FH MÜNSTER
University of Applied Sciences

GERMAN OWASP DAY 2018

Mapping technischer Schwachstellen aus der OWASP Top 10 auf ISO/IEC 27001 Controls

Tobias Kappert

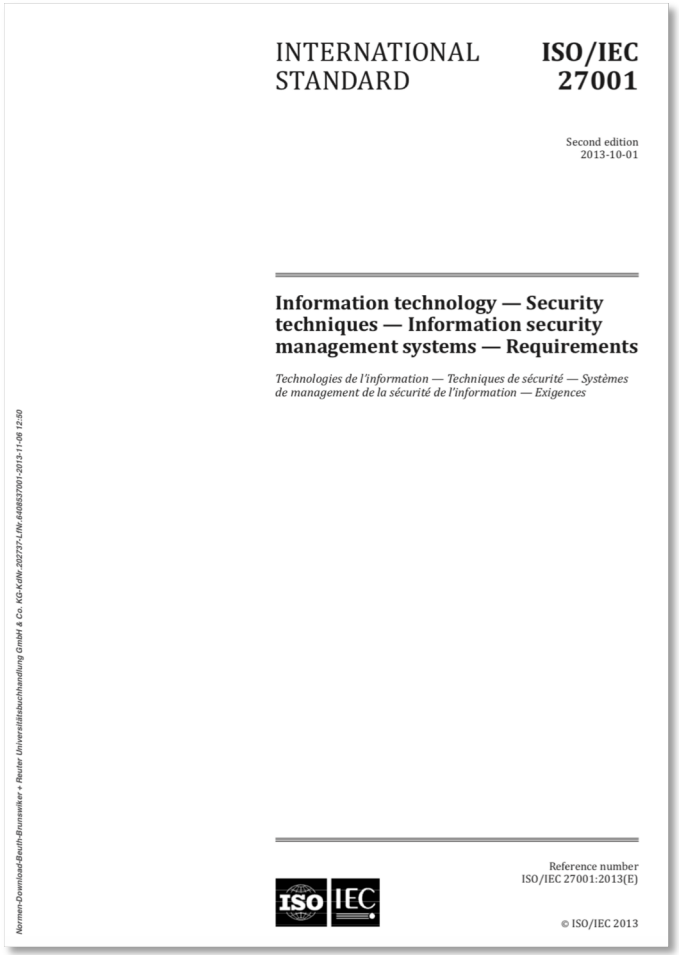
Münster, November 2018

ISO/IEC 27001

Standard für IT-Sicherheitsmanagement in Unternehmen nach ISO/IEC
- Schutz von Assets

ISO/IEC 27000-Familie ist sehr umfangreich
- Standards von ISO/IEC 27000 bis 27050 und 27799

Informations-Sicherheits-Management-System (ISMS)
- ISO/IEC 27001
- Zertifizierbar
- Annex A - Controls


INTERNATIONAL STANDARD

ISO/IEC 27001

Second edition
2013-10-01

Information technology — Security techniques — Information security management systems — Requirements

Technologies de l'information — Techniques de sécurité — Systèmes de management de la sécurité de l'information — Exigences

Reference number
ISO/IEC 27001:2013(E)

© ISO/IEC 2013

Normen-Download-Beuth-Brunswiker + Reuter Universitätsbuchhandlung GmbH & Co. KG-Kdnr. 202737-LfNr. 6488537001-2013-11-06 12:50

ISO/IEC 27001

Annex A - Controls

FH MÜNSTER
University of Applied Sciences

Aufbau Annex A

- Sicherheitsthema (14 Themen)
  - Maßnahmenziel (35 Ziele)
    - Abstrakte Zieldefinition
    - 1 bis *n* Controls je Ziel (114 Controls)

Hoher Abstraktionsgrad

- Controls definieren *was* geschützt werden soll
- Keine Vorgabe über das “Wie“

Control-Aufbau

- Nummer, Titel, Kurzbeschreibung

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.
A.6.1.2	Segregation of duties	*Control* Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization’s assets.
A.6.1.3	Contact with authorities	*Control* Appropriate contacts with relevant authorities shall be maintained.
A.6.1.4	Contact with special interest groups	*Control* Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.

+ Reuter Universitätsbuchhandlung GmbH & Co. KG-KdNr.202737-LfNr.6408537001-2013-11-06 12:50

ISO/IEC 27001 und ISMS

Mapping technischer Schwachstellen aus den OWASP Top 10 auf ISO 27001-Controls

Vorgehensweise

Generelles Vorgehen und Kriterien

Analyse

- OWASP Top 10
- Annex A – ISO Controls

Eigenschaften und Kriterien

- Risiken (Technischer und Business Impact)
- Angriffsmodell
  - Direkter Angriff
  - Angriff durch Ausnutzen menschlicher Komponente (Phishing)
- Schwachstellenart
  - Web oder Desktop

Mapping – direkt oder mittelbar

Vorgehensweise

Beispiel einer OWASP Top 10 Schwachstelle (SQL-Injection)

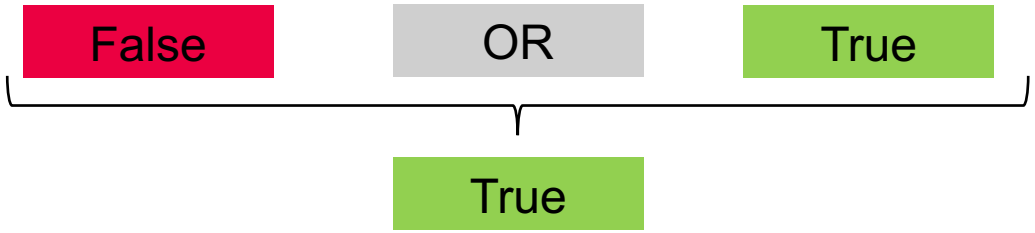
```
String sql = "SELECT * FROM users";
sql      += "WHERE username='" + username + "' ";
sql      += "AND   password='" + password + "' ";
ResultSet rs = st.executeQuery(sql);
```

Attack:

```
username=admin, password=' or '1' = '1
```

Resulting SQL command:

```
SELECT * FROM users
WHERE username='admin' AND password='' or '1' = '1'
```



Vorgehensweise

Mapping am Beispiel der SQL-Injection

	Relevant	SQL-Injection
A 11 Physical and environmental security	Nein	-
…	…	…
A 12.6.1 Management of technical vulnerabilities	Ja	Direkt
A 14.2.1 Secure development policy	Ja	Direkt
A 14.2.8 System security testing	Ja	Mittelbar
A 18.1.3 Protection of Records	Ja	Direkt

Vorgehensweise

Mapping am Beispiel einer Security Misconfiguration

	Relevant	Security Misconfiguration
A 11 Physical and environmental security	Nein	-
…	…	…
A 12.6.1 Management of technical vulnerabilities	Ja	Direkt
A 14.2.1 Secure development policy	Ja	Mittelbar
A 14.2.8 System security testing	Ja	Mittelbar
A 18.1.3 Protection of records	Ja	Direkt

Ergebnis

Mapping-Kreuz-Tabelle

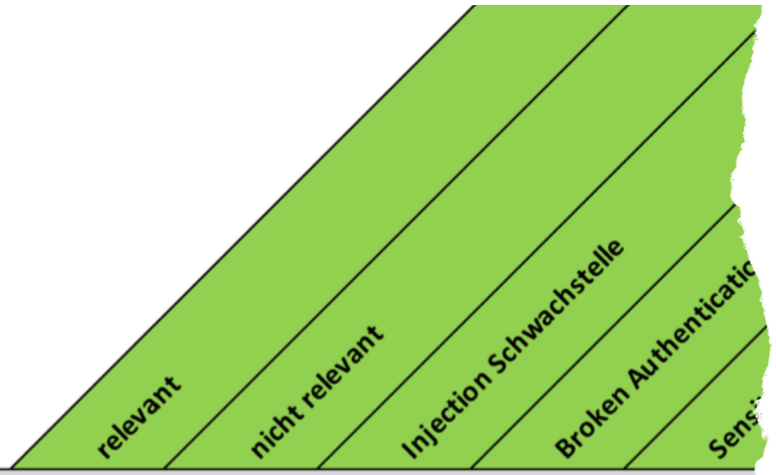
Cluster

- Alle Schwachstellen direkt
- Alle Schwachstellen mittelbar
- Alle Schwachstellen direkt/mittelbar
- Spezifische Schwachstellen

der gewählten OWASP Top 10

s jeweils von dem Security
e, Abhängigkeit oder den
und kommuniziert werden.

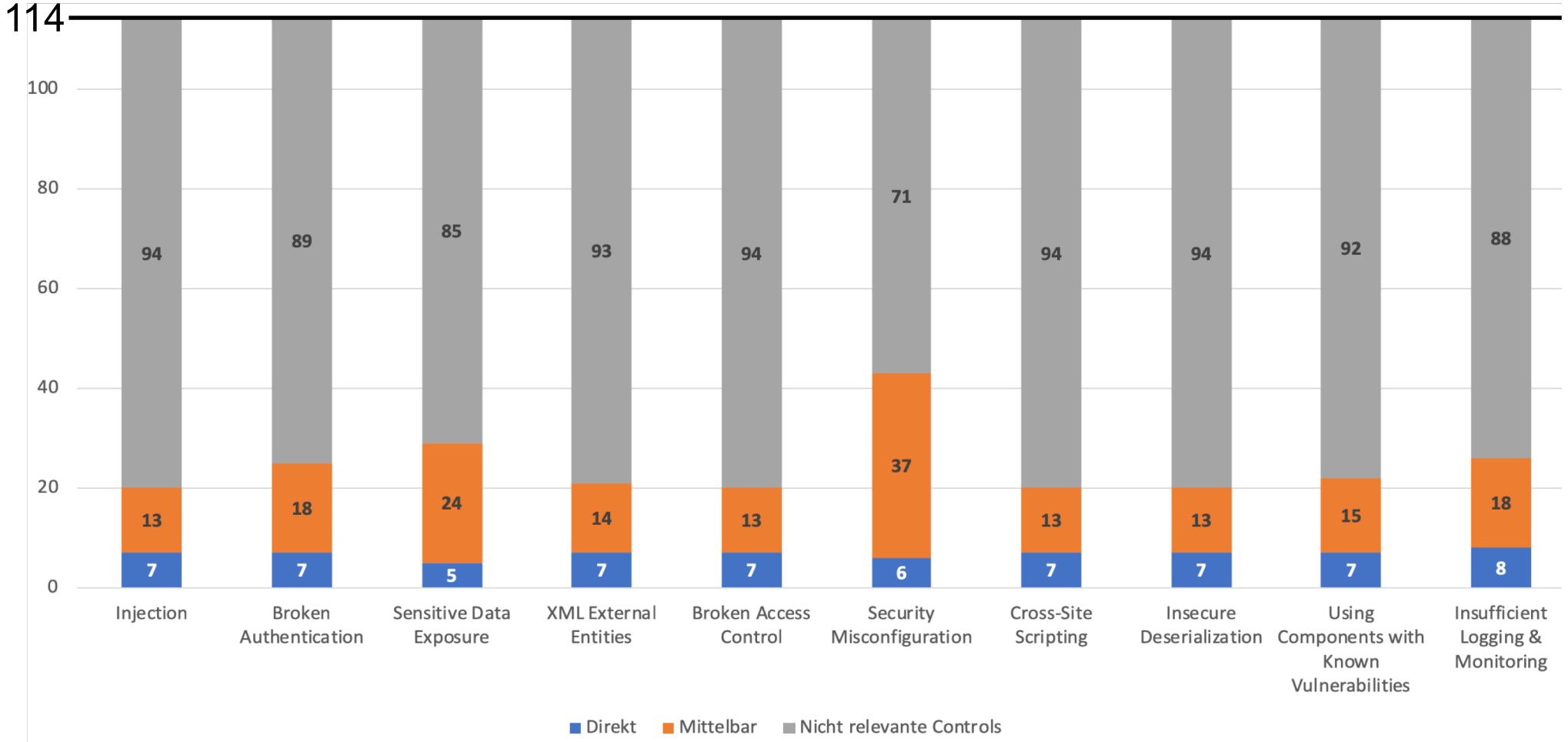
Gründe: die Anwendung, der



A.14.2.1	Secure development policy	Rules for the development of software and systems shall be established and applied to developments within the organization.	X		X	X	M
A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	X		X	X	X
A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of outsourced system development.	X		M	M	M

Ergebnisse

Ergebnisse der Arbeit



Github

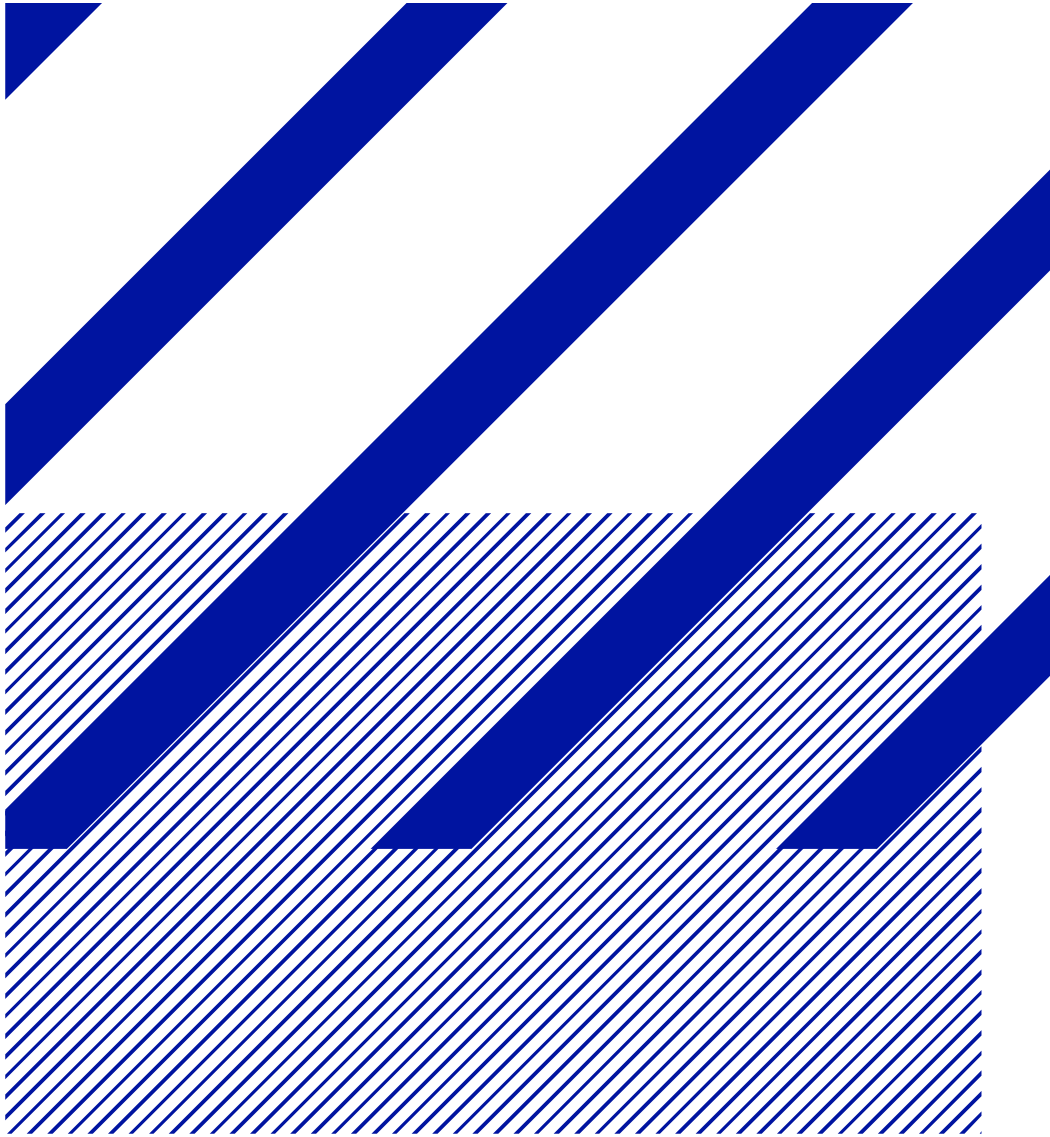
Ergebnisse der Arbeit

FH MÜNSTER
University of Applied Sciences

https://github.com/puQy/OWASP_ISO27k1Mapping

FH MÜNSTER
University of Applied Sciences

Vielen Dank für Ihre Aufmerksamkeit!



Tobias Kappert