THE KEY CHANGES IN THE ISO/IEC DIS 27002

BE THE BENCHMARK

SGS

INTRODUCTION

ISO/IEC 27002 is a guidance document and it is designed to use as a reference for selecting controls while implementing an Information Security Management System (ISMS) based on ISO/IEC 27001 or as a guidebook for organizations implementing commonly accepted information security controls. The current ISO/IEC 27002:2013 edition had been under reviewed since last year by ISO/IEC JTC 1/SC27 and is currently at DIS (Draft International Standard) stage. While part of controls remains unchanged, there are significant changes in control layout and other controls. Since the Annex A of ISO/IEC 27001:2013 is designed to align with ISO/IEC 27002, it is expected that the Annex A of ISO/IEC 27001 would be revised as well after the ISO/IEC 27002 is finalized.

This article highlights the key changes in the DIS as compared to ISO/IEC 27002:2013 edition. The audience is reminded that the DIS is still under review and the FDIS (Final Draft International Standard) or the final published standard may still vary from the DIS. It is not the purpose of this article to explain or justify the changes.

KEY CHANGES

NUMBER OF CONTROLS 93

There are 93 controls in DIS vs 114 controls in the 2013 edition.

NEW CONTROLS 12

12 new controls are introduced to address the evolvement in technologies and industrial practices.

CHANGING LANDSCAPE OF TECHNOLOGY USE AND DATA PROTECTION

5.7 Threat intelligence

5.23 Information security for use of cloud services

8.12 Data leakage prevention

INCLUSION OF SENSITIVE DATA PROTECTION CONTROLS

8.10 Information deletion

8.11 Data masking

RECOGNITION OF ESSENTIAL ROLE OF TECHNOLOGY IN BUSINESS RESILIENCE

5.30 ICT readiness for business continuity

OTHER NEW CONTROLS –

5.16 Identity management

7.4 Physical security monitoring

8.1 User endpoint devices

8.9 Configuration management

8.22 Web filtering

8.28 Secure coding

CONTROL CATEGORIES 4

Controls are regrouped into 4 categories, instead of 14 categories in 2013 edition. This new control layout facilitates management to assign responsibilities within the organization for information security enhancement.

ISO/IEC 27002:2013		
5 Information security policies	6 Organization of information security	7 Human resource security
8 Asset management	9 Access control	10 Cryptography
11 Physical and environmental security	12 Operations security	13 Communications security
14 System acquisition, development and maintenance	15 Supplier relationships	16 Information security incident management
17 Information security aspects of business continuity management		18 Compliance

ISO/IEC DIS 27002	
5 Organizational controls	6 Organization of information security
7 Physical controls	8 Technological controls

LEGACY CONTROLS 16

16 controls are removed.

5.1.2	Review of the policies for information security	12.4.2	Protection of log information
6.2.1	Mobile device policy	12.6.2	Restrictions on software installation
8.1.2	Ownership of assets	13.2.3	Electronic messaging
8.2.3	Handling of assets	14.1.2	Securing application services on public networks
9.4.3	Password management system	14.1.3	Protecting application services transactions
11.1.6	Delivery and loading areas	14.2.9	System acceptance testing
11.2.5	Removal of assets	16.1.3	Reporting information security weaknesses
11.2.8	Unattended user equipment	18.2.3	Technical compliance review

CONTROLS WITH MODIFICATIONS

SIMILAR CONTROLS ARE INTEGRATED TO BECOME ONE MAIN CONTROL. FOR INSTANCE:

ISO/IEC DIS 27002	ISO/IEC 27002:2013
SIMILAR CONTROLS ARE INTEGRATED TO BECOME ONE MAIN CONTROL. FOR INSTANCE:	
5.14 Information transfer	13.2.1 Information transfer policies and procedures
	13.2.2 Agreements on information transfer
8.24 Use of cryptography	10.1.1 Policy on the use of cryptographic controls
	10.1.2 Key management
	18.1.5 Regulation of cryptographic controls
CONTROLS OBJECTIVES ARE SEPARATED TO EMPHASIZE MONITORING	
8.15 Logging	12.4.1 Event logging
8.16 Monitoring activities	12.4.3 Administrator and operator logs
CLEARER FOCUS ON INFORMATION ASSET PROTECTION	
5.9 Inventory of information and other associated assets	8.1.1 Inventory of assets
5.10 Acceptable use of information and other associated assets	8.1.3 Acceptable use of assets

SUMMARY

While the explanation and justification of the changes in the DIS version are not released outside of JTC 1/SC27, it is apparent that the changes are to reflect the advancement of technologies and the evolving industrial practices. SGS will keep on top of changes and will keep our clients and the certification community abreast of the updates as soon as they come out.

SUBSCRIPTION

Subscribe to our newsletter for the latest news and events on international standards, regulations and management systems, and learn how to run your business for sustainable growth.

CONTACT SGS

www.sgsgroup.com.hk
learning.sgs.com/hk

hk.cbe@sgs.com

+852 2765 3620

facebook.com/sgshongkong

instagram.com/sgshongkong

www.sgs.com/linkedin

WWW.SGS.COM

WHEN YOU NEED TO BE SURE