Evaluating the Effectiveness of the ISO 27001:2013 based on the Annex A

Bahareh Shojaie · Hannes Federrath · Iman Saberi
University of Hamburg, Germany
http://svs.informatik.uni-hamburg.de

Universität Hamburg
DER FORSCHUNG | DER LEHRE | DER BILDUNG

9th International Workshop on Frontiers in Availability, Reliability and Security (FARES 2014), University of Fribourg, Swizerland, Sep 11, 2014

Introduction

- ISMS (Information Security Management System)
- ISO/IEC 27001

Annex A
(normative)

Reference control objectives and controls

The control objectives and controls listed in Table A.1 are directly derived from and aligned with those listed in ISO/IEC 27002:2013[1], Clauses 5 to 18 and are to be used in context with Clause 6.1.3.

Table A.1 — Control objectives and controls

A.5	**Information security policies**	
A.5.1	**Management direction for information security**	
Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1	Policies for information security	*Control* A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.
A.5.1.2	Review of the policies for information security	*Control* The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.
A.6	**Organization of information security**	
A.6.1	**Internal organization**	
Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1	Information security roles and responsibilities	*Control* All information security responsibilities shall be defined and allocated.
		Control

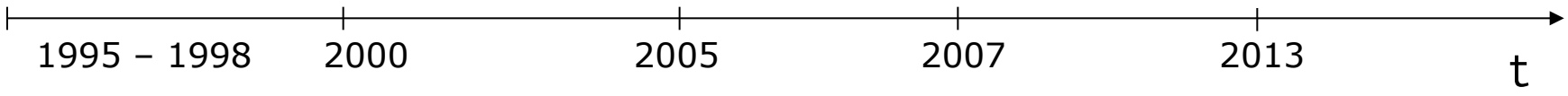
ISO 27001 History

Code of practice

BS 7799-1	ISO 17799:2000	ISO17799:2005	ISO27002:2007	ISO27002:2013

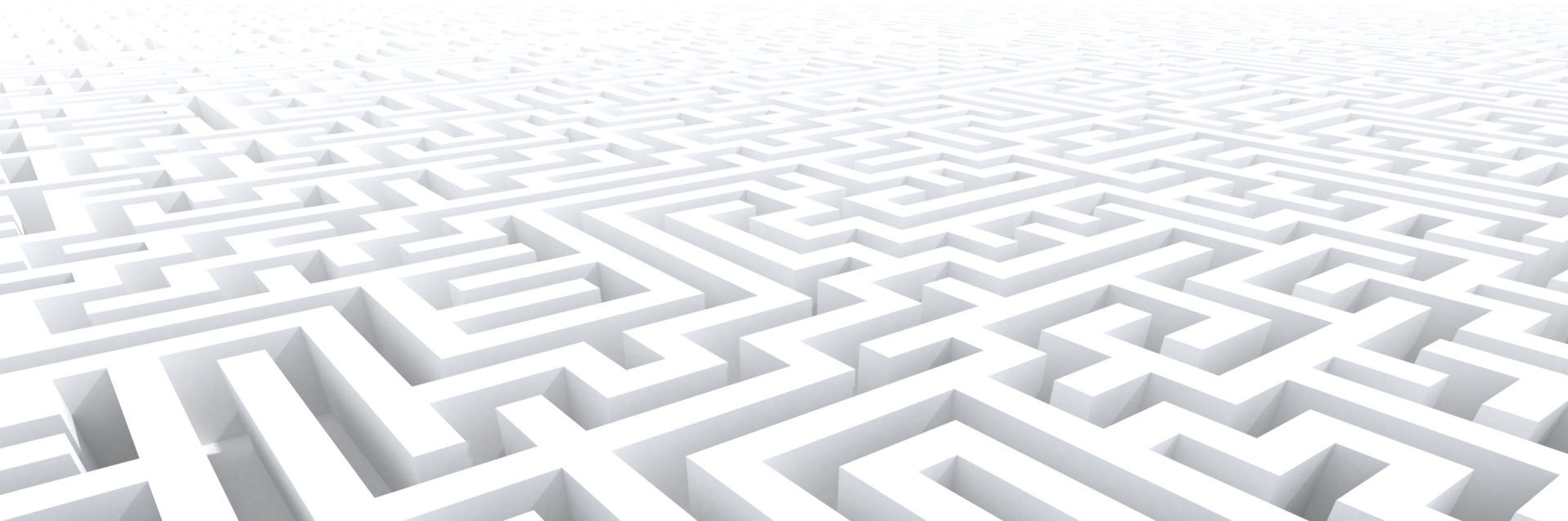
ISMS specification

BS 7799-2 Developed to support certification	BS 7799-2:2002	ISO 27001:2005	ISO27001:2013



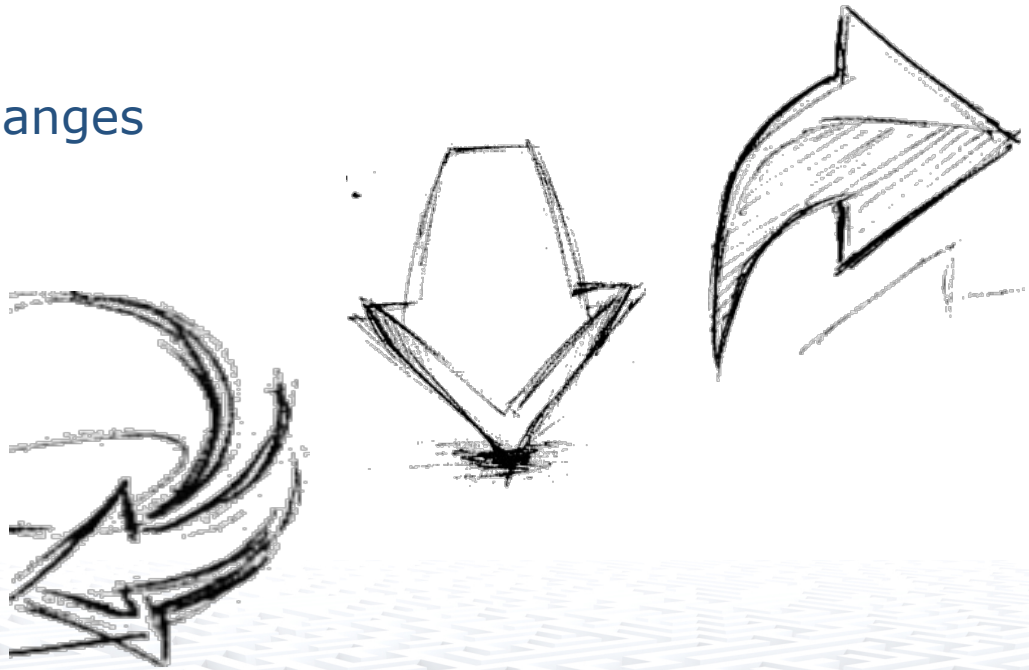
ISO 27001:2013 Looks Different..

- Annex SL
- ISO 27000:2013
- Terms & Definitions
- 114 controls in 14 groups vs. 133 controls in 11 groups
- Annex A



Transition to ISO 27001:2013

- Minimal Changes
- Rethink
- Updating



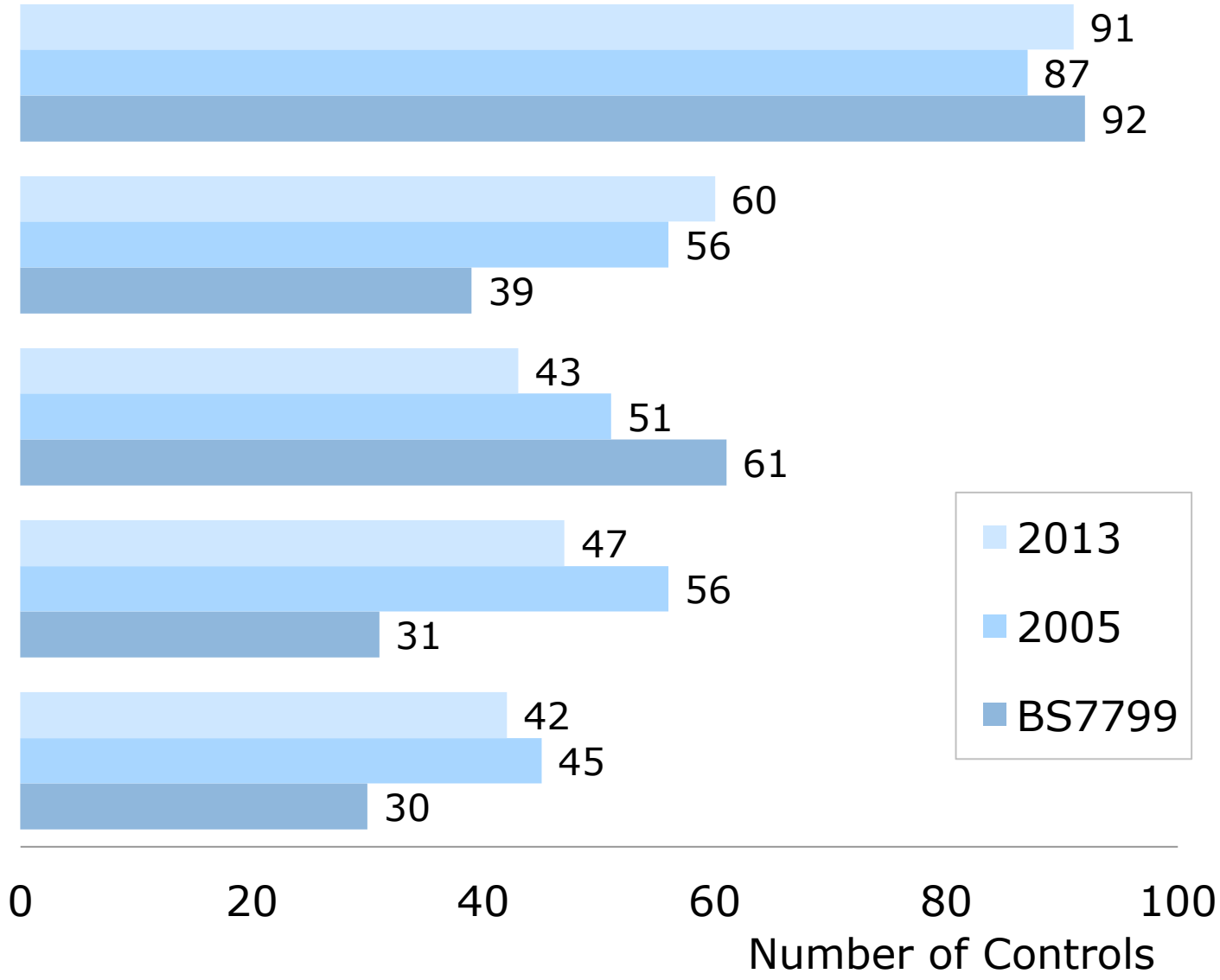
Our 5 Categories of the Annex A controls

- Data
  - e.g. A.8.1.1: Inventory of assets
- Hardware
  - e.g. A.8.3.1: Management of removable media
- Software
  - e.g. A.9.2.5: Review of user access rights
- People
  - e.g. A.9.2.2: User access provisioning
- Network
  - e.g. A.9.1.2: Access to networks services

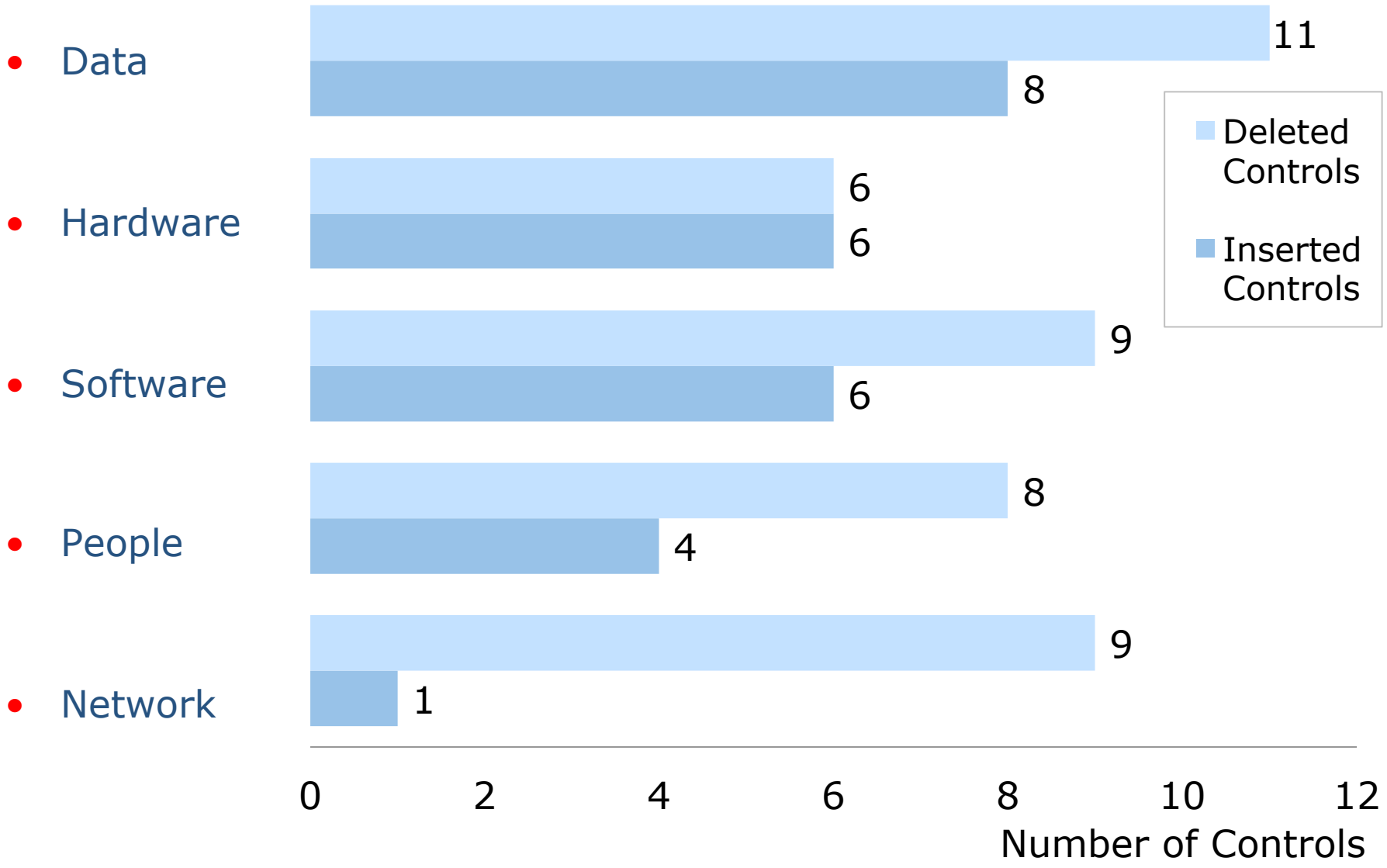
The assignment of the controls to our five categories can be found at https://svs.informatik.uni-hamburg.de/annexApaper/.

Our 5 Categories of the Annex A controls

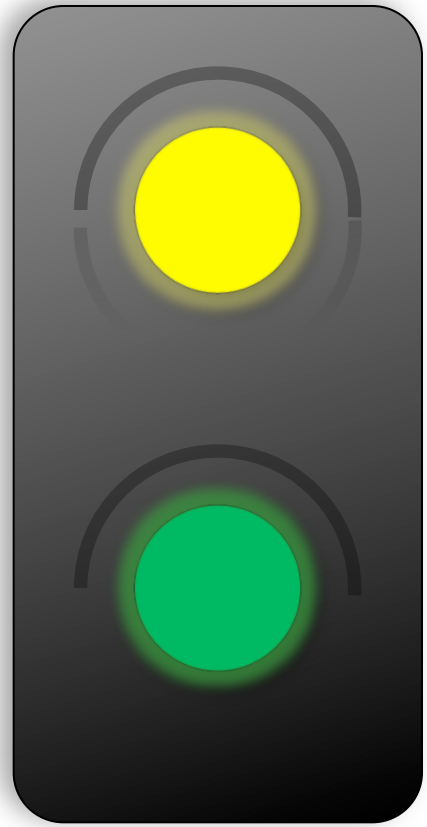
- Data
- Hardware
- Software
- People
- Network



Comparison between Inserted & Deleted Controls



Conclusion



May Require Improvement

- People
- Network

Acceptable Security

- Data
- Hardware
- Software

- Contact: shojaie@informatik.uni-hamburg.de