Chapter 1
Audits in Cybersecurity

Regner Sabillon
Universitat Oberta de Catalunya, Spain

ABSTRACT

The objective of this chapter is to provision a comprehensive literature review of the most relevant approaches for conducting cybersecurity audits. The study includes auditing perspectives for specific scopes and the best practices that many leading organizations are providing for security and auditing professionals to follow. The chapter reviews relevant features for auditing approaches in the following order: ISO/IEC 27001:2013, ISO/IEC 27002:2013, Control Objectives for Information and Related Technology (COBIT) 2019, Information Technology Infrastructure Library (ITIL) 4, AICPA, ISACA, NIST SP 800-53, NIST CSF v1.1, IIA, PCI DSS, ITAF, COSO, ENISA, NERC CIP, and CSAM.

INTRODUCTION

This study reviews the most important standards, frameworks, methodologies, guidelines, best practices and models that are used worldwide for planning, execution, reporting and follow-up audit phases in the areas of information security (InfoSec), cybersecurity and information technology.

The chapter reviews relevant features for auditing approaches in the following order: ISO/IEC 27001:2013; ISO/IEC 27002:2013; Control Objectives for Information and Related Technology (COBIT) 2019; Information Technology Infrastructure Library (ITIL) 4, AICPA; ISACA; NIST SP 800-53; NIST CSF v1.1; IIA; PCI DSS; ITAF; COSO; ENISA; NERC CIP and CSAM. Some methodologies have a specific purpose and others provide the audit approaches for certain institutions that have global impact.

ISO/IEC 27001: 2013

This international standard was designed and is maintained by the International Organization for Standardization (ISO). ISO standards are reviewed every five years, previous edition was published in 2005 and the second edition was released in 2013. The ISO/IEC 27001:2013 known as *Information technology - Security techniques – Information security management systems - Requirements*. It is based on the Information Security Management System (ISMS). ISO/IEC 27001:2013 can be used by organizations

DOI: 10.4018/978-1-6684-3698-1.ch001

to establish, implement, maintain and continually improve the ISMS. ISO/IEC 27001:2013 consists of 7 clauses (Table 1), control objectives and controls are aligned with ISO/IEC 27002:2013, which contains 14 control clauses, 35 security categories and 114 controls. Terminology is based on ISO/IEC 27000: *Information technology - Security techniques – Information security management systems – Overview and vocabulary.*

Clauses 9 and 10 provide guidelines for:

1. Monitoring, measurement, analysis and evaluation
2. Internal audit
3. Management review
4. Nonconformity and corrective action
5. And Continual Improvement of the ISMS

Table 1. ISO/IEC 27001:2013 Information Security Management Systems Clauses

ISO/IEC 27001: Security Control Clauses
1. Clause 4: Context of the organization 2. Clause 5: Leadership 3. Clause 6: Planning 4. Clause 7: Support 5. Clause 8: Operation 6. Clause 9: Performance Evaluation 7. Clause 10: Improvement

ISO/IEC 27002: 2013

This international standard was designed and is maintained by the International Organization for Standardization (ISO). ISO standards are reviewed every five years, previous edition was published in 2005 and the second edition was released in 2013. The ISO/IEC 27002:2013 known as *Information technology - Security techniques – Code of practice for information security controls*. It is based on the Information Security Management System (ISMS) from the ISO/IEC 27001. ISO/IEC 27002:2013 can be used by organizations to select controls with any ISMS implementation, implement universally accepted information security controls and to develop information security management guidelines for their specific business environments.

ISO/IEC 27002:2013 contains 14 control clauses (Table 2), 35 security categories (Table 3) and 114 controls.

In terms of audits, *ISO/IEC 27002:2013* highlights two specific controls for planning and conducting audits:

12.7.1 Information system audit controls: Requirements and activities are to be planned without causing impact to business processes. A guidance implementation is provided that includes 7 guidelines.