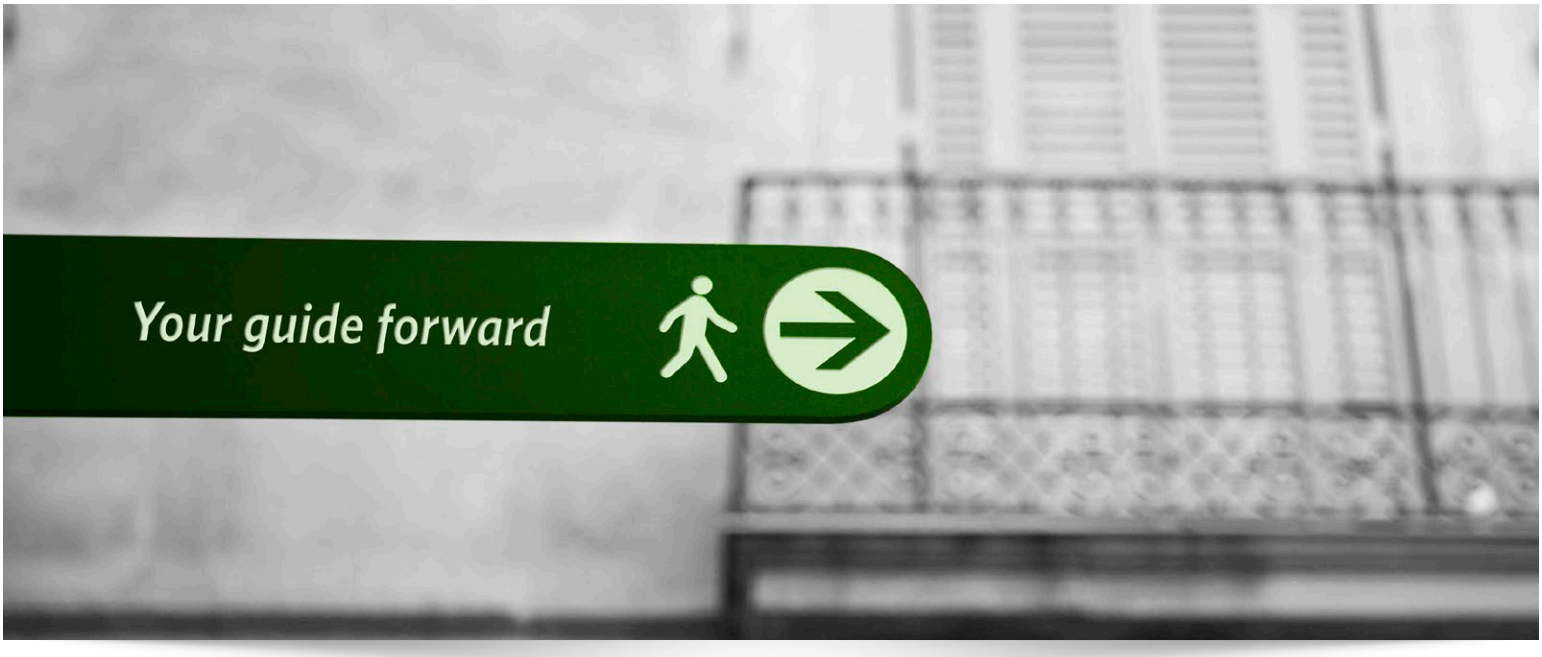
For 70 years, we have efficiently guided clients in minimizing operational and compliance risks and maximizing opportunities, while keeping an eye on the unexpected.

System and Organization Controls (SOC 1, SOC 2, & SOC 2+)

System and Organization Controls (SOC) reports allow organizations that perform information system and transaction processing services to other entities to demonstrate that they maintain effective internal controls by periodically issuing a report that is independently assessed by a certified public accountant.

Identifying The SOC Report That Is Right For You

Will the report be used by your customers and their auditors to plan and perform an audit or integrated audit of your customer's financial statements?	Yes	SOC 1
Will the report be used by your customers as part of their compliance with the Sarbanes-Oxley Act or similar law or regulation?	Yes	SOC 1
Will the report be used by your customers or stakeholders to gain confidence, and place trust in a service organization's systems?	Yes	SOC 2
Do your customers have the need for and ability to understand the details of the processing and controls at a service organization, the tests performed by the service auditor and results of those tests?	Yes	SOC 2
Do you wish to incorporate another framework (i.e., HIPAA/HITRUST, ISO, NIST, etc) to your SOC 2 report?	Yes	SOC 2+



Cherry Bekaert's Risk Assurance & Advisory Services

Relying on a SOC 1 or SOC 2 report from an independent certified public accounting firm can provide assurance to user organizations & their auditors, as well as key stakeholders and/or prospective clients that a third-party service provider's system of internal control is sound.

Our Risk Assurance & Advisory (RAS) experts have over three decades of SOC 1 and SOC 2 experience across a multitude of industries. Whether its preparing a third party for their first SOC 1 or SOC 2 audit with our readiness assessment services, or completing a SOC 1 or SOC 2 audit engagement, our experts work closely with your organization to ensure that all your needs are met. We recognize that each third-party organization is different no matter if the service provided, or industry operated in, are the same. Our clients do not rely a one-size fits all approach, so why should we?

SOC 1 Report

Report on Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting

These reports, prepared in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 18, Reporting on Controls at a Service Organization, meet the needs of customer organizations and customer organization auditors to understand internal controls associated with processing transactions that are important to the organizations' financial statements. Customer organization auditors evaluate these reports in the planning of their financial statement audits. SOC 1 reports may be either Type I or Type II as described to the right:

Type I

Report on the fairness of the presentation of management's description of the system and the suitability of the design of the controls as of a specified date.

Type II

Report on the fairness of the presentation of management's description of the system, and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives included in the description throughout a specified time period (typically 6 or 12 months).

Understanding the Service Organization

The service organization may perform control processes relevant to the user entity controls which are intended to mitigate risks related to security, availability, processing integrity, confidentiality, and/or privacy and are intended to assist management of a user entity in carrying out its responsibility for monitoring the services it receives, including the operating effectiveness of a service organization's controls over those services.

Questions that May Help Assess the Operational & Compliance Risks of a User Entity (not an all-inclusive list)

What risk is of concern as it relates to the service organization services?

Is there concern related to processing being adequately designed/ operating effectively to achieve operational and compliance objectives?

Is assurance needed regarding other internal controls and/or security of the outsourced operations?

What data, application and transaction processing is being performed by a service organization?

What is the risk related to adherence to other performance/contractual expectations?

How is information protected? What policies, procedures, communications and monitoring support the security, confidentiality and privacy of information being processed/stored?

How is information available? What policies, procedures, communications and monitoring support the availability and processing integrity of information being processed?

How do the operational and compliance controls at the service organization compare to existing user entity controls?

What documentation on how the environment and services are assessed for risk and controls is available to the user entity?

What is the separation of compliance responsibilities between the service organization and the user entity?

Examples of Services Provided by Service Organizations

Cloud Computing

Providing on-demand network access to a shared pool of configurable computing resources. Examples include networks, servers, storage, applications and services.

Financial Services Customer Accounting

Processing financial transactions on behalf of customers of a bank or investment company. Examples are processing customer securities transactions, maintaining customer account records, providing customer transaction confirmations and statements, and providing related customer services through the Web.

Contact Center for Customer Service

Providing customers of user entities with online or telephonic post-sales support, and service management. Examples of these services are warranty inquiries and processing, troubleshooting and responding to customer complaints.

Logical Security Management

Managing access to networks and computing systems for user entities. Examples include granting access to a system and preventing, or detecting and mitigating, system intrusion.

Sales Force Automation

Providing and maintaining software to automate business tasks for user entities that have a sales force. Examples of such tasks are order processing, information sharing, order tracking, contact management, customer management, sales forecast analysis and employee performance evaluation.

Healthcare Claims Management

Providing medical providers, employers, and insured parties of employers with systems that securely and confidentially support the processing of medical records, and related health insurance claims.

SOC 2 & SOC 2+ Reports

Report on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy

SOC 2 reports are intended to meet the needs of a 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 the service organization uses to process users' data, and the confidentiality and privacy of the information processed by these systems. Examples of stakeholders who may need these reports are:

- Management or those charged with governance of the user entities and of the service organization;
- Customers of the service organization; and
- Regulators, business partners, suppliers, and others who have an understanding of the service organization and its controls.

These reports can play an important role in:

- Oversight of the organization
- Vendor management programs
- Internal corporate governance and risk management processes
- Regulatory oversight

SOC 2 reports may be either Type I or Type II as described below:

Type I

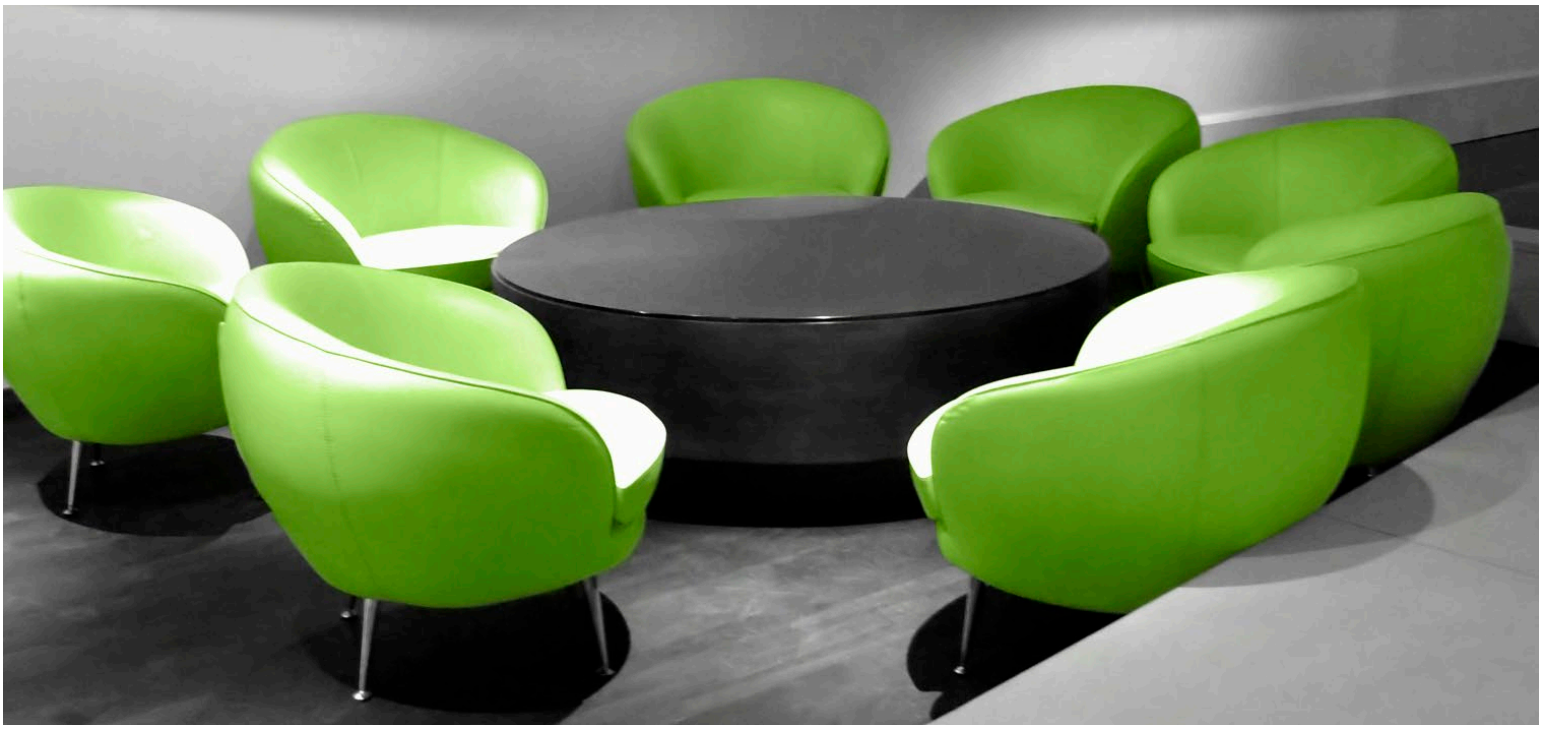
Report on management's description of a service organization's system and the suitability of the design of controls at a moment in time.

Type II

Report on management's description of a service organization's system, and the suitability of the design and operating effectiveness of controls over a period of time (typically 6 or 12 months).

In addition, the AICPA allows service providers to incorporate other frameworks into their SOC 2 audit resulting in what is referred to as a SOC 2+. These reports can be used to demonstrate assurance in areas that go beyond the Trust Services Principles in order to include compliance with various regulatory and industry frameworks. Examples include:

- NIST 800-53 or 171
- ISO 27001
- HITRUST (HIPAA Compliance)
- PCI
- Cloud Security Alliance (CSA)



Comparing SOC Reports

	Under what professional standard is the engagement performed?	What is the subject matter of the engagement?
1	SSAE No. 18 AT-C section 320 AICPA Guide, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting (SOC 1) effective January 1, 2017	Controls at a service organization relevant to user entities internal control over financial reporting.
2	SSAE No. 18 AT-C section 205, Attestation Engagements AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy	Controls at a service organization relevant to security, availability, processing integrity confidentiality or privacy. If the report addresses the privacy principle, the service organization's compliance with the commitments in its statement of privacy practices.

To provide information to the auditor of a user entity's financial statements about controls at a service organization that may be relevant to a user entity's internal control over financial reporting. It enables the user auditor to perform risk assessment procedures, and if a Type II report is provided, to assess the risk of material misstatement of financial statement assertions affected by the service organization's processing.

A description of the service organization's system.

A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a Type II report, the operating effectiveness of the controls.

In a Type II report, a description of the service auditor's tests of the controls and the results of the tests.

Auditors of the user entity's financial statements, management of the user entities, and management of the service organization.

What is the purpose of the report?

To provide management of a service organization, user entities and other specified parties with information and a CPA's opinion about controls at the service organization that may affect user entities' security, availability, processing integrity, confidentiality or privacy.

A Type II report that addresses the privacy principle also provides a CPA's opinion about the service organization's compliance with the commitments in its statement of privacy practices.

What are the components of the report?

A description of the service organization's system.

A service auditor's report that contains an opinion on the fairness of the presentation of the description of the service organization's system, the suitability of the design of the controls, and in a Type II report, the operating effectiveness of the controls.

If the report addresses the privacy principle, the service auditor's opinion on whether the service organization complied with the commitments in its statement of privacy practices.

In a Type II report, a description of the service auditor's tests of controls and the results of the tests.

In a Type II report that addresses the privacy principle, a description of the service auditor's tests of the service organization's compliance with the commitments in its statement of privacy practices and the results of those tests.

Who are the intended users of the report?

Parties that are knowledgeable about:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, subservice organizations, and other parties;
- Internal control and its limitations; and
- The criteria and how controls address those criteria.

Let us be your guide forward

Neal W. Beggan, CISA, CRISC, CRMA, CCSFP
Principal, Risk Assurance & Advisory Services
nbeggan@cbh.com | 703.584.8393

Steven J. Ursillo, Jr., CPA, CISA, CISSP
Partner, Risk Assurance & Advisory Services
sursillo@cbh.com | 401.250.5605

John Richardson, CPA, CISA, CCSFP
Director, Risk Assurance & Advisory Services
jrichardson@cbh.com | 919.782.1040

Nick Stone, CPA, CISA
Director, Risk Assurance & Advisory Services
nstone@cbh.com | 919.782.1040

04.29.19

Cherry Bekaert LLP
CPAs & Advisors

cbh.com/riskadvisory

An independent member of Baker Tilly International