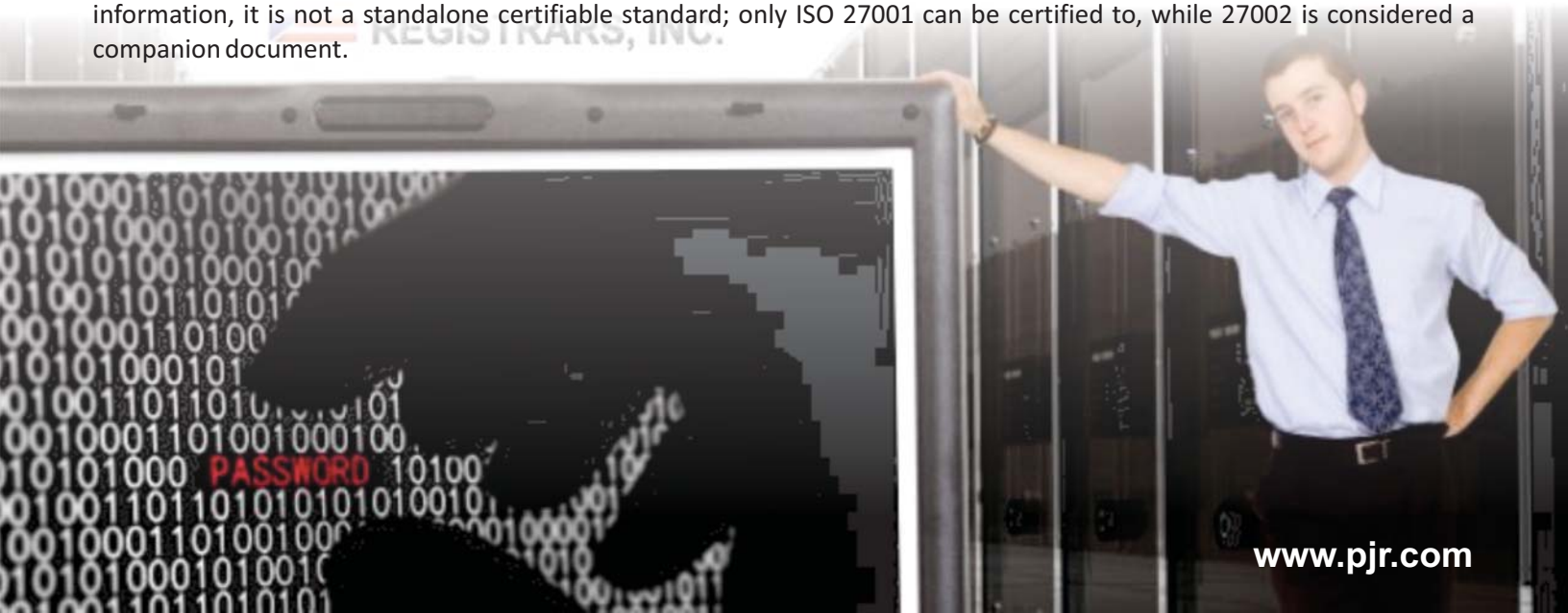
PERRY JOHNSON REGISTRARS, INC.

ISO 27002: How Is It Different From 27001 And What's New?

ISO 27001 is a globally-known standard for information security and technology, offering businesses of all sizes the assurance of tried-and-true practices to protect not only their assets, but their clients' as well. But slightly less well-known is ISO 27002 – a name that has cropped up far more often in the past several months as updates and changes have been announced. What exactly *is* 27002, and how does it influence ISO 27001?

Where ISO 27001 is the fundamental core of the ISO 27000 series of standards, ISO 27002 is a supplementary standard. It focuses on the information security controls listed in Annex A of 27001 that companies may choose to implement, and offers advice on how to best implement them. However, where the ISO 27001 standard merely offers a list of these controls with a brief description, 27002 does a deep dive on each one; each control has at least a page of content dedicated to it!

If this level of detail was included in ISO 27001's standard, it would become unnecessarily long. With over 100 controls to cover, the depth and breadth needed to do each one justice needed its own document. That said, while ISO 27002 is rich in information, it is not a standalone certifiable standard; only ISO 27001 can be certified to, while 27002 is considered a companion document.



Within ISO 27002:2013, the 114 information security controls are broken into 14 categories, as follows:

- Information security policies
- Human resource security
- Access Control
- Physical and environmental security
- System acquisition, development, and maintenance
- Information security incident management
- Information security aspects of business continuity management
- Organization of information security
- Asset management
- Cryptography
- Operations security
- Communications security
- Supplier relationships
- Compliance

Using both ISO 27001 and 27002 in tandem is crucial, especially as an organization conducts a risk assessment to identify and give priority to information security threats. Not all controls will apply to every business; establishing which controls to focus on is the most important first step.

But what is changing in ISO 27002 that's been bringing awareness of the standard to public awareness? Simply put, the standard is being restructured. As opposed to the 14 sections of 114 controls, ISO 27002:2022 will be condensed into 93 controls in the following 4 sections, plus 2 annexes:

- Organizational controls (clause 5)
- Physical controls (clause 7)
- Annex A – Using attributes
- People controls (clause 6)
- Technological controls (clause 8)
- Annex B – Correspondence with ISO/IEC 27002:2013

This restructuring of ISO 27002 will also mean that ISO 27001 is looking at an upcoming update as well, with updated reference to the new 27002 sections as well as the new reduced number of controls. Once this new revision of ISO 27001 is released, there will be an approximately 2-3 year transition period during which certified companies will be expected to adopt the new control set and update their systems to match.

To stay up-to-date on ISO 27001 and 27002 updates, join PJR's mailing list by visiting our website: **www.pjr.com**! To learn more about our ISMS programs and free resources, give us a call at **(248) 358-3388** today!