Federal Office
for Information Security

Mapping
from BSI C5 to ISO/IEC 27017

Refers to version 1.0 of BSI C5

Version 1.0

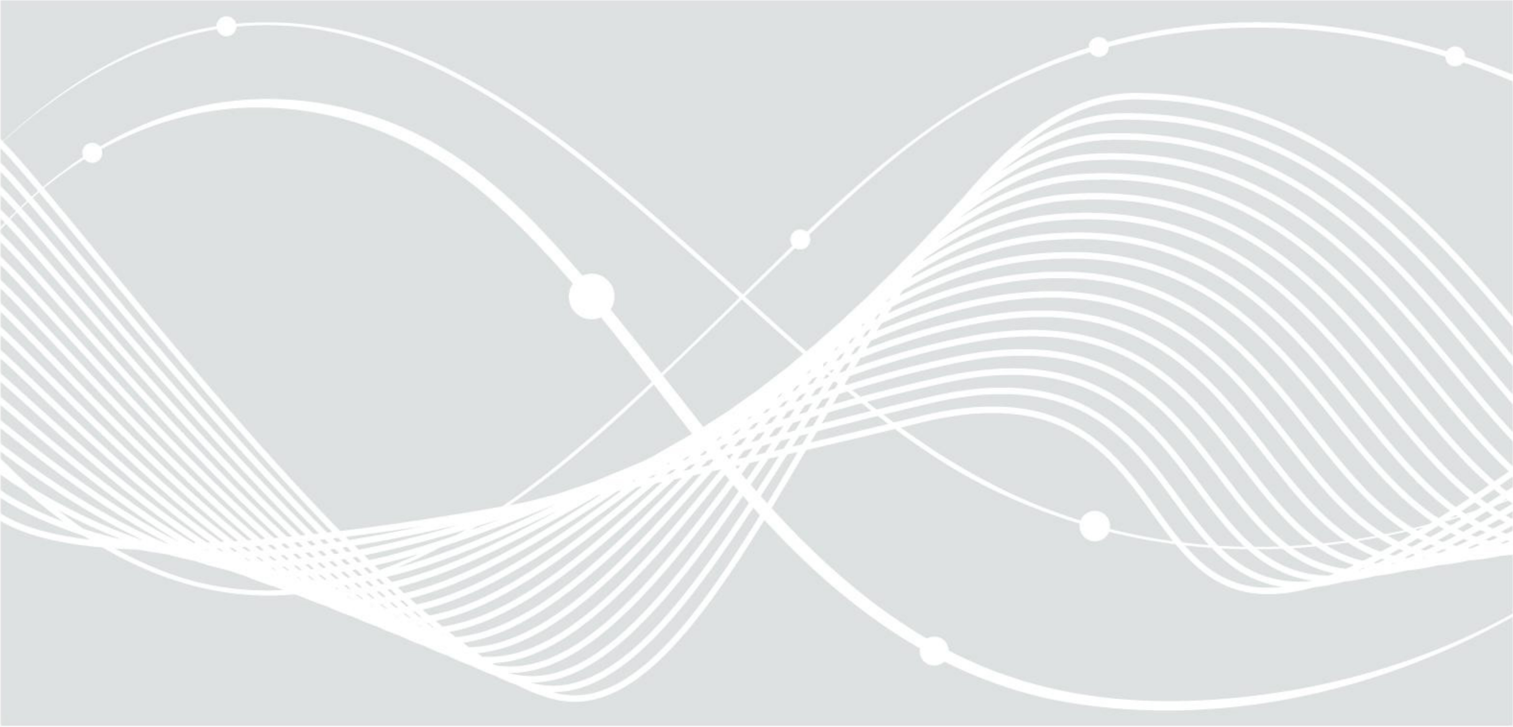

Table of Contents

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-6666
E-Mail: cloudsecurity@bsi.bund.de
Internet: https://www.bsi.bund.de/EN/C5

1 Introduction

The ISO standard 27017 "Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services" is a set of information security guidelines focusing on cloud services. It extends the ISO/IEC 27002 standard "Information technology - Security techniques - Code of practice for information security controls" with cloud specific aspects.

The extension of the standard is twofold. The "Implementation Guidelines" of ISO/IEC 27002 is extended with examples related to cloud computing, covering the perspectives both ofcloud service customers and cloud service providers. All the implementation guidelines of ISO/IEC 27002 are valid for cloud computing and are referenced in ISO/IEC 27017.

Furthermore, ISO/IEC 27017 introduces new controls for cloud computing. They are marked with the prefix “CLD” and extend the standard ISO/IEC 27001 „Information technology - Security techniques - Information security management systems – Requirements“ with seven new controls. For these controls, implementation guidelines for cloud service customer und cloud service provider are added.

For BSI C5 (Cloud Computing Compliance Controls Catalogue) there already exists a mapping of C5 controls to those of ISO/IEC 27001. The following table shows how the additional controls of ISO/IEC 27017 are covered by BSI C5 controls. Just as the other mappings on BSI website, the following table is meant to provide a first overview. It cannot substitute an in-depth analysis in the run-up to an audit.

2 Table

ISO 27017	C5	Explanation
CLD.6.3.1	OIS-03	CLD.6.3.1 describes the definition of roles and responsibilities within a cloud computing environment. This control is completely met with C5's OIS-03 control.
CLD.8.1.5	PI-02 PI-05	CLD.8.1.5 covers the deletion and removal of cloud service customer assets. PI-05 and PI-02 deal with the removal and return of customer data, i.e. customer assets. Commentary: In contrast to ISO, The AM (Asset Management) section of C5 covers assets that contribute to the provisioning of cloud services and not the customer data as assets themselves. As a consequence, these controls are not mapped here.
CLD.9.5.1	RB-23	The control CLD.9.5.1 describes the segregation in virtual computing environments. It is covered by RB-23.
CLD.9.5.2	RB-22	CLD.9.5.2 is concerned with the hardening of virtual machines. C5 does not differentiate between physical and virtual resources and therefore there is no specific control for virtual resources. This issue is covered by RB-23.
CLD.12.1.5	IDM-01 IDM-05 IDM-06	CLD.12.1.5 is about administrator's operational security. Whereas the focus in ISO/IEC 27017 is more on the customer side, C5 covers the provider's administrator operational security in IDM-01, IDM-05, and IDM-06.
CLD.12.4.5	-	CLD.12.4.5 describes the cloud service customer's ability to monitor cloud services. The functionality is provided by the cloud service provider. This control is not covered in C5.
CLD.13.1.4	KOS-01 to KOS-08	CLD.13.1.4 describes the alignment of physical and virtual networks. C5 makes no distinction between physical and virtual environments. Network security is covered in C5 controls KOS-01 to KOS-08.

3 Conclusion

The mapping shows clearly that BSI C5 covers the additional controls of ISO/IEC 27017 for the cloud service provider almost comprehensively. The control about monitoring for cloud service customer (CLD.12.4.5) is currently not covered by BSI C5.