Standards define mandatory requirements for IT audit and assurance.

They inform:
- IT audit and assurance professionals of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics
- Management and other interested parties of the profession’s expectations concerning the work of practitioners
- Holders of the Certified Information Systems Auditor™ (CISA®) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder’s conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

Guidelines provide guidance in applying IT Audit and Assurance Standards. The IT audit and assurance professional should consider them in determining how to achieve implementation of the standards, use professional judgement in their application and be prepared to justify any departure. The objective of the IT Audit and Assurance Guidelines is to provide further information on how to comply with the IT Audit and Assurance Standards.

Tools and Techniques provide examples of procedures an IT audit and assurance professional might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IT auditing work, but do not set requirements. The objective of the IT Audit and Assurance Tools and Techniques is to provide further information on how to comply with the IT Audit and Assurance Standards.

COBIT® is an IT governance framework and supporting tool set that allows managers to bridge the gaps amongst control requirements, technical issues and business risks. COBIT enables clear policy development and good practice for IT control throughout enterprises. It emphasises regulatory compliance, helps enterprises increase the value attained from IT, enables alignment and simplifies implementation of the COBIT framework’s concepts. COBIT is intended for use by business and IT management as well as IT audit and assurance professionals; therefore, its usage enables the understanding of business objectives and communication of good practices and recommendations to be made around a commonly understood and well-respected framework. COBIT is available for download on the ISACA web site, www.isaca.org/cobit.

Links to current guidance are posted on the standards page, www.isaca.org/standards.

The titles of issued standards documents are:

**IT Audit and Assurance Standards**
- S1 Audit Charter Effective 1 January 2005
- S2 Independence Effective 1 January 2005
- S3 Professional Ethics and Standards Effective 1 January 2005
- S4 Professional Competence Effective 1 January 2005
- S5 Planning Effective 1 January 2005
- S6 Performance of Audit Work Effective 1 January 2005
- S7 Reporting Effective 1 January 2005
- S8 Follow-up Activities Effective 1 January 2005
- S9 Irregularities and Illegal Acts Effective 1 September 2005
- S10 IT Governance Effective 1 September 2005
- S11 Use of Risk Assessment in Audit Planning Effective 1 November 2005
- S12 Audit Materiality Effective 1 July 2006
- S13 Using the Work of Other Experts Effective 1 July 2006
- S14 Audit Evidence Effective 1 July 2006
- S15 IT Controls Effective 1 February 2008
- S16 E-commerce Effective 1 February 2008

**IT Audit and Assurance Guidelines**
- G1 Using the Work of Other Experts Effective 1 March 2008
- G2 Audit Evidence Requirement Effective 1 May 2008
- G3 Use of Computer-assisted Audit Techniques (CAATs) Effective 1 March 2008
- G4 Outsourcing of IS Activities to Other Organisations Effective 1 May 2008
- G5 Audit Charter Effective 1 February 2008
- G6 Materiality Concepts for Auditing Information Systems Effective 1 May 2008
- G7 Due Professional Care Effective 1 March 2008
- G8 Audit Documentation Effective 1 March 2008
- G9 Audit Considerations for Irregularities Effective 1 September 2008
- G10 Audit Sampling Effective 1 August 2008
- G11 Effect of Pervasive IS Controls Effective 1 August 2008
- G12 Organisational Relationship and Independence Effective 1 August 2008
- G13 Use of Risk Assessment in Audit Planning Effective 1 August 2008
- G14 Application Systems Reviews Effective 1 October 2008
- G15 Audit Planning Revised Effective 1 Mar 2010
- G16 Effect of Third Parties on an Organisation’s IT Controls Effective 1 March 2009
- G17 Effect of Non-audit Role on the IS Auditor’s Independence Effective 1 May 2010
- G18 IT Governance Effective 1 May 2010
- G19 Withdrawn 1 September 2008
- G20 Reporting Effective 16 September 2010
- G21 Enterprise Resource Planning (ERP) Systems Reviews Effective 16 September 2010
- G22 Business-to-consumer (B2C) E-commerce Reviews Effective 1 October 2008
- G23 System Development Life Cycle (SDLC) Reviews Effective 1 August 2003
- G24 Internet Banking Effective 1 August 2003
- G25 Review of Virtual Private Networks Effective 1 July 2004
- G26 Business Process Re-engineering (BPR) Project Reviews Effective 1 July 2004
- G27 Mobile Computing Effective 1 September 2004
- G28 Computer Forensics Effective 1 September 2004
- G29 Post-implementation Review Effective 1 January 2005
- G30 Competence Effective 1 June 2005
- G31 Privacy Effective 1 June 2005
- G32 Business Continuity Plan (BCP) Review From IT Perspective Effective 1 September 2005
- G33 General Considerations for the Use of the Internet Effective 1 March 2006
- G34 Responsibility, Authority and Accountability Effective 1 March 2006
- G35 Follow-up Activities Effective 1 March 2006
- G36 Biometric Controls Effective 1 February 2007
- G37 Configuration and Release Management Effective 1 November 2007
- G38 Access Controls Effective 1 February 2008
- G39 IT Organisation Effective 1 May 2008
- G40 Security Architecture—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
- G41 Information Security Risk Assessment Effective 1 January 2005
- P1 IS Risk Assessment Measurement Effective 1 July 2002
- P2 Digital Signatures and Key Management Effective 1 July 2002
- P3 Intrusion Detection Systems (IDS) Review Effective 1 August 2003
- P4 Malicious Logic Effective 1 August 2003
- P5 Control Risk Self-assessment Effective 1 August 2005
- P6 Firewall Reviews Effective 1 August 2003
- P7 Irregularities and Illegal Acts Effective 1 December 2003
- P8 Security Architecture—Penetration Testing and Vulnerability Analysis Effective 1 September 2004
- P9 Evaluation of Management Controls Over Encryption Methodologies Effective 1 January 2005
- P10 Business Application Change Control Effective 1 October 2005
- P11 Electronic Funds Transfer (EFT) Effective 1 May 2007

**Standards for Information System Control Professionals**
- Effective 1 September 1999
  - 310 Statement of Scope
  - 010 Responsibility, Authority and Accountability
  - 520 Independence
  - 010 Professional Independence
  - 020 Organisational Relationship
  - 530 Professional Ethics and Standards
  - 010 Code of Professional Ethics
  - 020 Due Professional Care
  - 540 Competence
  - 010 Skills and Knowledge
  - 020 Continuing Professional Education
  - 550 Planning
  - 010 Control Planning
  - 560 Performance of Work
  - 010 Supervision
  - 020 Evidence
  - 030 Effectiveness
  - 570 Reporting
  - 010 Periodic Reporting
  - 580 Follow-up Activities
  - 010 Follow-up
  - Code of Professional Ethics Effective 1 January 2011