ISO IEC 27002
OLD versus NEW

ISO 27002 is a comprehensive information security standard

Perhaps the biggest difference between the old and the new standard is the structure. ISO 27002 2005 had 11 core sections (5 to 14) while ISO 27002 2013 now has 14 (5 to 18). These new sections discuss cryptography, communications security, and supplier relationships (sections 10, 13, and 15 respectively). However, while the new standard has three more sections, it is in fact shorter and more focused than the old. The old standard had 106 pages of content while the new one has only 78.

ISO 27002 2013 also has several new subsections. These new subsections discuss project management security (6.1.5), asset handling (8.2.3), software installation (12.6.2), secure development (14.2.1), secure system engineering principles (14.2.5), secure development environments (14.2.6), system security testing (14.2.8), supplier security (15.1.1, 15.1.2, and 15.1.3), the assessment of security events (16.1.4), planning, implementing, and verifying information security continuity (17.1.1, 17.1.2, and 17.1.3), and the use of redundant information processing facilities (17.2.1).

In addition, most sections have been rewritten, at least to some extent, and some sections have been split up or moved to other sections. For example, the old section 14 on business continuity has been entirely reworked. In addition, the old sections on how to organize security (6), on communications and operations (10), and access control (11) were all entirely reworked, split up, and moved to other more suitable sections. And the old introductory section 4 on risk management was entirely removed, presumably because ISO 27005 and ISO 31000 now discuss this in detail and so ISO 27002 does not need to cover the same ground.

There have also been some changes in terminology. *Privileges* have become *privileged access rights*, the word *passwords* has largely been replaced by the more cumbersome phrase *secret authentication information*, *third party users* are now known as *external party users*, the verb *check* has been replaced by *verify*, *malicious code* is now *malware*, *audit logs* are now *event logs*, *online transactions* are now referred to as *application service transactions*, and our favorite: *electronic commerce* is now *application services passing over public networks*. Evidently this is progress.

Praxiom Research Group Limited
First Edmonton Place 14 Floor 10665 Jasper Ave
Edmonton, Alberta, Canada, T5J 3S9 780-461-4514
info@praxiom.com info@praxiom.org praxiom@gmail.com
We ship worldwide. Our products are used in over 100 countries.