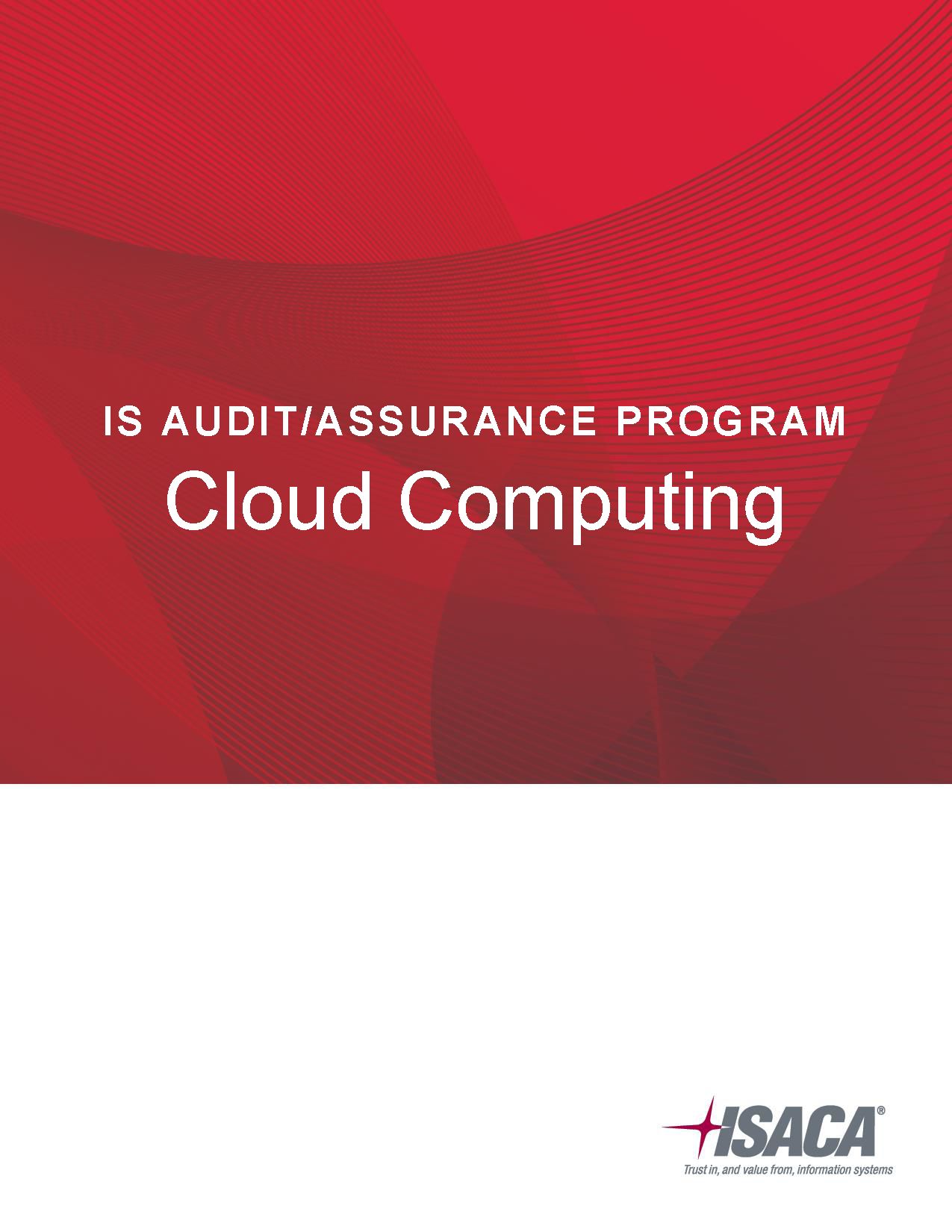
****

**ISACA®**

ISACA (isaca.org) helps global professionals lead, adapt and assure trust in an evolving digital world by offering innovative and world-class knowledge, standards, networking, credentialing and career development. Established in 1969, ISACA is a global nonprofit association of 140,000 professionals in 180 countries. ISACA also offers the Cybersecurity NexusTM (CSX), a holistic cybersecurity resource, and COBIT®, a business framework to govern enterprise technology.

**Disclaimer**

ISACA has designed and created *IS Audit/Assurance Program Cloud Computing* (the “Work”) primarily as an educational resource for audit professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, audit professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

**Reservation of Rights**

©2016 Information Systems Audit and Control Association, Inc. (ISACA). All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorization of ISACA. Reproduction and use of all or portions of this publication are permitted solely for academic, internal and noncommercial use and for consulting/advisory engagements, and must include full attribution of the material’s source. No other right or permission is granted with respect to this work.

**ISACA**

3701 Algonquin Road, Suite 1010

Rolling Meadows, IL 60008 USA

Phone: +1.847.253.1545

Fax: +1.847.253.1443

Email: *info@isaca.org*

Web site: *www.isaca.org*

Provide feedback: *www.isaca.org/audit programs*

Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*

Follow ISACA on Twitter: *https://twitter.com/ISACANews*

Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*

Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

ISBN 978-1-60420-693-7

**Table of Contents**

[IS Audit/Assurance Program for Cloud Computing 4](#_Toc457644144)

[Audit Subject: Cloud Computing Governance and Security 4](#_Toc457644145)

[Audit Objectives 4](#_Toc457644146)

[Audit Scope 4](#_Toc457644147)

[Business Impact and Risk 5](#_Toc457644148)

[Minimum Audit Skills 5](#_Toc457644149)

[Testing Steps 5](#_Toc457644150)

**Note:** The Audit Program Worksheet is provided in a separate file.

# IS Audit/Assurance Program for Cloud Computing

## Audit Subject: Cloud Computing Governance and Security

Cloud computing is viewed as a significant change to the platform in which business services are translated, used and managed. Many consider it to be as large a shift in IT as was the advent of the personal computer (PC) or of Internet access. However, a major difference between the cloud and those technologies is that the introductions of those earlier technologies encompassed a slower development phase. With the cloud, the required pieces have come together more rapidly for implementation.[[1]](#footnote-1)

Depending on business needs, any or all of these benefits could be a sufficient reason to consider a cloud computing solution. The recent world economy has pushed many enterprises to be more fiscally conservative. In the IT space, cloud computing presents a potentially significant savings by enabling enterprises to maximize dynamic computing on a pay-per-use basis. For enterprises to gain benefit from the use of cloud computing, a clear governance strategy and management plan must be developed. The governance strategy should set the direction and objectives for cloud computing within the enterprise, and the management plan should execute the achievement of the objectives.

## Audit Objectives

* Provide management with an assessment of cloud computing policies and procedures and their operating effectiveness.
* Identify internal control and regulatory deficiencies that could affect the organization.
* Identify cloud computing vendor management control concerns that could affect the reliability, accuracy and security of the enterprise data due to weaknesses in mobile computing controls.

## Audit Scope

* The governance affecting cloud computing
* The contractual compliance between the service provider and customer

Because the areas under review rely heavily on the effectiveness of core IT general controls, it is recommended that audit/assurance reviews of the following areas be performed prior to the execution of the cloud computing review, so that appropriate reliance can be placed on these assessments:

* Identity management (if the enterprise’s identity management system is integrated with the cloud computing system)
* Security incident management (to interface with and manage cloud computing incidents)
* Network perimeter security (as an access point to the Internet)
* Systems development (in which the cloud is part of the application infrastructure)
* Project management
* IT risk management
* Data management (for data transmitted and stored on cloud systems)
* Vulnerability management

#### Out of Scope

This cloud computing assurance review is not designed to provide assurance on the design and operational effectiveness of the cloud computing service provider’s internal controls.

## Business Impact and Risk

Using cloud services brings multiple benefits to cloud users, but it also raises many concerns, which, if not handled well, can quickly turn the cloud experience into an information security management nightmare derived from the loss of controls over physical and logical assets. The business impact and risk associated with the use of cloud computing services, compared to traditional outsourcing, include the following areas/processes:

* Greater dependency on third parties:
* Increased vulnerabilities in external interfaces
* Increased risk in aggregated data centers
* Immaturity of the service providers with the potential for service provider ongoing concern issues
* Increased reliance on independent assurance processes
* Increased complexity of compliance with laws and regulations:
* Greater magnitude of privacy risk
* Transborder flow of personally identifiable information (PII)
* Affecting contractual compliance
* Reliance on the Internet as the primary conduit to the enterprise’s data introduces:
* Security issues with a public environment
* Availability issues of Internet connectivity
* Due to the dynamic nature of cloud computing:
* The location of the processing facility may change according to load balancing
* The processing facility may be located across international boundaries
* Operating facilities may be shared with competitors
* Legal issues (liability, ownership, etc.) relating to differing laws in hosting countries may put data at risk

## Minimum Audit Skills

Cloud computing incorporates many IT processes. Because the focus is on information governance, IT management, network, data, contingency and encryption controls, the audit and assurance professional should have the requisite knowledge of these issues. In addition, proficiency in risk assessment, information security components of IT architecture, risk management, and the threats and vulnerabilities of cloud computing and Internet-based data processing is required. Therefore, it is recommended that the audit and assurance professional who is conducting the assessment has the requisite experience and organizational relationships to effectively execute the assurance processes. Because cloud computing is dependent on web services, the auditor should have at least a basic understanding of Organization for the Advancement of Structured Information Standards (OASIS) Web Services Security (WS-Security or WSS) Standards ([*www.oasis-open.org*](http://www.oasis-open.org)).

It is also important that the auditor has sufficient functional and business knowledge to assess alignment with the business strategy. Professionals holding the CISA certification should comply with ITAF standard 1006 Proficiency.

## Testing Steps

Refer to the accompanying spreadsheet file.

1. ISACA, *Controls and Assurance in the Cloud: Using COBIT® 5,* USA, 2014 [↑](#footnote-ref-1)