ISO/IEC 27014:2020 (E)

Information security, cybersecurity and privacy protection — Governance of information security

Contents

Foreword

Introduction

1 Scope

2 Normative references

3 Terms and definitions

4 Abbreviated terms

5 Use and structure of this document

6 Governance and management standards

- 6.1 Overview
- 6.2 Governance activities within the scope of an ISMS
- 6.3 Other related standards
- 6.4 Thread of governance within the organization

7 Entity governance and information security governance

- 7.1 Overview
- 7.2 Objectives
- 7.2.1 Objective 1: Establish integrated comprehensive entity-wide information security
- 7.2.2 Objective 2: Make decisions using a risk-based approach
- 7.2.3 Objective 3: Set the direction of acquisition
- 7.2.4 Objective 4: Ensure conformance with internal and external requirements
- 7.2.5 Objective 5: Foster a security-positive culture
- 7.2.6 Objective 6: Ensure the security performance meets current and future requirements of the entity
- 7.3 Processes
- 7.3.1 General
- 7.3.2 Evaluate
- 7.3.3 Direct
- 7.3.4 Monitor
- 7.3.5 Communicate

8 The governing body's requirements on the ISMS

- 8.1 Organization and ISMS
- 8.2 Scenarios (see Annex B)

Annex A (informative) Governance relationship

Annex B (informative) Types of ISMS organization

Annex C (informative) Examples of communication

Page count: 16