

## Certified Information System Auditor

---

What is a Certified Information System Auditor (CISA) and what are Information System Audits? The best way to address these questions is to draw a parallel with the roles of CPAs and financial audits.

In a financial audit, the entity being audited provides its financial information and makes certain assertions about the validity of the information. The auditor then performs tests to conclude whether the assertions made are reasonably correct.

Given the varying complexity of information systems and the reliance placed on the systems, it should come as no surprise that there are certain assertions made by an entity, or division, about the information systems utilized. The assertions may be about the logical or physical security of the system, the availability of the system, the processes involved in the system backups, or disaster recovery plans, to name a few areas.

Some practical examples of where the services of a CISA may be of value are:

1. Review or audit of the system backup policies and practices to verify that the practices are reasonable and should provide the required information at the critical time when backups are needed.
2. Audit the information systems internal controls for proper segregation of duties related to the management of the information system and the information contained in the system.
3. Assist with development of an implementation plan or review compliance with regulatory requirements such as the FTC Red Flag rules or the HIPAA Security Rule.
4. Providing advice in the selection of a co-location site or service provider or auditing the compliance of the entities to contractual specifications.
5. Conducting a brief overview of the existing information system's status and the steps needed to better align the system with best practices.

Certification as an Information Systems Auditor demonstrates a level of competence and capability needed to effectively review and provide an opinion or consult on matters specific to information systems. CISA's have, in a manner similar to Certified Public Accountants, test, time and ethical requirements. To receive certification a candidate must pass an exam demonstrating competency in: IS Audit, IT Governance, Systems and Infrastructure Life Cycle Management, IT Service Delivery and Support, Protection of Information Assets, and Business Continuity and Disaster Recovery. The Candidate must have five years of applicable work experience. Continuing Education requirements consist of 120 CPE hours every three years with no fewer than 20 in any given year. The candidate must also, similar to a CPA, adhere to a particular ethical code of conduct.

One point of difference is a CPA license is granted by a state or similar governmental entity. CISA is not a license, but a certification awarded by ISACA (Information Systems Audit and Control Association). ISACA was started in 1967 and is globally

recognized as an authority on information systems audits and a resource for consultation on information systems and related controls.

For more information on CISA, ISACA and other information systems topics and regulations visit the following sites using the following links:

ISACA & CISA :

<http://isaca.org/>

IS audits overview and general information:

[http://en.wikipedia.org/wiki/Information\\_technology\\_audit](http://en.wikipedia.org/wiki/Information_technology_audit)

SAS 70 reports overview:

[http://en.wikipedia.org/wiki/Statement\\_on\\_Auditing\\_Standards\\_No.\\_70:\\_Service  
\\_Organizations](http://en.wikipedia.org/wiki/Statement_on_Auditing_Standards_No._70:_Service_Organizations)

FTC Red Flag Rules:

<http://ftc.gov/redflagsrule>

HIPAA Security Rule:

<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/index.html>

National Institute of Standards and Technology:

<http://www.nist.gov/>