ISO/IEC TR 3445:2022-03 (E)

Information technology - Cloud computing - Audit of cloud services

Contents

Page

Foreword ... **v**

Introduction ... **vi**

1 Scope ... **1**

2 Normative references ... **1**

3 Terms and definitions ... **1**
3.1 Terms related to the use of audit and assessment ... 1
3.2 Terms related to cloud service audit ... 3

4 Abbreviated terms ... **5**

5 Overview of cloud computing and the activities of a cloud auditor ... **5**
5.1 Overview of cloud computing ... 5
5.1.1 General ... 5
5.1.2 Cloud computing roles, sub-roles and activities ... 6
5.2 Overview of the activities of a cloud auditor ... 7
5.2.1 Cloud auditor ... 7
5.2.2 Responsibilities of a cloud auditor ... 8
5.2.3 Cloud auditor's cloud computing activities ... 9
5.2.4 Relationship of the cloud auditor to CSPs, CSCs, and other CSNs ... 10

6 Overview of the audit of cloud services ... **10**
6.1 General ... 10
6.2 Objectives of an audit of cloud service ... 11
6.2.1 General ... 11
6.2.2 Audit objectives ... 11
6.2.3 Audit boundaries ... 13
6.2.4 Relationship of an audit and the organization ... 13
6.3 Types of cloud audit ... 15
6.3.1 Overview ... 15
6.3.2 Internal audit ... 15
6.3.3 External audit ... 16
6.3.4 Exemplary tests and audits ... 17
6.3.5 Relationship between audit and assessment for cloud computing ... 19
6.3.6 Relationships among audit processes and reports ... 19
6.3.7 Conformity Assessment – Objectives and expectations ... 24
6.4 Cloud audit and trust ... 24

7 Audit specifications and challenges ... **25**
7.1 Overview ... 25
7.2 Establishing audit scope ... 25
7.3 Audit risk assessment ... 25
7.3.1 General ... 25
7.3.2 Risk assessment of cloud computing systems and legacy or non-cloud computing system ... 26
7.4 Security controls assessment ... 26
7.5 Required laws, regulations, and government requirements ... 27
7.6 Policies ... 28
7.6.1 General ... 28
7.6.2 Geolocation data ... 28
7.7 Cloud service agreement (CSA) ... 28
7.8 Cloud capabilities types, cloud service categories and key characteristics ... 29

7.9 Cross-cutting aspects 31
7.10 Emerging technologies and cloud native 31
7.11 Define metrics and security parameters 32
7.12 Determining matrix 33
7.13 Assessment of cloud governance 33
7.14 Challenges of conducting an audit of cloud services 33
7.14.1 General 33
7.14.2 Third party auditability 33
7.14.3 Change management 33
7.14.4 Patch management 34
7.14.5 Multi-tenant environment 34
7.14.6 Auditability and assurance 34
7.14.7 Availability requirement 34

8 Approaches to conducting audits 35
8.1 Typical Scenarios 35
8.2 Cloud audit – opportunities and meeting objectives 35
8.2.1 General 35
8.2.2 Stakeholders and related activities on cloud audit 36
8.3 Processes – identify, analyse, evaluate 36
8.4 Data flow – lifecycle - confidentiality, integrity, availability 37
8.5 Automation of cloud service audits and assessments 37

Annex A (informative) **Sample list of standards and frameworks applicable to audit of cloud services 39**

Annex B (informative) **Compilation of frameworks, schemes, and auditing programs for certification, attestation and authorization which are relevant to cloud security 44**

Bibliography 49