ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A5	**Information security policies**	
A5.1	**Management direction for information security**	
A5.1.1	Policies for information security	Not applicable
A5.1.2	Review of the policies for information security	Not applicable
NOTES	The management of the policies is not defined and not applicable on OWASP, as it is a testing methodology but it can review the policies but strictly being around to its' top 10.	
A6	**Organization of information security**	
A6.1	**Internal organization**	
A6.1.1	Information security roles and responsibilities	Defined
A6.1.2	Segregation of duties	Defined
A6.1.3	Contact with authorities	Not applicable
A6.1.4	Contact with special interest groups	Not applicable
A6.1.5	Information security in project management	Not applicable
NOTES	Defining roles in accordance with the access controls and similarly segregating the duties come under OWASP top 10 however if it based on organizations internal structure than OWASP is not linked.	
A6.2	**Mobile devices and teleworking**	
A6.2.1	Mobile device policy	Not applicable
A6.2.2	Teleworking	Limited
NOTES	The working structure under teleworking can be tested by OWASP under the given set of policies of the organization.	
A7	**Human resource security**	
A7.1	**Prior to employment**	
A7.1.1	Screening	Not applicable
A7.1.2	Terms and conditions of employment	Not applicable
NOTES	This section has no link with the OWASP top 10 principles.	
A7.2	**During employment**	
A7.2.1	Management responsibilities	Not applicable
A7.2.2	Information security awareness, education and training	Defined
A7.2.3	Disciplinary process	Not applicable
NOTES	For the awareness OWASP has proper set of documentation which is officially available online and organization can study and could make policies accordingly.	

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A7.3	**Termination and change of employment**	
A7.3.1	Termination or change of employment responsibilities	Limited
NOTES	The termination of employees or responsibilities has no direct link with the OWASP however, considering the access controls or to sensitive data exposure then OWASP could be linked otherwise has no direct link with this section.	
A8	**Asset management**	
A8.1	**Responsibility for assets**	
A8.1.1	Inventory of assets	Nonexistent
A8.1.2	Ownership of assets	Nonexistent
A8.1.3	Acceptable use of assets	Defined
A8.1.4	Return of assets	Nonexistent
NOTES	OWASP however highlights dealing with using components of known vulnerabilities however there is need to make up the inventory of the assets to reduce their usage and prevent from any further damage if any.	
A8.2	**Information classification**	
A8.2.1	Classification of information	Nonexistent
A8.2.2	Labelling of information	Limited
A8.2.3	Handling of assets	Initial
NOTES	No information classification found in the OWASP however OWASP in monitoring and logging asks to monitor the web applications which can be further enhanced in terms of information classification i.e. confidential, private, public etc. Logging and monitoring by OWASP is mentioned but to very limited scale which can be used for fulfilling this section of OWASP.	
A8.3	**Media handling**	
A8.3.1	Management of removable media	Initial
A8.3.2	Disposal of media	Nonexistent
A8.3.3	Physical media transfer	Nonexistent
NOTES	Media handling w.r.t web applications is an important part which should be described because loss or theft of any media or if dumping of media goes wrong than an organization could suffer severe circumstances and OWASP has no criteria mentioned to handle the media as per the above stated points.	

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A9	**Access control**	
A9.1	**Business requirements of access control**	
A9.1.1	Access control policy	Not applicable
A9.1.2	Access to networks and network services	Defined
NOTES	The policy depends upon the organization and every penetration tester should come with the rules of engagement and disclosure agreements so it does not apply on the OWASP but a basic pre-engagement step for every pen-tester. However, if considering the OWASP checklist documentation it can be seen there are number of experiments fulfilling the criteria for access controls.	
A9.2	**User access management**	
A9.2.1	User registration and de-registration	Managed
A9.2.2	User access provisioning	Managed
A9.2.3	Management of privileged access rights	Managed
A9.2.4	Management of secret authentication information of users	Defined
A9.2.5	Review of user access rights	Defined
A9.2.6	Removal or adjustment of access rights	Defined
NOTES	This section is managed very carefully by OWASP, in the OTG checklist full control is managed in terms of testing this domain.	
A9.3	**User responsibilities**	
A9.3.1	Use of secret authentication information	Defined
NOTES	The secret authentication is defined not directly but testing in terms of session management, cache checks, weak credentials etc. also the testing of authentication indirectly fulfills the secret authentication.	
A9.4	**System and application access control**	
A9.4.1	Information access restriction	Managed
A9.4.2	Secure log-on procedures	Managed
A9.4.3	Password management system	Managed
A9.4.4	Use of privileged utility programs	Defined
A9.4.5	Access control to program source code	Defined
NOTES	The access controls alongside broken authentication is very well managed in the OWSAP, very well list of testing presented in the checklist along with the tools.	
A10	**Cryptography**	
A10.1	**Cryptographic controls**	

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A10.1.1	Policy on the use of cryptographic controls	Not applicable
A10.1.2	Key management	Limited
NOTES	Specifically, key management is not mentioned in the scope of OWASP, however, considering cryptographic approach OWASP checks for encryption standards and also one of the main point of sensitive data exposures describes importance of data. Moreover, insecure deserialization also focusses on the this schema.	
A11	**Physical and environmental security**	
A11.1	**Secure areas**	
A11.1.1	Physical security perimeter	Not applicable
A11.1.2	Physical entry controls	Not applicable
A11.1.3	Securing offices, rooms and facilities	Limited
A11.1.4	Protecting against external and environmental threats	Limited
A11.1.5	Working in secure areas	Not applicable
A11.1.6	Delivery and loading areas	Not applicable
NOTES	OWASP is a testing methodology specifically for web applications and it is about testing the applications based on web or cloud. So, it does not involve any channels to secure physical structure.	
A11.2	**Equipment**	
A11.2.1	Equipment siting and protection	Not applicable
A11.2.2	Supporting utilities	Defined
A11.2.3	Cabling security	Not applicable
A11.2.4	Equipment maintenance	Defined
A11.2.5	Removal of assets	Limited
A11.2.6	Security of equipment and assets off-premises	Limited
A11.2.7	Secure disposal or reuse of equipment	Defined
A11.2.8	Unattended user equipment	Defined
A11.2.9	Clear desk and clear screen policy	Not applicable
NOTES	The OWASP in its sensitive data exposure and components with known vulnerabilities section address some of the issues to not use components or remove any components with known vulnerabilities.	

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A12	**Operations security**	
A12.1	**Operational procedures and responsibilities**	
A12.1.1	Documented operating procedures	Defined
A12.1.2	Change management	Defined
A12.1.3	Capacity management	Not applicable
A12.1.4	Separation of development, testing and operational environments	Not applicable
NOTES	The documentation is the initial phase for any pen-tester however OWASP also provides documentation standards including OTG and OTG checklist also other documentations officially where change management is defined in terms of access controls and authorization part. However, capacity management is not applicable which is to be done between the organizations and therefore OWASP does not provide any support related to it.	
A12.2	**Protection from malware**	
A12.2.1	Controls against malware	Optimized
NOTES	This is the main thing which OWASP is known for so it basically provides all the guidelines in various way defined in OTG/ OTG checklist, which discusses various standards in accordance to protection against malware.	
A12.3	**Backup**	
A12.3.1	Information backup	Limited
NOTES	Backup is not directly defined but however OWASP in various ways targets to backup the files or make them encrypted to ensure confidentiality and integrity.	
A12.3	**Logging and monitoring**	
A12.4.1	Event logging	Defined
A12.4.2	Protection of log information	Defined
A12.4.3	Administrator and operator logs	Defined
A12.4.4	Clock synchronization	Limited
NOTES	OWASP provides in its top 10 section related to insufficient logging and monitoring and shows the importance to manage and protect logs in order to stay safe from an exploits.	
A12.5	**Control of operational software**	
A12.5.1	Installation of software on operational systems	Defined

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
NOTES	The security and misconfiguration section of OWASP deals with the insecure or outdated patches which should be updated or removed and hence any installation depends on such configuration files.	
A12.6	**Technical vulnerability management**	
A12.6.1	Management of technical vulnerabilities	Optimized
A12.6.2	Restrictions on software installation	Managed
NOTES	The management of technical vulnerabilities and proper testing method alongside tools are discussed in the OWASP top 10. The access controls and authorization deals with the restriction part of the software installation.	
A12.7	**Information systems audit considerations**	
A12.7.1	Information systems audit controls	Defined
NOTES	The controls in access controls section of OWASP also authorization deals with the above stated auditing.	
A13	**Communications security**	
A13.1	**Network security management**	
A13.1.1	Network controls	Optimized
A13.1.2	Security of network services	Optimized
A13.1.3	Segregation in networks	Limited
NOTES	The controls along with testing are very well described in the OWASP, access controls and testing of several services on the network like WebDAV, FTP, backend DB server etc. are defined by OWASP also in the OTG checklist. The network segregation is defined as in-directly involving controls of access and services.	
A13.2	**Information transfer**	
A13.2.1	Information transfer policies and procedures	Not applicable
A13.2.2	Agreements on information transfer	Not applicable
A13.2.3	Electronic messaging	Defined
A13.2.4	Confidentiality or nondisclosure agreements	Defined
NOTES	The transfer of information is addressed in terms of encryption and testing of information access, authorization and injection etc.	
A14	**System acquisition, development & maintenance**	
A14.1	**Security requirements of information systems**	
A14.1.1	Information security requirements analysis and specification	Nonexistent
A14.1.2	Securing application services on public networks	Defined
A14.1.3	Protecting application services transactions	Managed

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
NOTES	The need of requirements should be defined in the OWASP which has importance in understanding the infrastructure to work on, also on the other side application services are defined and ways to protect in different formats are very well mentioned in the OTG along with services transactions.	
A14.2	**Security in development and support processes**	
A14.2.1	Secure development policy	Not applicable
A14.2.2	System change control procedures	Optimized
A14.2.3	Technical review of applications after operating platform changes	Managed
A14.2.4	Restrictions on changes to software packages	Managed
A14.2.5	Secure system engineering principles	Not applicable
A14.2.6	Secure Development Environment	Not applicable
A14.2.7	Outsourced development	Not applicable
A14.2.8	System security testing	Defined
A14.2.9	System acceptance testing	Not applicable
NOTES	The OWASP is cloud based methodology to find the vulnerabilities in the web application but to protect provide solutions accordingly but system engineering rules and testing is not application on OWASP as engineering is something different however after the implementation of engineering principles OWASP can test the web based services or applications.	
A14.3	**Test data**	
A14.3.1	Protection of test data	Limited
NOTES	It depends what kind of test data is there if it is in accordance with the OWASP then it can be testing with top 10 rules of OWASP.	
A15	**Supplier relationships**	
A15.1	**Information security in supplier relationships**	
A15.1.1	Information security policy for supplier relationships	Not applicable
A15.1.2	Addressing security within supplier agreements	Not applicable
A15.1.3	ICT supply chain	Not applicable
NOTES	The above section is solely based on the organization and the policies they have with their suppliers.	
A15.2	**Supplier service delivery management**	
A15.2.1	Monitoring and review of supplier services	Not applicable
A15.2.2	Managing changes to supplier services	Not applicable
NOTES	The OWASP has no engagements with these policies as they are organization based.	
A16	**Information security incident management**	
A16.1	**Management of information security incidents & improvements**	

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
A16.1.1	Responsibilities and procedures	Not applicable
A16.1.2	Reporting information security events	Not applicable
A16.1.3	Reporting information security weaknesses	Not applicable
A16.1.4	Assessment of and decision on information security events	Not applicable
A16.1.5	Response to information security incidents	Not applicable
A16.1.6	Learning from information security incidents	Not applicable
A16.1.7	Collection of evidence	Not applicable
NOTES	The incidence response plan is managed by the incident response team, this has no link with the OWASP however, organization should have its' own security team to deal and plan if some incident occurs. Moreover, incidence response team can consider OWASP top 10 to build up the security model.	
A17	**Information security aspects of BCM**	
A17.1	**Information security continuity**	
A17.1.1	Planning information security continuity	Not applicable
A17.1.2	Implementing information security continuity	Not applicable
A17.1.3	Verify, review and evaluate information security continuity	Not applicable
NOTES	Deciding the continuity model is the internal responsibility of the organization but an organizaiton can check OWASP top 10 to make a model but directly OWASP has no link with this part.	
A17.2	**Redundancies**	
A17.2.1	Availability of information processing facilities	Not applicable
NOTES	The business continuity management is to make sure things are available even is breakdown occurs so it is not applicable for OWASP however the internal testing team is responsible for the smooth running of business if any incidence takes place.	
A18	**Compliance**	
A18.1	**Compliance with legal and contractual requirements**	
A18.1.1	Identification of applicable legislation and contractual requirements	Not applicable
A18.1.2	Intellectual property rights	Not applicable
A18.1.3	Protection of records	Defined
A18.1.4	Privacy and protection of personally identifiable information	Defined
A18.1.5	Regulation of cryptographic controls	Limited
NOTES	If considering the testing aspect then OWASP fulfills the protection however if building up the compliance then OWASP has no link with this section.	
A18.2	**Information security reviews**	
A18.2.1	Independent review of information security	Limited
A18.2.2	Compliance with security policies and standards	Not applicable
A18.2.3	Technical compliance review	Not applicable

ISO 27001 Security Controls and OWASP

Section	Information security control	Status
NOTES	The review section for the compliance of the organization is limited because OWASP has to stick with its top 10 rules.	
		114