Review – ISO/IEC 24760-3:2016

Information technology — Security techniques — A framework for identity management — Part 3: Practice

"IT Security and Privacy - A framework for identity management - Part 3: Practice," *International Organization for Standards*, Technical Committee ISO/IEC JTC 1, Subcommittee SC 27, August 2016, https://www.iso.org/standard/57915.html.

Reviewer: Espen Bago

Abstract

The document reviewed here is the third and final part of the ISO/IEC 24760 standard, focusing on "Practice", which in the abstract is described as providing *"guidance for the management of identity information and for ensuring that an identity management system conforms to ISO/IEC 24760-1 and ISO/IEC 24760-2".* Parts 1 and 2 covers "*Terminology and concepts"* and "*Reference architecture and requirements".* ISO/IEC 24760-3 is in its first edition, dated 2016-08.

Review

An important note here is that this review is written looking exclusively at Part 3 without having detailed knowledge of the prior parts. Based on the references within Part 3 to the other parts, this document is not intended to be used in isolation, but since each part is licensed and sold separately, reviewing it in isolation from the other parts may give an indication of its individual worth.

ISO/IEC 24760-3 states its own purpose as to *specify relevant concepts, operational structures and practices that may enable the required assurance and control for use of both identity information and identity management systems*. The implication is that this document provides good practices for identity management, with the main target audience being those who are starting an identity initiative or need to better control an ongoing initiative of this sort.

This intention of providing practices for achieving central and typical goals within identity is laudable, and it is something often searched for by practitioners. But this document fails to deliver on the promises due to several factors, the most important ones being inconsistency of structure and inconsistency of content in each section.

The core of the ISO/IEC 24760-3 are the 12 pages about risk mitigation for identity, identifiers and identity information, auditing and about control objectives and controls, with this last section on controls and objectives taking up the main part. These sections list advice (practices) for different parts of the work necessary when setting up and maintaining identity management systems, and when extracting that information, there is plenty of useful information that could read as a checklist of advice and suggestions.

The challenge is that getting to that useful information and extracting it, is hard due to the convoluted setup in subsections that are difficult to follow, especially since the subsections do not consistently contain the same level or detail of information. Thus it is unnecessarily challenging to understand the given practices either as a whole or to find the relevant, sought after practice for a given situation. Additionally, when found, such information tends to be very simplistic or high level. As an example, the section auditing an identity management system mainly states that audits should be done, and that their purpose should be to validate that the system functions in accordance to its requirements and policies.

A future revision of this standard would benefit from simplifying its section structure, with emphasis on making it clearer what it is trying to express. Possibly, since most of the information is very high level in nature, a format closer to a checklist might also be beneficial.

As it stands now, this standard is most accessible to the most experienced practitioners, since they are better equipped to navigate the document. But these practitioners are also those least in need of the information, since they normally already know most of the practices from experience. Most practitioners new to the area would struggle putting the current (2016-08) version ISO/IEC 24760-3 to use for the stated purpose.

There are no figures in the main body of the document, which seems reasonable as the practices described do not lend themselves to be easily visualized.

Apart from the aforementioned core of the document, half of the ISO/IEC 24760-3 are taken up by two annexes. The reason these are not so far reviewed as being core, is that nothing in the text refers to them, and they are not directly related to anything in the preceding text. Put simply, these annexes of 16 pages out of the total 38 appear out of place, giving the impression that they were included to reach a certain page length.

That being said, the two articles in the annexes are well written and cover interesting areas. Had they been directly relevant to the stated purpose of the standard, the annexes would be enough to warrant a recommendation of the whole document.

For reference, the annexes, including descriptive figures and diagrams, cover practices for federating identity (or potentially rather access) management systems - annex A - and a breakdown of what attribute-based credentials are and how they can be used for authentication. Anyone needing either specific information on setting up federated systems, or working with attribute-based credentials, would probably find this document worth perusing.