



## **ISO 27001**

ISO/IEC 27001:2013 (ISO 27001) is an international standard that helps organizations manage the security of their information assets. It provides a management framework for implementing an ISMS (information security management system) to ensure the confidentiality, integrity, and availability of all corporate data (such as financial information, intellectual property, employee details or information managed by third parties).

It was published in 2013 by the ISO (International Organization for Standardization) and IEC (International Electrotechnical Commission) and belongs to the ISO 27000 family of standards. It is the only internationally recognized certifiable information security standard.

ISO 27001 is supported by its code of practice for information security management, ISO/IEC 27002:2013, which explains how to implement information security controls for managing information security risks.

URS along with our international partner that has the experience of hundreds of ISO 27001 projects, will take care of the ISO 27001 regulation.

URS will begin the project with compliance training, compliance plans & policies co-developed by URS & Mullen Coughlin plus a compliance task monitoring & tracking system so your business can progress to additional ISO 27001 compliance services. We will also provide ongoing project management, quarterly webinars, and a review of your cyber insurance annually.

### **ISO 27001 Controls and Requirements**

ISO 27001 consists of 114 controls (included in Annex A and expanded on in ISO 27002) that provide a framework for identifying, treating, and managing information security risks.

## A summary of the ISO/IEC 27001: 2013 controls

- A.5 Information security policies
- A.6 Organization of information security
- A.7 Human resources security
- A.8 Asset management
- A.9 Access control
- A.10 Cryptography
- A.11 Physical and environmental security
- A.12 Operational security
- A.13 Communications security
- A.14 System acquisition, development, and maintenance
- A.15 Supplier relationships
- A.16 Information security incident management
- A.17 Information security aspects of business continuity management
- A.18 Compliance

In addition to the controls, ISO 27001 is made up of 10 management system clauses that provide guidance on the implementation, management, and continual improvement of an ISMS.

- 1, 2, and 3: Scope, normative references, and terms and definitions
- 4: Context of the organization
- 5: Leadership
- 6: Planning
- 7: Support
- 8: Operation
- 9: Performance evaluation
- 10: Improvement