SmartONE STANDARD 5002

Initial Coin Offering – Code of practice for ICO controls

Contents

Foreword

SmartOne aims to bring the disruptive capabilities of blockchain-based enterprise to the legal sector by creating a means of access to legal services for the crypto community.

SmartOne's services include a marketplace for legal advice, automated document preparation and individual legal consulting. Our focus is on providing legal solutions for
....
....

Introduction

0.1   Background and context

....
....

0.2   ICO control requirements

....
....

0.3   Selecting controls

....
....

0.4   Developing your own guidelines

....
....

0.5   Related standards

....
....

Code of practice for ISO controls

1 Scope

....
....
....
....

2 Normative references

....
....

3 Terms and definitions

....
....

4 Structure of this standard

....
....

4.1 Clauses

Each clause defining ICO controls contains one or more main categories.

4.2 Control categories

a) ....
....
....

b) ....
....

Control descriptions are structured as follows:

Control

Defines the specific control statement, to satisfy the control objective

Implementation guidance

Provide more detailed information to support the implementation of the control and meeting the control objective. The guidance may not be entirely suitable or sufficient in all situations and may not fulfil the organisations specific control requirements

Other information

Provides further information that may need to be considered, for example, legal considerations and references to other standards.

5   Policies

....
....
....
....

6   Organisation

....
....

....
....

X   Cryptography

x.1   Cryptographic controls

Objective: to ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information

10.1.1   Policy on the use of cryptographic controls

Control

A policy on the use of cryptographic controls for the protection of information should be developed and implemented

Implementation guidance

When developing a cryptographic policy the following should be considered:

a)   ....
     ....
     ....

b)   ....
     ....
     ....

....
....
....
....

Other information

....
....
....
....
....
....