Anton Mishchenko

OVERVIEW OF CYBER SECURITY AUDITING STANDARDS

May 26, 2024

Contents

[Tables 1](#_Toc167631695)

[Figures 1](#_Toc167631696)

[Backround 2](#_Toc167631697)

[ITU-T Recommendation X.816 2](#_Toc167631698)

[ISO 27006 2](#_Toc167631699)

[ISO 27007 2](#_Toc167631700)

[NIST SP 800-53 3](#_Toc167631701)

[NIST SP 800-92 3](#_Toc167631702)

[References 5](#_Toc167631703)

# Tables

[Table 1 Number of ISO 9001 certificates issued per year. 4](#_Toc167631666)

# Figures

[Figure 1 ISO 9001 main clauses & PDCA cycle. 4](#_Toc167631669)

# Backround

Auditing standards and recommendations such as ITU-T Recommendation X.816 provide organizations with a structured guide to achieve the desired level of assurance in network and computer system security. These standards cover an extensive range of aspects of auditing, such as how auditing should be structured, log management practices, quality of reporting, auditing controls, and audit management. Standards range in detail and scope, some focusing more on specific aspects such as alarm frameworks and OS audit sources. In contrast, others provide general guidelines applicable to a wide range of organizations. The following are summaries of different auditing standards and recommendations.[[1]](#endnote-1)

## ITU-T Recommendation X.816

This standard provides recommendations and guidelines for open system security auditing and alarm handling. It outlines the basic vocabulary and scope for which these recommendations are meant. Following that, different alarm model architecture is defined and discussed. Lastly, it covers topics of audit policies and what considerations must be considered when developing policies. This includes requirements for performing different audit types and levels and legal implications. Overall, it discusses topics of audit goals, phases that need to be completed during an audit and responsibilities of the personnel involved.  [(Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T), 1995)](#_References)

## ISO 27006

This standard focuses on building criteria and guidelines for organizations conducting an audit of ISMS systems. When organizations want to be certified with ISO 27001 standard, certifier organizations are required to follow ISO 27006 standard to conduct an audit correctly. Guidelines outlined in ISO 27006 standard cover different requirements. General requirements cover liability and conflicts of interest. Structural and resource requirements cover topics of organizing and safeguarding committees, training, education, and expertise. Additionally, information collection requirements and guidelines on how to conduct the audit processes are discussed.  [(International Organization for Standardization, 2015)](#_References)

## ISO 27007

Another standard from the International Organization for Standardization, ISO 27007, includes guidelines and recommendations on the topics of audit programme management, auditor skillsets and compliance. These guidelines are discussed in the context of ISMS systems and are meant for organizations conducting an external and internal audits. Management of audits includes recommendations for the establishment, implementation of the programme, and monitoring. Previous steps are followed by a review and improvement of the audit programme. Audit conduction includes guidelines on preparation for an audit, conduction of audit activities and distribution of the report followed by a follow-up. Additionally, guidelines on auditor evaluation and compliance are included.  [(International Organization for Standardization, 2020)](#_References)

## NIST SP 800-53

This publication from NIST covers a large range of security controls, including relevant topics for their successful implementation. It contains a section for the audit and accountability (AU) family of controls that focuses on auditing practices and accountability maintenance. Firstly, an audit policy's construction and guidelines are outlined to help organizations establish security goals. Following that, different aspects of logging are covered, such as contents, storage, and failures. Additionally, audit record topics are discussed that include generation, review, report, retention, non-repudiation and more. Lastly, more specific issues are discussed, such as alternative logging capabilities and cross-organizational logging.  [(National Institute of Standards and Technology, 2020)](#_References)

## NIST SP 800-92

This NIST publication focuses on recommendations for security log management. It addresses the need for log management and fundamental issues, such as the balance between limited log processing resources in the face of the continuous generation of logs. Guidance is given in a practical form that is applicable to the real world. Organizations are recommended to use this guide to create and maintain an appropriately managed logging system throughout their organization. Additionally, sections of this publication cover aspects of system-level and organization-level management, policies related to log management, infrastructure components and their architecture.  [(Kent, 2006)](#_References)

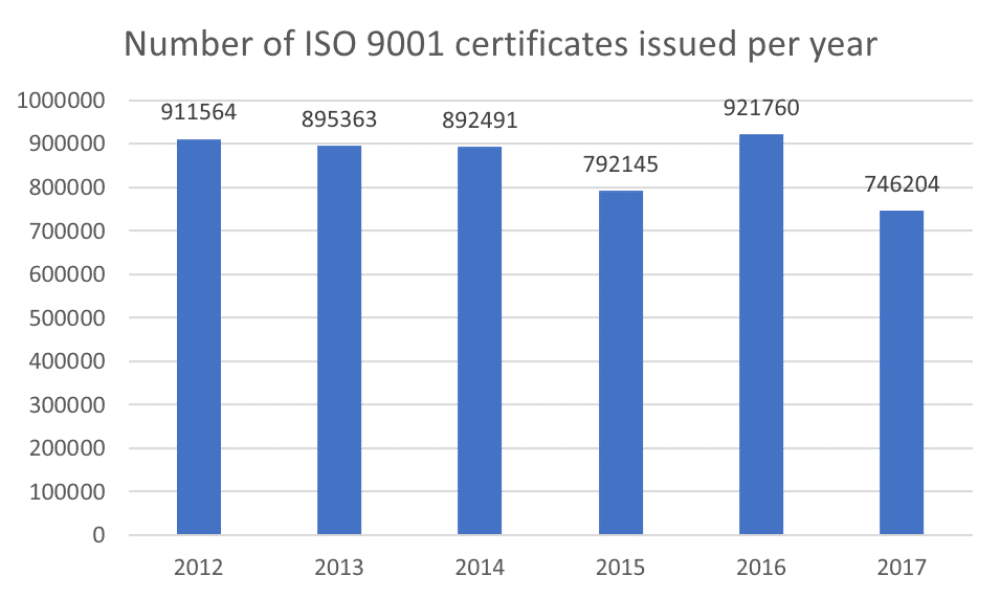


Table 1 Number of ISO 9001 certificates issued per year.[[2]](#footnote-1)

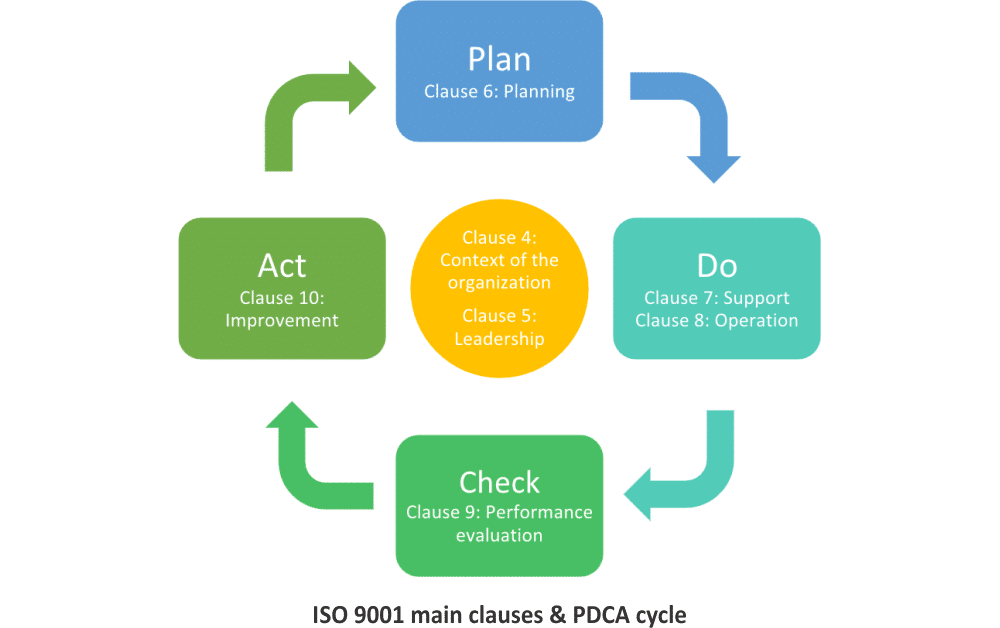


Figure 1 ISO 9001 main clauses & PDCA cycle.[[3]](#footnote-2)

# References

Hammar, M. (2024, March 4). *What is the ISO 9001 standard? A straightforward overview*. Retrieved from 9001Academy: https://advisera.com/9001academy/what-is-iso-9001/

International Organization for Standardization. (2015). Information technology — Security techniques — Requirements for bodies providing audit and certification of information security management systems. *(ISO/IEC 27006, 3rd ed.)*.

International Organization for Standardization. (2020). Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing. *(ISO/IEC 27007, 3rd ed.)*.

Kent, K. &. (2006). Guide to computer security log management. *(NIST Special Publication 800-92)*.

National Institute of Standards and Technology. (2020). Security and privacy controls for information systems and organizations. *(NIST Special Publication 800-53 Revision 5)*.

Telecommunication Standardization Sector of the International Telecommunications Union (ITU-T). (1995). Security audit and alarms framework. *X.816*.

1. This was created for XCMP-1560 UDA03 [↑](#endnote-ref-1)
2. [(Hammar, 2024)](#_References) [↑](#footnote-ref-1)
3. [(Hammar, 2024)](#_References) [↑](#footnote-ref-2)