

# LPO NETWORK

Linking Users & Providers of Legal Process Outsourcing (LPO) Services  
CORPORATE RISK ADVISORS, L.L.C. • [www.corpriskadvisors.com](http://www.corpriskadvisors.com)

**ISO 27001: The Emerging Gold Standard for Data Protection** by Edward J. Burke (with co-author Manisha Dwivedi, not pictured)



Edward J. Burke (with co-author Manisha Dwivedi, not pictured)

Bodhi Global Services Ltd.  
[edward.burke@bodhiglobal.com](mailto:edward.burke@bodhiglobal.com)

As increasing numbers of companies decide to outsource significant parts of their business and legal operations overseas, the need for strict data protection protocols becomes more critical.

With confidential and sensitive information traveling across international boundaries (whether physically or virtually), companies must assure themselves that the information remains protected. This is important not only because of the company's imperative to protect its own confidential data, but also because new laws relating to data protection and privacy typically require certain levels of protection to be in place before data from a country can be reviewed outside its boundaries. [Note 1]

Furthermore, as a corollary to the increased importance of corporate governance measures, companies are now beginning to analyze the risks to which their data and corporate information is subject (*e.g.*, breach of security and theft of data), calculating the probability of such risks occurring, and determining the negative impact of such an occurrence. A security risk relating to corporate information can be defined as any activity or event which threatens the achievement of identified business objectives by compromising the availability, confidentiality or integrity of the information.

The International Organization for Standardization ("ISO") [Note 2] published the ISO 27001 standard in October 2005. [Note 3] This standard specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an Information Security Management System ("ISMS") within the context of the company's overall risk management processes. It covers all types of organizations and specifies the requirements for the implementation of security controls customized to the needs of the individual company. The standard defines its approach as "[t]he application of a system of processes within an organization, together with the

identification and interactions of these processes, and their management." It employs the PDCA (Plan-Do-Check-Act) model to structure the processes.

Under ISO 27001, the company establishes the ISMS policy according to the characteristics of the business, including the company organization, its location, assets and technology. When articulating the risks of the business, the company identifies the assets within the ISMS, the threats to those assets, the vulnerabilities that might be exploited by those threats, and the impact that the loss of confidentiality, integrity and availability might have on those assets. Under the company's ISMS, it will analyze and evaluate the risks (*e.g.*, the consequences of a loss of confidentiality), assess the realistic likelihood of security failures occurring in the light of prevailing threats, estimate the levels of risk and determine whether the risks are acceptable. Annex A of ISO 27001 lists a number of controls that can be put into place to mitigate or possibly eliminate the risks to which information is subject, including the following:

- **Security policy** – management direction and support for information security
- **Organization of assets and resources** – management of information security within the organization
- **Asset classification and control** – identifying assets and providing appropriate protection to corporate information
- **Personnel security** – reducing the risks of human error, theft, fraud or misuse of facilities
- **Physical and environmental security** – preventing unauthorized access, damage and interference to the business premises
- **Communications and operations management** – ensuring the secure operation of the business facilities
- **Access control** – controlling the access to information (*e.g.*, controls on use of mobile computing devices like laptops; implementation of perimeter security devices)
- **Systems development and maintenance** – ensuring that security is built into the information systems
- **Information security incident management** – ensuring an effective management system that can respond to security incidents and avoid their reoccurrence
- **Business continuity and management** – anticipating interruptions to business activities and protecting important business processes from the effects of major disasters
- **Compliance** – avoiding breaches of any criminal and civil law, as well as statutory, regulatory or contractual obligation.

Outside auditors certify whether the company has adequately complied with ISO 27001. Certification of the company's ISMS is one means of providing assurance that the company has implemented a system for the management of information security that is aligned with the internationally accepted standard. Credibility is the key advantage of being certified by a respected and independent third party. The assurance it provides gives confidence to management, business partners, clients and auditors that the organization is serious about information security management.

In light of the heightened global concern about providing data and information security and protecting confidential client information, LPOs in India have begun the process of implementing data security protocols like ISO 27001. By providing standards of security that can be measured

objectively, LPOs have recognized the importance of having a systematized and defensible approach to data security and are leading the way to achieving this important goal in the legal support services industry.

## Endnotes

[Note 1] See Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *Official Journal of the European Communities of 23 November 1995*, No. L. 281 p. 31. Section 56 of the Directive provides as follows: "Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals, guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third countries which ensure an *adequate level of protection*; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations." (*Emphasis added*).

[Note 2] The ISO was founded in 1947 and is headquartered in Geneva, Switzerland. Its purpose is to develop standards that support and facilitate international trade.

[Note 3] The standard was published by ISO and the International Electrotechnical Commission. Its full name is ISO/IEC 27001:2005 – Information technology – Security techniques – Information security management systems – Requirements, but it is commonly referred to as "ISO 27001."

[Note 4] PDCA is an iterative four-step process typically used to implement change. "Plan" involves establishing the objectives and processes necessary to deliver results in accordance with the project specifications. "Do" involves implementing the process. "Check" involves monitoring and evaluating the processes and results against the objectives and specifications of the project. "Act" involves taking action to achieve the desired goals, as well as modifying the process to continually improve it.

About the Authors: Ed Burke is President of Bodhi Global Services Ltd. and is based in New York. Manisha Dwivedi is an Associate with Bodhi Global and is based in Mumbai, India. The authors would like to thank PCS Technology Limited - Consulting Division (<http://www.pcstech.com>) for its review of this article. PCS has been providing consulting services to Bodhi Global relating to its implementation of the ISO 27001 standards in its Indian facilities.



**Network**, *noun*. (1) an open fabric woven of interlaced and knotted strands; (2) something made up of interdependent or related parts; *verb*. (1) communicate. Synonyms: acquaint, advise, announce, broadcast, collaborate, connect, connections, contact, convey, correspond, disseminate, enlighten, inform, interface, interchange, link, proclaim, publicize, publish, relate, tell, transmit. [*Rogert's New Millennium™ Thesaurus, First Edition*]