ISO 27001 Security Controls and PTES

Section	Information security control
A5	**Information security policies**
A5.1	**Management direction for information security**
A5.1.1	Policies for information security
A5.1.2	Review of the policies for information security
NOTES	The management of the policies is not defined and not applicable however the pre-engagement step include rules of engagement and timing metrics etc.
A6	**Organization of information security**
A6.1	**Internal organization**
A6.1.1	Information security roles and responsibilities
A6.1.2	Segregation of duties
A6.1.3	Contact with authorities
A6.1.4	Contact with special interest groups
A6.1.5	Information security in project management
NOTES	PTES does not deal with this section.
A6.2	**Mobile devices and teleworking**
A6.2.1	Mobile device policy
A6.2.2	Teleworking
NOTES	The PTES only involves a little part of testing in terms of Wi-Fi.
A7	**Human resource security**
A7.1	**Prior to employment**
A7.1.1	Screening
A7.1.2	Terms and conditions of employment
NOTES	This section has no link with the PTES technical guidelines.
A7.2	**During employment**
A7.2.1	Management responsibilities
A7.2.2	Information security awareness, education and training
A7.2.3	Disciplinary process
NOTES	For the awareness organizations may refer to PTES technical guidelines.

ISO 27001 Security Controls and PTES

Section	Information security control
A7.3	**Termination and change of employment**
A7.3.1	Termination or change of employment responsibilities
NOTES	There is no policy or any principle under this section.
A8	**Asset management**
A8.1	**Responsibility for assets**
A8.1.1	Inventory of assets
A8.1.2	Ownership of assets
A8.1.3	Acceptable use of assets
A8.1.4	Return of assets
NOTES	The PTES should have asset management but although it is not present in PTES.
A8.2	**Information classification**
A8.2.1	Classification of information
A8.2.2	Labelling of information
A8.2.3	Handling of assets
NOTES	PTES does not classify any information however, there are tools which can dig the websites and harvest the important information from the network.
A8.3	**Media handling**
A8.3.1	Management of removable media
A8.3.2	Disposal of media
A8.3.3	Physical media transfer
NOTES	PTES does not include any documentation regarding physical medium issues.
A9	**Access control**

ISO 27001 Security Controls and PTES

Section	Information security control
A9.1	**Business requirements of access control**
A9.1.1	Access control policy
A9.1.2	Access to networks and network services
NOTES	There is no policy however there are range of tools mentioned by PTES to test the networks and services.
A9.2	**User access management**
A9.2.1	User registration and de-registration
A9.2.2	User access provisioning
A9.2.3	Management of privileged access rights
A9.2.4	Management of secret authentication information of users
A9.2.5	Review of user access rights
A9.2.6	Removal or adjustment of access rights
NOTES	Removal or adjustment of access rights are not provided by PTES however through intelligence gathering section several tools can be used which will provide many useful information.
A9.3	**User responsibilities**
A9.3.1	Use of secret authentication information
NOTES	To prevent the above situation, PTES provides ability to test the network by brute forcing or sniffing using tools like Wireshark etc. moreover, running vulnerability scanners can provide more vulnerabilities related to authentication issues.
A9.4	**System and application access control**
A9.4.1	Information access restriction
A9.4.2	Secure log-on procedures
A9.4.3	Password management system
A9.4.4	Use of privileged utility programs
A9.4.5	Access control to program source code
NOTES	There is no clause to implement restriction, however after vulnerability assessment one can know how to secure the above stated information.
A10	**Cryptography**
A10.1	**Cryptographic controls**

ISO 27001 Security Controls and PTES

Section	Information security control
A10.1.1	Policy on the use of cryptographic controls
A10.1.2	Key management
NOTES	PTES can address these issues as mentioned online in key distribution attack section but there is no well defined explanation for this section.
A11	**Physical and environmental security**
A11.1	**Secure areas**
A11.1.1	Physical security perimeter
A11.1.2	Physical entry controls
A11.1.3	Securing offices, rooms and facilities
A11.1.4	Protecting against external and environmental threats
A11.1.5	Working in secure areas
A11.1.6	Delivery and loading areas
NOTES	PTES has no set of rules to deal with the physical and environmental section.
A11.2	**Equipment**
A11.2.1	Equipment siting and protection
A11.2.2	Supporting utilities
A11.2.3	Cabling security
A11.2.4	Equipment maintenance
A11.2.5	Removal of assets
A11.2.6	Security of equipment and assets off-premises
A11.2.7	Secure disposal or reuse of equipment
A11.2.8	Unattended user equipment
A11.2.9	Clear desk and clear screen policy
NOTES	The PTES framework does not cover this section.

ISO 27001 Security Controls and PTES

Section	Information security control
A12	**Operations security**
A12.1	**Operational procedures and responsibilities**
A12.1.1	Documented operating procedures
A12.1.2	Change management
A12.1.3	Capacity management
A12.1.4	Separation of development, testing and operational environments
A12.2	**Protection from malware**
A12.2.1	Controls against malware
A12.3	**Backup**
A12.3.1	Information backup
A12.3	**Logging and monitoring**
A12.4.1	Event logging
A12.4.2	Protection of log information
A12.4.3	Administrator and operator logs
A12.4.4	Clock synchronization
A12.5	**Control of operational software**
A12.5.1	Installation of software on operational systems
A12.6	**Technical vulnerability management**
A12.6.1	Management of technical vulnerabilities
A12.6.2	Restrictions on software installation
A12.7	**Information systems audit considerations**
A12.7.1	Information systems audit controls
NOTES	In the above section A-12; the PTES deals in accordance to protect system form malwares through testing process and also to check whether the vulnerabilities could be exploitable or not through exploitation process.
A13	**Communications security**

ISO 27001 Security Controls and PTES

Section	Information security control
A13.1	**Network security management**
A13.1.1	Network controls
A13.1.2	Security of network services
A13.1.3	Segregation in networks
A13.2	**Information transfer**
A13.2.1	Information transfer policies and procedures
A13.2.2	Agreements on information transfer
A13.2.3	Electronic messaging
A13.2.4	Confidentiality or nondisclosure agreements
NOTES	In section A-13; network issues are addressed through scanning the vulnerabilities using openVas, Nessus, neXpose etc. and after finding vulnerabilities checking for the exploits. The section 4 of PTES deals with exploitation.
A14	**System acquisition, development & maintenance**
A14.1	**Security requirements of information systems**
A14.1.1	Information security requirements analysis and specification
A14.1.2	Securing application services on public networks
A14.1.3	Protecting application services transactions
A14.2	**Security in development and support processes**
A14.2.1	Secure development policy
A14.2.2	System change control procedures
A14.2.3	Technical review of applications after operating platform changes
A14.2.4	Restrictions on changes to software packages
A14.2.5	Secure system engineering principles
A14.2.6	Secure Development Environment
A14.2.7	Outsourced development
A14.2.8	System security testing
A14.2.9	System acceptance testing
A14.3	**Test data**
A14.3.1	Protection of test data

ISO 27001 Security Controls and PTES

Section	Information security control
NOTES	Section A-14; the main aim of securing services can be achieved by implementing PTES principles of gathering information, scanning for vulnerabilities and exploiting vulnerabilities if needed. However, no information is provided for restriction, or outsourcing etc. But can be achieved after scanning for vulnerabilities in the network.
A15	**Supplier relationships**
A15.1	**Information security in supplier relationships**
A15.1.1	Information security policy for supplier relationships
A15.1.2	Addressing security within supplier agreements
A15.1.3	ICT supply chain
A15.2	**Supplier service delivery management**
A15.2.1	Monitoring and review of supplier services
A15.2.2	Managing changes to supplier services
NOTES	There are no details for supplier relationships (A15) in PTES.
A16	**Information security incident management**
A16.1	**Management of information security incidents & improvements**
A16.1.1	Responsibilities and procedures
A16.1.2	Reporting information security events
A16.1.3	Reporting information security weaknesses
A16.1.4	Assessment of and decision on information security events
A16.1.5	Response to information security incidents
A16.1.6	Learning from information security incidents
A16.1.7	Collection of evidence
NOTES	The incidence response plan is managed by the incident response team, this has no link with the PTES however, organization should have its' own security team to deal and plan if some incident occurs.
A17	**Information security aspects of BCM**
A17.1	**Information security continuity**
A17.1.1	Planning information security continuity
A17.1.2	Implementing information security continuity
A17.1.3	Verify, review and evaluate information security continuity
A17.2	**Redundancies**
A17.2.1	Availability of information processing facilities

ISO 27001 Security Controls and PTES

Section	Information security control
NOTES	Section A17; The business continuity management is to make sure things are available even is breakdown occurs and deciding the continuity model is the internal responsibility of the organization.
A18	**Compliance**
A18.1	**Compliance with legal and contractual requirements**
A18.1.1	Identification of applicable legislation and contractual requirements
A18.1.2	Intellectual property rights
A18.1.3	Protection of records
A18.1.4	Privacy and protection of personally identifiable information
A18.1.5	Regulation of cryptographic controls
NOTES	If considering the testing aspect then PTES fulfills the protection however if building up the compliance then PTES has no link with this section.
A18.2	**Information security reviews**
A18.2.1	Independent review of information security
A18.2.2	Compliance with security policies and standards
A18.2.3	Technical compliance review
NOTES	Section A18; PTES is a procedure of implementing the vulnerability scan and the penetration test. So, there are many possibilities that this might not directly link to compliance but however the end approach is to protect the data.