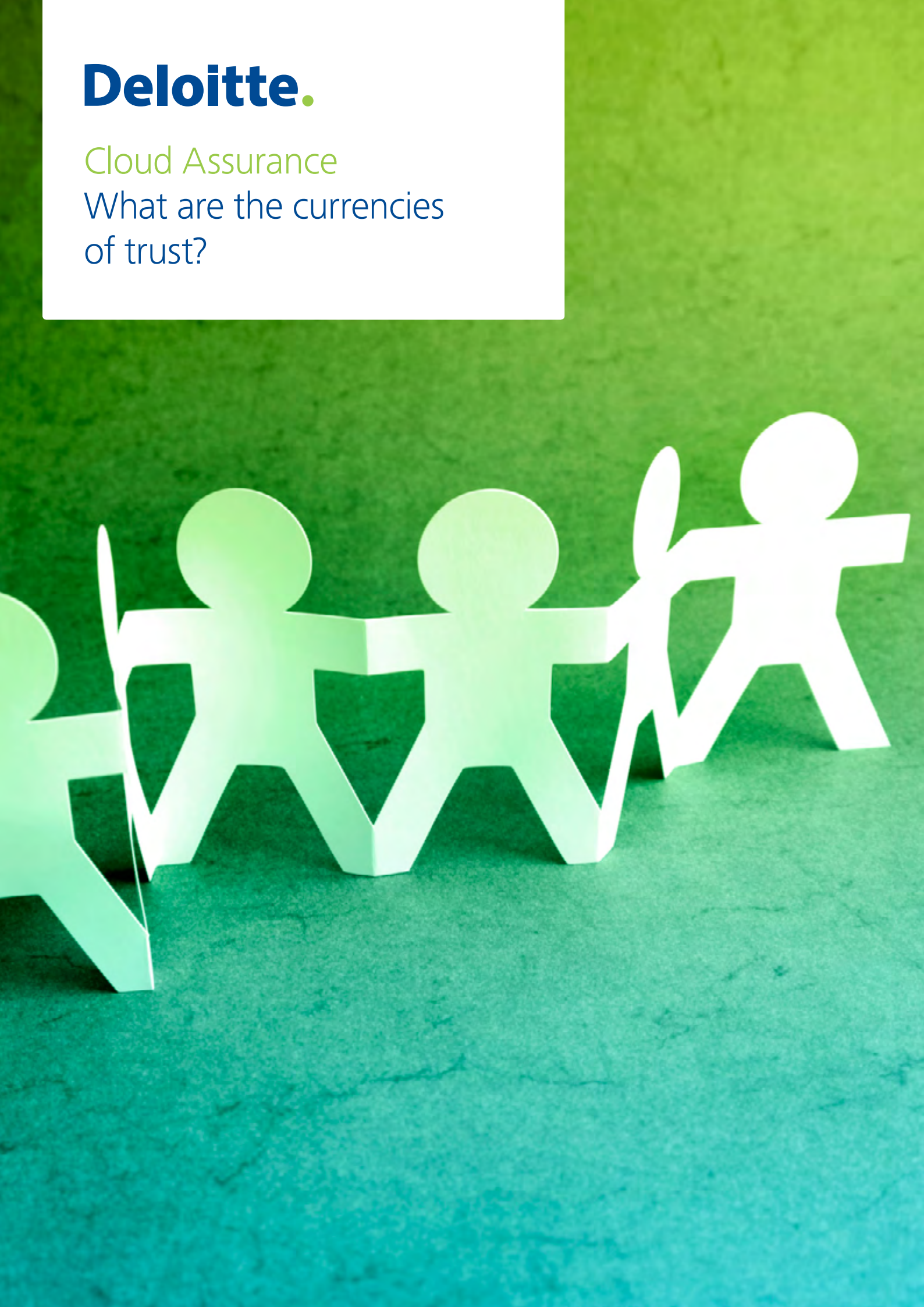
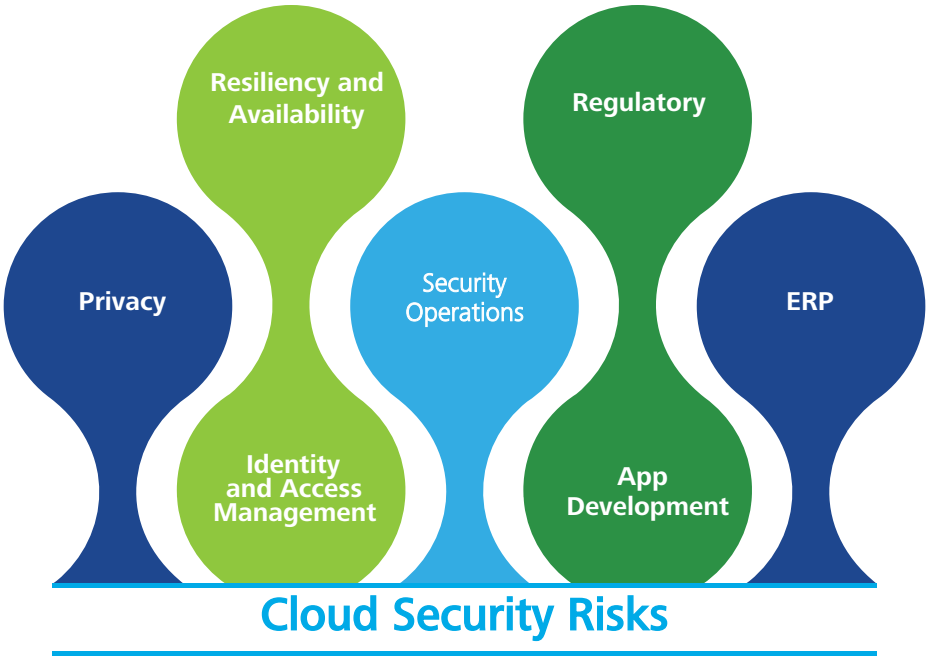
Deloitte.

Cloud Assurance

What are the currencies of trust?



Organizations in today's environment are heavily dependent on Cloud providers. Comfort on security of data is one of the major concerns that is in the mind of the various stakeholders including management, auditors, customers. In this article we have articulated the assurance levels that can be obtained on a Cloud Platform to mitigate some of the cloud related security risks.



Cloud-Relevant Assurance Level

Service Organization Control Reports (SOC2/3)	Service Organization Control Reports (SOC1 — SSAE 16) (f.k.a. SAS70)	International Organization for Standardization	EULA/SLA
Controls at a Service Organization (SOC) relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy — This new reporting structure from the American Institute of Certified Public Accounts (AICPA) which includes the risk areas in a SOC report beyond the traditional financial audit scope mandated by SAS70/SSAE16 to mitigate some of the key risk barriers to adoption of the Cloud.	SSAE 16/SOC1 reports are going to be required by customers who have processes and data with their service providers that are relevant to financial reporting.	The ISO 27001 Info. Sec. Mgmt. systems certification is a way to demonstrate the implementation of good security practices that is validated by a third party. However, some customers may require specific assurance through testing and validation that those good security practices are effective in mitigating the risks.	End-user license agreements and service-level agreements can be very good for meeting operational requirements. Understanding what to expect and what to look for will be key to meeting your requirements.

Which trust currency is most appropriate for my organization?

A new report on internal controls

As a Cloud Service Provider, you may not have the same responsibilities and accountability as the data owners, but you nevertheless take on significant risks associated with managing and protecting the data in the cloud on behalf of your clients.

Cloud Risk Reliance

Provider responsibility examples
- Security Operations
- Resilience
- Availability

Subscriber responsibility examples
- Privacy
- App Development

As a Cloud Subscriber, you can outsource the data assets, but not the responsibility or accountability associated with those assets.

Cloud Assurance

SOC 2 Overview

A new report on internal controls

What is SOC 2?

Service organization controls (SOC) 2 is a new internal controls offering that utilizes **AICPA standards** to allow a service auditor to provide an opinion on the security, availability, processing integrity, confidentiality, and/or privacy of a s**ervice organization's controls**. It also allows the flexibility to incorporate objective rationale, for example, around service-level agreements, National Institute of Standards and Technology Frameworks, and adherence to public industry-specific standards (i.e., HIPAA, Utility Frameworks). SOC 2 became effective in summer 2011.

SOC 2 can be applied for regulatory or nonregulatory purposes to cover business areas outside of financial reporting. The report can be distributed to customers and other stakeholders to demonstrate a focus on system and processing controls to meet their requirements.

The need for assurance in these areas can be addressed through one or more of the five SOC 2 Trust Principles:

- **Security** against unauthorized access or appropriation, either physical or logical
- **Availability** of operations
- **Processing integrity**, including complete, accurate, and timely processing
- **Confidentiality** of information
- **Privacy,** in keeping with AICPA's trust principles and the organization's privacy policy (e.g., personally identifiable information (PII) and confidential data) or other regulations

SOC 2 will be similar in structure and general approach to the traditional legacy SAS 70 report (now SOC 1) with an option for a Type 1 or Type 2 report. A Type 1 only covers the design of controls, while a Type 2 covers design and operating effectiveness.

Illustrative applications of SOC 2		
All Industries	SOC 2 for Service Organizations	The application for SOC 2 is very broad and can be applied to virtually every industry and business sector. SOC 2 will allow service organizations to provide assurance to customers and other stakeholders that effective internal controls are in place.
	Deloitte's Capabilities	Deloitte is recognized as one of the market leaders in legacy SAS 70 reports and internal control services. We have a dedicated practice of risk and control specialists with deep industry focus and experience to reduce ramp-up time.
Cloud Computing	SOC 2 for Cloud Service Providers	Cloud service providers need to provide their customers assurance of effective controls across all the SOC 2 Trust Principles in order for those customers to comfortably entrust the cloud provider with their sensitive data and critical computing needs. SOC 2 reports provide a way to build trust with customers and demonstrate compliance in controls with various industry regulations and standards (e.g., HIPAA/HITECH, GLBA, FISMA).
	Deloitte's Capabilities	Deloitte has considerable cloud computing capabilities with experience serving the largest cloud providers and the most demanding cloud customers. We are leaders in security, privacy, and internal control services. Our strong brand in assurance makes us a first choice provider for SOC 2 services to cloud providers.
Power and Utilities	SOC 2 for Power and Utilities Compliance	Power and Utilities companies can leverage SOC 2 to demonstrate compliance with various regulatory body requirements, industry frameworks, and standards such as NERC Critical Infrastructure Protection (NERC CIP), Smart Grid: NIST IR 7628 — Guidelines for Smart Grid Cyber Security, Advanced Metering Infrastructure (AMI)-SEC System Security Requirements, and state privacy requirements.
	Deloitte's Capabilities	Deloitte is one of the leading Big Four firms in the attest space for the Utilities industry with deep industry experience. We also have significant qualifications around Smart Grid, which positions us as a leader in the marketplace for this service.
FISMA	SOC 2 for Federal Guidelines	Companies that have established contracts or plan to do business with the Federal government can leverage SOC 2 to demonstrate that controls meet the FISMA requirements. This report can provide assurance that agencies have documented information security controls that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.
	Deloitte's Capabilities	Deloitte has significant qualifications and experienced staff within the federal government and commercial sector, as well as proficiency in building FISMA programs and conducting FISMA assessments.

Contacts

N. Ramu
Partner,
Deloitte Touche Tohmatsu India LLP
Phone: +91 99896 10301
Email: ramun@deloitte.com

Abhay Gupte
Partner,
Deloitte Touche Tohmatsu India LLP
Phone: + 91 98211 44933
Email: agupte@deloitte.com

Deloitte Touche Tohmatsu India Private Limited (U74140MH199 5PTC093339), a private company limited by shares, was converted into Deloitte Touche Tohmatsu India LLP, a limited liability partnership (LLP Identification No. AAE-8458),with effect from October 1, 2015.