ISPME - ISO 27002:2013 Policy Mapping Table

The following table illustrates how specific control objectives outlined in ISO 27002:2013[1] are addressed by sample security policies within Information Security Policies Made Easy and the Information Shield Common Policy Library (CPL).

ISO Category Control Objectives	ISPME/CPL Sample Policy Document
4 Risk Assessment	**IT Risk Assessment Policy**
5 Information security policies 5.1 Management direction for information security	**Information Security Program Policy**
6 Organization of information security 6.1 Internal organization 6.2 Mobile devices and teleworking	**Information Security Organization Policy** **Mobile Computing Security Policy**
7 Human resource security 7.1 Prior to employment 7.2 During employment 7.3 Termination and change of employment	**Personnel Security Management Policy** **Security Awareness and Training Policy**
8 Asset management **8.1 Responsibility for assets** 8.1.3 Acceptable use of assets 8.1.4 Return of assets	**Asset Management Policy** **Acceptable Use of Assets Policy** **Information Ownership Policy**
8.2 Information classification	**Information Classification Policy**
8.3 Media handling 8.3.2 Disposal of media	**Media Handling Security Policy** **Information Disposal Policy**
9 Access control **9.1 Business requirements of access control** **9.4 System and application access control**	**Access Control Policy**
9.2 User access management **(registration, provisioning and review)**	**Account and Privilege Management Policy**
9.3 User responsibilities	**Acceptable Use of Assets Policy**
10 Cryptography **10.1 Cryptographic controls**	**Encryption and Key Management Policy**

11 Physical and environmental security 11.1 Secure areas	**Physical Security Policy**
11.2 Equipment Security 11.2.2 Supporting utilities 11.2.3 Cabling security	**Physical Security Policy**
11.2.8 Unattended user equipment 11.2.9 Clear desk and clear screen policy	**Acceptable Use of Assets**
12 Operations security 12.1 Operational procedures and responsibilities 12.1.2 Change management	**Change Management Policy**
12.2 Protection from malware	**Malicious Software Management Policy**
12.3 Backup	**Backup and Recovery Policy**
12.4 Logging and monitoring	**Log Management and Monitoring Policy**
12.5 Control of operational software 12.6 Technical vulnerability management	**System Configuration Management Policy**
12.7 Information systems audit considerations	**Audit and Compliance Assessment Policy**
13 Communications security 13.1 Network security management	**Network Security Management Policy**
13.2 Information transfer	**Information Exchange Policy**
14 System acquisition, development and maintenance 14.1 Security requirements of information systems 14.2 Security in development and support processes 14.3 Test data	**Application Development Security Policy**
15 Supplier relationships 15.1 Information security in supplier relationships 15.2 Supplier service delivery management	**Third Party Security Management Policy**
16 Information security incident management 16.1 Management of information security incidents and improvements	**Incident Reporting and Response Policy**
17 Information security aspects of business continuity management 17.1 Information security continuity 17.2 Redundancies	**IT Business Continuity Policy**

18 Compliance 18.1 Compliance with legal and contractual requirements 18.1.2 Intellectual property Rights	**Information Security Program Policy**
18.1.4 Privacy and protection of personally identifiable information	**Customer Data Privacy Management Policy**
18.2 Information security reviews	**Audit and Compliance Assessment Policy**

References:

[1] ISO/IEC 27002:2013 – Code of practice for information security management 2013 Update. Published by ISO and available at BSI [http://www.bsi-global.org/]