ISO/IEC 27001:2013

Thema Änderungen der Kontrollen der ISO/IEC 27001:2013 im Vergleich zur Fassung aus 2005

Datum 20.01.2014

Legende: gering / mittel / hoch

Änderungs-grad	Kapitel	ISO/IEC 27001:2013	Kapitel	ISO/IEC 27001:2005	Änderung in 2013 zu 2005
	A.5	**Information security policies**	**A.5**	**Security policy**	
	A.5.1	**Management direction for information security**	**A.5.1**	**Information security policy**	
	A.5.1.1	Policies for information security	A.5.1.1	Information security policy document	
	A.5.1.2	Review of the policies for information security	A.5.1.2	Review of the information security policy	
	A.6	**Organization of information security**	**A.6**	**Organization of information security**	
	A.6.1	**Internal organization**	**A.6.1**	**Internal organization**	
		Keine Kontrolle	A.6.1.1	Management commitment to information security	entfallen
		Keine Kontrolle	A.6.1.2	Information security co-ordination	entfallen
	A.6.1.1	Information security roles and responsibilities	A.6.1.3	Allocation of information security responsibilities.	
			A.8.1.1	Roles and responsibilities	überführt in A.6.1.1
			A.6.1.4	Authorization process for information processing facilities	entfallen
	A.6.1.2	Segregation of duties	A.10.1.3	Segregation of duties	
	A.6.1.3	Contact with authorities	A.6.1.6	Contact with authorities	
	A.6.1.4	Contact with special interest groups	A.6.1.7	Contact with special interest groups	
	A.6.1.5	Information security in project management		*Keine Kontrolle*	**neu**
	A.6.2	**Mobile devices and teleworking**	**A.11.7**	**Mobile computing and teleworking**	
	A.6.2.1	Mobile device policy	A.11.7.1	Mobile computing and communications	
	A.6.2.2	Teleworking	A.11.7.2	Teleworking	
			A.6.2.1	Identification of risks related to external parties	entfallen
			A.6.2.2	Addressing security when dealing with customers	entfallen
	A.7	**Human resource security**	**A.8**	**Human Resource Security**	
	A.7.1	**Prior to employment**	**A.8.1**	**Prior to employment**	
	A.7.1.1	Screening	A.8.1.2	Screening	
	A.7.1.2	Terms and conditions of employment	A.8.1.3	Terms and conditions of employment	
	A.7.2	**During employment**	**A.8.2**	**During employment**	
	A.7.2.1	Management responsibilities	A.8.2.1	Management responsibilities	
	A.7.2.2	Information security awareness, education and training	A.8.2.2	Information security awareness, education, and training	
	A.7.2.3	Disciplinary process	A.8.2.3	Disciplinary process	
	A.7.3	**Termination and change of employment**	**A.8.3**	**Termination or change of employment**	
	A.7.3.1	Termination or change of employment responsibilities	A.8.3.1	Termination responsibilities	
	A.8	**Asset management**	**A.7**	**Asset Management**	
	A.8.1	**Responsibility for assets**	**A.7.1**	**Responsibility for assets**	
	A.8.1.1	Inventory of assets	A.7.1.1	Inventory of assets	
	A.8.1.2	Ownership of assets	A.7.1.2	Ownership of assets	
	A.8.1.3	Acceptable use of assets	A.7.1.3	Acceptable use of assets	
	A.8.1.4	Return of assets	A.8.3.2	Return of assets	
	A.8.2	**Information classification**	**A.7.2**	**Information classification**	
	A.8.2.1	Classification of information	A.7.2.1	Classification guidelines	
	A.8.2.2	Labelling of information	A.7.2.2	Information labeling and handling	
	A.8.2.3	Handling of assets	A.10.7.3	Information handling procedures	
	A.8.3	**Media handling**	**A.10.7**	**Media handling**	

© 2014 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Änderungs-grad	Kapitel	ISO/IEC 27001:2013	Kapitel	ISO/IEC 27001:2005	Änderung in 2013 zu 2005
	A.8.3.1	Management of removable media	A.10.7.1	Management of removable media	
	A.8.3.2	Disposal of media	A.10.7.2	Disposal of media	
	A.8.3.3	Physical media transfer	A.10.8.3	Physical media in transit	
		Keine Kontrolle	A.10.7.4	Security of system documentation	entfallen
	A.9	**Access control**	**A.11**	**Access control**	
	A.9.1	**Business requirements of access control**	**A.11.1**	**Business requirement for access control**	
	A.9.1.1	Access control policy	A.11.1.1	Access control policy	
	A.9.1.2	Access to networks and network services	A.11.4.1	Policy on use of network services	
	A.9.2	**User access management**	**A.11.2**	**User access management**	
	A.9.2.1	User registration and de-registration	A.11.2.1	User registration	
	A.9.2.2	User access provisioning		*Keine Kontrolle*	**neu**
	A.9.2.3	Management of privileged access rights	A.11.2.2	Privilege management	
	A.9.2.4	Management of secret authentication information of users	A.11.2.3	User password management	
	A.9.2.5	Review of user access rights	A.11.2.4	Review of user access rights	
	A.9.2.6	Removal or adjustment of access rights	A.8.3.3	Removal of access rights	
	A.9.3	**User responsibilities**	**A.11.3**	**User responsibilities**	
	A.9.3.1	Use of secret authentication information	A.11.3.1	Password use	ersetzt
	A.9.4	**System and application access control**	**A.11.5**	**Operating system access control**	
	A.9.4.1	Information access restriction	A.11.6.1	Information access restriction	
	A.9.4.2	Secure log-on procedures	A.11.5.1	Secure log-on procedures	
		Keine Kontrolle	A.11.5.5	Session time-out	überführt in A.9.4.2
		Keine Kontrolle	A.11.5.6	Limitation of connection time	überführt in A.9.4.2
		Keine Kontrolle	A.11.5.2	User identification and authentication	entfallen
	A.9.4.3	Password management system	A.11.5.3	Password management system	
	A.9.4.4	Use of privileged utility programs	A.11.5.4	Use of system utilities	
	A.9.4.5	Access control to program source code	A.12.4.3	Access control to program source code	
		Keine Kontrolle	A.11.6	**Application and information access control**	entfallen
		Keine Kontrolle	A.11.6.2	Sensitive system isolation	entfallen
	A.10	**Cryptography**	**A.12.3**	**Cryptographic controls**	
	A.10.1	**Cryptographic controls**		**Kein Unterkapitel**	**neu**
	A.10.1.1	Policy on the use of cryptographic controls	A.12.3.1	Policy on the use of cryptographic controls	
	A.10.1.2	Key management	A.12.3.2	Key management	
	A.11	**Physical and environmental security**	**A.9**	**Physical and environmental security**	
	A.11.1	**Secure areas**	**A.9.1**	**Secure areas**	
	A.11.1.1	Physical security perimeter	A.9.1.1	Physical security perimeter	
	A.11.1.2	Physical entry controls	A.9.1.2	Physical entry controls	
	A.11.1.3	Securing offices, rooms, and facilities	A.9.1.3	Securing offices, rooms, and facilities	
	A.11.1.4	Protecting against external and environmental threats	A.9.1.4	Protecting against external and environmental threats	
	A.11.1.5	Working in secure areas	A.9.1.5	Working in secure areas	
	A.11.1.6	Delivery and loading areas	A.9.1.6	Public access, delivery, and loading areas	
	A.11.2	**Equipment**	**A.9.2**	**Equipment security**	
	A.11.2.1	Equipment siting and protection	A.9.2.1	Equipment siting and protection	
	A.11.2.2	Supporting utilities	A.9.2.2	Supporting utilities	
	A.11.2.3	Cabling security	A.9.2.3	Cabling security	
	A.11.2.4	Equipment maintenance	A.9.2.4	Equipment maintenance	
	A.11.2.5	Removal of assets	A.9.2.7	Removal of property	
	A.11.2.6	Security of equipment and assets off-premises	A.9.2.5	Security of equipment off-premises	

© 2014 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Änderungs-grad	Kapitel	ISO/IEC 27001:2013	Kapitel	ISO/IEC 27001:2005	Änderung in 2013 zu 2005
	A.11.2.7	Secure disposal or re-use of equipment	A.9.2.6	Secure disposal or re-use of equipment	
	A.11.2.8	Unattended user equipment	A.11.3.2	Unattended user equipment	
	A.11.2.9	Clear desk and clear screen policy	A.11.3.3	Clear desk and clear screen policy	
	A.12	**Operations security**	**A.10**	**Operations Security**	
	A.12.1	**Operational procedures and responsibilities**	**A.10.1**	**Operational procedures and responsibilities**	
	A.12.1.1	Documented operating procedures	A.10.1.1	Documented operating procedures	
	A.12.1.2	Change management	A.10.1.2	Change management	
	A.12.1.3	Capacity management	A.10.3.1	Capacity management	
	A.12.1.4	Separation of development, testing and operational environments	A.10.1.4	Separation of development, test, and operational facilities	
	A.12.2	**Protection from malware**	**A.10.4**	**Protection against malicious and mobile code**	
	A.12.2.1	Controls against malware	A.10.4.1	Controls against malicious code	
			A.10.4.2	Controls against mobile code	überführt in 12.2.1
	A.12.3	**Backup**	**A.10.5**	**Back-up**	
	A.12.3.1	Information backup	A.10.5.1	Information back-up	
	A.12.4	**Logging and monitoring**	**A.10.10**	**Monitoring**	
	A.12.4.1	Event logging	A.10.10.1	Audit logging	
		Keine Kontrolle	A.10.10.2	Monitoring system use	überführt in 12.4.1
	A.12.4.2	Protection of log information	A.10.10.3	Protection of log information	
	A.12.4.3	Administrator and operator logs	A.10.10.4	Administrator and operator logs	
		Keine Kontrolle	A.10.10.5	Fault logging	entfallen
	A.12.4.4	Clock synchronisation	A.10.10.6	Clock synchronization	
	A.12.5	**Control of operational software**		**Kein Unterkapitel**	**neu**
	A.12.5.1	Installation of software on operational systems	A.12.4.1	Control of operational software	
	A.12.6	**Technical vulnerability management**	**A.12.6**	**Technical Vulnerability Management**	
	A.12.6.1	Management of technical vulnerabilities	A.12.6.1	Control of technical vulnerabilities	
	A.12.6.2	Restrictions on software installation		*Keine Kontrolle*	**neu**
	A.12.7	**Information systems audit considerations**	**A.15.3**	**Information systems audit considerations**	
	A.12.7.1	Information systems audit controls	A.15.3.1	Information systems audit controls	
		Keine Kontrolle	A.15.3.2	Protection of information systems audit tools	entfallen
	A.13	**Communications security**	**A.11.4**	**Network access control**	
	A.13.1	**Network security management**	**A.10.6**	**Network security management**	
			A.11.4	**Network access control**	überführt in 13.1
	A.13.1.1	Network controls	A.10.6.1	Network controls	
			A.11.4.2	User authentication for external connections	entfallen
	A.13.1.2	Security of network services	A.10.6.2	Security of network services	
			A.11.4.3	Equipment identification in networks	entfallen
			A.11.4.4	Remote diagnostic and configuration port protection	entfallen
	A.13.1.3	Segregation in networks	A.11.4.5	Segregation in networks	
			A.11.4.6	Network connection control	entfallen
			A.11.4.7	Network routing control	entfallen
	A.13.2	**Information transfer**	**A.10.8**	**Exchange of information**	
	A.13.2.1	Information transfer policies and procedures	A.10.8.1	Information exchange policies and procedures	
	A.13.2.2	Agreements on information transfer	A.10.8.2	Exchange agreements	
	A.13.2.3	Electronic messaging	A.10.8.4	Electronic messaging	
	A.13.2.4	Confidentiality or non-disclosure agreements	A.6.1.5	Confidentiality agreements	
		Keine Kontrolle	A.10.8.5	Business information systems	entfallen

© 2014 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Änderungs-grad	Kapitel	ISO/IEC 27001:2013	Kapitel	ISO/IEC 27001:2005	Änderung in 2013 zu 2005
	A.14	**System acquisition, development and maintenance**	**A.12**	**Information systems acquisition, development and maintenance**	
	A.14.1	**Security requirements of information systems**	**A.12.1**	**Security requirements of information systems**	
	A.14.1.1	Information security requirements analysis and specification	A.12.1.1	Security requirements analysis and specification	
	A.14.1.2	Securing application services on public networks	**A.10.9**	**Electronic commerce services**	
			A.10.9.1	Electronic commerce	überführt in A.14.1.2
			A.10.9.3	Publicly available information	überführt in A.14.1.2
	A.14.1.3	Protecting application services transactions	A.10.9.2	On-Line transactions	
		Keine Kontrolle	**A.12.2**	**Correct processing in applications**	entfallen
		Keine Kontrolle	A.12.2.1	Input data validation	entfallen
		Keine Kontrolle	A.12.2.2	Control of internal processing	entfallen
		Keine Kontrolle	A.12.2.3	Message integrity	entfallen
		Keine Kontrolle	A.12.2.4	Output data validation	entfallen
			A.12.4	Security of system files	überführt in A.14.2
			A.12.4.3	Access control to program source code	überführt in A.14.2
	A.14.2	**Security in development and support processes**	**A.12.5**	**Security in development and support processes**	
	A.14.2.1	Secure development policy		*Keine Kontrolle*	**neu**
	A.14.2.2	System change control procedures	A.12.5.1	Change control procedures	
	A.14.2.3	Technical review of applications after operating platform changes	A.12.5.2	Technical review of applications after operating system changes	
	A.14.2.4	Restrictions on changes to software packages	A.12.5.3	Restrictions on changes to software packages	
		Keine Kontrolle	A.12.5.4	Information leakage	entfallen
	A.14.2.5	Secure system engineering principles		*Keine Kontrolle*	**neu**
	A.14.2.6	Secure development environment		*Keine Kontrolle*	**neu**
	A.14.2.7	Outsourced development	A.12.5.5	Outsourced software development	
	A.14.2.8	System security testing		*Keine Kontrolle*	**neu**
	A.14.2.9	System acceptance testing	A.10.3	**System planning and acceptance**	
			A.10.3.2	System acceptance	überführt in A.14.2.9
	A.14.3	**Test data**		**Kein Unterkapitel**	**neu**
	A.14.3.1	Protection of test data	A.12.4.2	Protection of system test data	
	A.15	**Supplier relationships**	**A.6.2**	**External parties**	
	A.15.1	**Information security in supplier relationships**		**Kein Unterkapitel**	**neu**
	A.15.1.1	Information security policy for supplier relationships	A.6.2.3	Addressing security in third party agreements	aufgeteilt in 15.1.1 und 15.1.2
	A.15.1.2	Addressing security within supplier agreements	A.6.2.3	Addressing security in third party agreements	aufgeteilt in 15.1.1 und 15.1.2
	A.15.1.3	Information and communication technology supply chain		*Keine Kontrolle*	**neu**
	A.15.2	**Supplier service delivery management**	**A.10.2**	**Third party service delivery management**	überführt in 15.2
			A.10.2.1	Service delivery	überführt in 15.2
	A.15.2.1	Monitoring and review of supplier services	A.10.2.2	Monitoring and review of third party services	
	A.15.2.2	Managing changes to supplier services	A.10.2.3	Managing changes to third party services	
	A.16	**Information security incident management**	**A.13**	**Information security incident management**	
	A.16.1	**Management of information security incidents and improvements**	**A.13.2**	**Management of information security incidents and improvements**	
	A.16.1.1	Responsibilities and procedures	A.13.2.1	Responsibilities and procedures	
	A.16.1.2	Reporting information security events	**A.13.1**	**Reporting information security events and weaknesses**	
			A.13.1.1	Reporting information security events	überführt in A.16.1.2

© 2014 Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft

Änderungs-grad	Kapitel	ISO/IEC 27001:2013	Kapitel	ISO/IEC 27001:2005	Änderung in 2013 zu 2005
	A.16.1.3	Reporting information security weaknesses	A.13.1.2	Reporting security weaknesses	
	A.16.1.4	Assessment of and decision on information security events		*Keine Kontrolle*	**neu**
	A.16.1.5	Response to information security incidents		*Keine Kontrolle*	**neu**
	A.16.1.6	Learning from information security incidents	A.13.2.2	Learning from information security incidents	
	A.16.1.7	Collection of evidence	A.13.2.3	Collection of evidence	
	A.17	**Information security aspects of business continuity management**	**A.14**	**Business Continuity Management**	
	A.17.1	**Information security continuity**		**Kein Unterkapitel**	**neu**
		Keine Kontrolle	A.14.1.1	Including information security in the business continuity management process	entfallen
		Keine Kontrolle	A.14.1.3	Developing and implementing continuity plans including information security	entfallen
		Keine Kontrolle	A.14.1.4	Business continuity planning framework	entfallen
	A.17.1.1	Planning information security continuity	A.14.1.2	Business continuity and risk assessment	
	A.17.1.2	Implementing information security continuity		*Keine Kontrolle*	**neu**
	A.17.1.3	Verify, review and evaluate information security continuity	A.14.1.5	Testing, maintaining and re-assessing business continuity plans	
	A.17.2	**Redundancies**		**Kein Unterkapitel**	**neu**
	A.17.2.1	Availability of information processing facilities		*Keine Kontrolle*	**neu**
	A.18	**Compliance**	**A.15**	**Compliance**	
	A.18.1	**Compliance with legal and contractual requirements**	**A.15.1**	**Compliance with legal requirements**	
	A.18.1.1	Identification of applicable legislation and contractual requirements	A.15.1.1	Identification of applicable legislation	
	A.18.1.2	Intellectual property rights	A.15.1.2	Intellectual property rights (IPR)	
	A.18.1.3	Protection of records	A.15.1.3	Protection of organizational records	
	A.18.1.4	Privacy and protection of personally identifiable information	A.15.1.4	Data protection and privacy of personal information	
		Keine Kontrolle	A.15.1.5	Prevention of misuse of information processing facilities	entfallen
	A.18.1.5	Regulation of cryptographic controls	A.15.1.6	Regulation of cryptographic controls	
	A.18.2	**Information security reviews**		**Kein Unterkapitel**	**neu**
	A.18.2.1	Independent review of information security	A.6.1.8	Independent review of information security	
	A.18.2.2	Compliance with security policies and standards	**A.15.2**	**Compliance with security policies and standards, and technical compliance**	
			A.15.2.1	Compliance with security policies and standards	überführt in 18.2.2
	A.18.2.3	Technical compliance review	A.15.2.2	Technical compliance checking	

Deloitte bezieht sich auf Deloitte Touche Tohmatsu Limited, eine „private company limited by guarantee“ (Gesellschaft mit beschränkter Haftung nach britischem Recht), und/oder ihr Netzwerk von Mitgliedsunternehmen. Jedes dieser Mitgliedsunternehmen ist rechtlich selbstständig und unabhängig. Eine detaillierte Beschreibung der rechtlichen Struktur von Deloitte Touche Tohmatsu Limited und ihrer Mitgliedsunternehmen finden Sie auf www.deloitte.com/de/UeberUns.

Diese Veröffentlichung enthält ausschließlich allgemeine Informationen und weder die Deloitte & Touche GmbH Wirtschaftsprüfungsgesellschaft noch Deloitte Touche Tohmatsu Limited („DTTL“), noch eines der Mitgliedsunternehmen von DTTL oder ihre verbundenen Unternehmen (insgesamt das „Deloitte Netzwerk“) erbringen mittels dieser Veröffentlichung professionelle Beratungs- oder Dienstleistungen.