secure islands

ISO 27001

IQProtector™ FOR ISO 27001 COMPLIANCE

MAY 2015

ISO 27001

TABLE OF CONTENTS

WHAT IS ISO 27001?

Published in 2013 and replacing the previous standard from 2005, ISO 27001 is an information security standard jointly created by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

The ISO 2700x series of specifications actually encompasses a number of standards, numbered from 27000 to 27008. In this paper, we'll focus on the most-referenced and relevant of these, the standard for ISMS (27001). ISO 27001 defines the policies and procedures – including legal, technical, and physical controls – that make up an organization's information security management system (ISMS).

According to the standard's creators, the goal of ISO 27001 is to "…provide requirements for establishing, implementing, maintaining and continually improving an information security management system." This high-level goal is achieved through a long and detailed list of specific information security requirements, which are delineated in the 30-page document.

For more information read: ISO/IEC 27001:2013 | Information technology | Security techniques | Information security management systems | Requirements.

WHY ISO 27001 COMPLIANCE?

From a purely practical point of view, ISO 27001 certification is rapidly becoming a requirement to do business with many major multinationals. Even in situations where certification is not strictly required, vendors who are certified are preferred.

But beyond this, achieving ISO 27001 compliance is an opportunity for organizations to take an in-depth and structured look at their information security management systems. The certification process demands that risks be identified, and controls put in place to manage and mitigate them. It stipulates that controls be adapted to the diverse aspects of the organizational business model, and scaled to meet growing demand. Moreover, and perhaps most important in today's volatile and security-conscious business climate, ISO 27001 compliance demonstrably enhances stakeholder and customer trust in the safety of their data.

A SMOOTHER, MORE PRODUCTIVE PATH TO COMPLIANCE

Meeting the requirements delineated in ISO 27001 demands the adoption of strategic security tools that seamlessly integrate with existing workflow and infrastructure, easily scale with enterprise growth, and do not impede productivity. Effective solutions for ISO 27001 compliance need to facilitate the secure, smooth flow of information, while still protecting sensitive data from any source throughout the information lifecycle.

Secure Islands **IQProtector Suite** offers a revolutionary information security paradigm that is naturally in-line with the spirit and letter of ISO 27001. Unlike traditional solutions that demand compliance workarounds or clunky workflow adaptations - **IQProtector Suite's data-centric security model delivers a smoother, more productive path to compliance by making organizational information security inherently simpler and more intuitive.**

Secure Islands' IQ Protector Suite leverages a data-centric approach to data protection – applying classification and protection to sensitive data on creation. It intelligently generates, applies and enforces encryption policies enterprise-wide for data at rest, in motion and in use - ensuring that data classification remains intact throughout the entire data lifecycle

Based on flexibly-defined parameters, IQProtector Suite classifies in real-time sensitive data from any source – users, applications, file repositories or directories. Then, leveraging existing IRM and encryption frameworks, IQProtector Suite intelligently generates, applies and enforces encryption policies enterprise-wide. Moreover, IQProtector Suite provides advanced tracking and reporting based on big-data analytics, allowing organizations complete, enterprise-wide visibility of internal and external data usage.

MEETING SPECIFIC ISO 27001 REQUIREMENTS

IQProtector Suite facilitates compliance with the majority of ISO 27001's electronic information security requirements, including the following sections of the standard's "Control Objectives and Controls" specification:

Section A.5.1 Management direction for information security

IQProtector provides management with direction and support for information security by performing a content-aware, infrastructure-agnostic, usage-based discovery process. IQProtector analyzes and classifies data accessed during actual business activity, creating an enterprise-wide mapping of where sensitive data resides, who accesses it, where it is sent, and how it is used. This granular data usage visibility assists in enterprise policy definition, helping management identify, assess, and eliminate risks at their roots.

Section A.6.1 Internal organization

IQProtector helps establish a management framework to initiate and control the implementation and operation of information security within the organization by creating and enforcing enterprise-wide entitlements which are constantly updated, infrastructure-agnostic, and enforced transparently. This creates a strict and documentable segregation of duties for each individual piece of data, which is applied to both privileged and regular users - enabling complete and centrally-governed visibility over sensitive data usage.

Section A.6.2 Mobile devices and teleworking

IQProtector ensures the security of teleworking and use of mobile devices by applying data protection that is completely infrastructure and device agnostic. IQProtector's Mobile AD RMS Support is an easy-to-use, easy-to-manage and easy-to-deploy solution for secure emailing, including attachments. Mobile AD RMS Support enables application of AD RMS protection over any mobile OS, without end user training, and with no client installation on the mobile device.

Section A.7.3 Termination and change of employment

IQProtector ensures that employees and contractors are aware of and fulfil their information security responsibilities, and protects the organization's interests as part of the process of changing or terminating employment. Based on an ongoing infrastructure-agnostic, usage-based discovery process, IQProtector extends organizational AD RMS capabilities, enabling creation of effective enterprise-wide entitlements. Once in place, these entitlements are enforced transparently and automatically – and updated instantly, enterprise-wide, when employment status or other relevant parameters change.

Section A.8.1 Responsibility for assets

IQProtector identifies organizational assets and defines appropriate protection responsibilities by analyzing and classifying data accessed during actual business activity, then creating an enterprise-wide mapping of where sensitive data resides, who accesses it, where it is sent, and how it is used. This granular data usage visibility assists in enterprise policy definition, helping management identify, assess, and eliminate risks at their roots.

Section A.8.2 Information classification

IQProtector helps ensure that information receives an appropriate level of protection in accordance with its importance to the organization, as defined by policy or user-driven classification. Leveraging a powerful classification engine, **IQProtector** adaptively applies intelligent categorization based on both content and context – resulting in non-intrusive, multi-layer, persistent classification of sensitive data from any source – users, applications, file repositories, directories, devices, and more. Designed to maximize both security and productivity, **IQProtector** offers organizations fully automated policy-based classification, user-driven classification, or classification according to system recommendation.

Section A.8.3 Media handling

IQProtector prevents unauthorized disclosure, modification, removal or destruction of information stored on media by ensuring that all sensitive information stored on endpoints of any type is secured. **IQProtector** detects, captures and protects user-generated data or data downloaded or uploaded from various data stores, storing it in encrypted format without compromising search or indexing operations.

Section A.9.2 User access management

IQProtector limits access to information and information processing facilities, providing users with access only to information they have been specifically authorized to use. IQProtector enforces policy-based entitlements transparently and automatically, supporting separation of duties on any piece of data among privileged and other users, and facilitating constantly-monitored, centrally-governed compartmentalization of information while enabling complete visibility over sensitive data usage.

Section A.10.1 Cryptographic controls

IQProtector extends the capabilities of existing IRM systems like Microsoft RMS, ensuring proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information. A powerful classification-based IRM enabler, IQProtector makes sure that sensitive information is consistently and persistently encrypted, without impeding search indexers and anti-virus programs, ECM/DMS systems, backup systems, or workflow. Harnessing the flexibility and security of MS Azure AD/Azure RMS, IQProtector also facilitates secure key exchange, and always retains encryption keys and identities within the organization.

Section A.12.1.2 Change management

IQProtector ensures that changes to the organization, business processes, information processing facilities and systems that affect information security are controlled. By automating and centralizing enforcement of corporate security policies, permissions, user access to sensitive information, IQProtector facilitates enterprise-wide response to change at the click of a button, from one central location.

Section A.12.2 Protection from malware

IQProtector ensures that information and information processing facilities are protected against malware-based intrusions. Even if corporate networks are breached, IQProtector-protected networks are immune to data leakage, since all sensitive information is persistently and automatically encrypted, and inaccessible to unauthorized parties. Moreover, IQProtector facilitates more effective anti-malware activity, by making sure encrypted content is still accessible to scanning by anti-malware programs.

Section A.12.4 Logging and monitoring

IQProtector records events and generates evidence to create a full enterprise-wide audit trail covering access and usage of data classified as sensitive. IQProtector logs every action involving sensitive data (save, forward, open, attempts to change classification, and much more) for auditing and forensics purposes. Moreover, IQProtector leverages big data analytics to enable ongoing data-centric risk assessment and reporting, identifying trends and spotting risks based on actual data usage.

Section A.12.7 Information systems audit considerations

IQProtector minimizes the impact of audit activities on operational systems by enabling immediate and ongoing access to audit trail data and analysis from one central location.

Section A.13.1.3 Segregation in networks

IQProtector ensures that groups of information services, users and information systems shall be segregated on networks, by creating and enforcing strict and documentable segregation of duties for each individual piece of data, delivering complete and centrally-governed visibility over sensitive data usage.

Section A.13.2 Information transfer

To maintain the security of information transferred within an organization and with any external entity, IQProtector identifies and classifies sensitive data of any origin – database, application, or file. Once classified and tagged as sensitive, this data is persistently protected – whether in use by an authorized user, in transit electronically or physically, or in storage. Since IQProtector embeds protection within the data itself, the system can recognize not only who accesses the data, but also where it is accessed. Using secure and tamper-proof geo-location technology, IQProtector delivers demonstrable cross-border data protection.

Section A.14.2.7 Outsourced development

To ensure that information security is an integral part of information systems across the entire lifecycle, including information systems which provide services over public networks, IQProtector applies persistent protection to **all sensitive data.** Since IQProtector embeds protection within the data itself, sensitive data is protected in use, in storage, and in transit – whether over public or private networks. Designed to facilitate productivity as well as security, IQProtector leverages MS Azure to enable secure collaboration over public internet, enforcing corporate security policies even when communication is with partners or customers outside of the organizational network.

A.15.1 Information security in supplier relationships

IQProtector ensures protection of organizational assets accessible by suppliers by enforcing policy-based entitlements transparently and automatically, supporting separation of duties on any piece of data among internal users and suppliers, and facilitating centrally-governed compartmentalization of information. Moreover, IQProtector enables secure collaboration with suppliers, enforcing corporate security policies even when communication is over public networks and with partners outside of the organizational network. Leveraging MS Azure AD/Azure RMS, IQProtector also facilitates secure key exchange, retaining encryption keys and identities **within the organization**.

A.16.1 Management of information security incidents and improvements

IQProtector ensures a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses. Leveraging sophisticated online analytical processing (OLAP), real-time forensic-level analysis, and behavioral anomaly detection - IQProtector analytics keeps security policy in-line with real-world usage. By quantifying internal and external exposure based on data, locations, and users, IQProtector helps optimize security policies, delivering a powerful yet accessible decision-making toolset.

A.18.1 Compliance with legal and contractual requirements

IQProtector helps organizations avoid breaches of legal, statutory, regulatory or contractual obligations related to information security by allowing full access to archived encrypted files, emails and documents in accordance with regulatory requirements. IQProtector helps organizations maintain compliance with no compromise on information security, allowing simple, user-transparent archiving with no disruption to normal workflow.

ABOUT IQPROTECTOR SUITE

Secure Islands' IQProtector Suite leverages a unique data-centric approach to data protection that Gartner recently called "visionary." With no impact on archiving, eDiscovery or other enterprise services, solutions from Secure Islands protect sensitive data from its source and throughout its life cycle – at rest, in motion, and in use.

Based on flexibly-defined parameters, IQProtector Suite classifies in real-time sensitive data from any source – users, applications, file repositories or directories. Then, leveraging existing IRM and encryption frameworks, IQProtector Suite intelligently generates, applies and enforces encryption policies enterprise-wide.

ABOUT SECURE ISLANDS

Secure Islands develops and markets advanced Information Protection and Control (IPC) solutions for the borderless enterprise. Offering policy-driven classification and protection for unstructured data, Secure Islands lays the foundation for sensitive information security in enterprises as they shift from perimeter defense to persistent protection. Secure Islands' holistic approach literally redefines information security and assists the enterprise in regaining control by identifying, classifying and protecting sensitive information throughout its lifecycle. Founded in 2006 and headquartered in Israel, the company's solutions are deployed in top-tier Fortune 500 firms and government agencies worldwide. For more information, please visit www.secureislands.com.