7.3.2 Standards

7.3.2.1 ISO17799-2005 rating

Rate each item as **Poor**, **Fair**, or **Good** indicating the extent to which compliance is observed under “Rate”. Ratings are usually done as part of an information protection posture assessment. Identify goals for the program under “Goal”. For areas with sub-areas (indicated in blue) rate them by adding 0 for poor, 1 for fair, and 2 for good for each sub-area they encompass. Do final calculations for your ISO17799-2005 rating as indicated at the end by summing areas and generating a final value.

7.3.2.1.1 Risk assessment and treatment

Area	*Rate*	*Goal*
4 - Risk assessment and treatment		
4.1 Assessing security risks		
4.2 Treating security risks		
Total (sum columns and divide by 2)		

7.3.2.1.2 Security policy

Area	*Rate*	*Goal*
5 Security policy		
5.1 Information security policy		
5.1.1 Information security policy document		
5.1.2 Review of the information security policy		
Total (sum columns and divide by 2)		

7.3.2.1.3 Organization of information security

Area	*Rate*	*Goal*
6 - Organization of information security		
6.1 Internal organization		
6.1.1 Management commitment in information security		
6.1.2 Information security coordination		
6.1.3 Allocation of information security responsibilities		
6.1.4 Authorization process for information processing facilities		
6.1.5 Confidentiality agreements		
6.1.6 Contact with authorities		

Area	Rate	Goal
6.1.7 Contact with special interest groups		
6.1.8 Independent review of information security		
6.2 External parties		
6.2.1 Identification of risks related to external parties		
6.2.2 Addressing security when dealing with customers		
6.2.3 Addressing security in third party agreements		
Total (sum columns and divide by 2)		

7.3.2.1.4 Asset management

Area	Rate	Goal
7 - Asset management		
7.1 Responsibility for assets		
7.1.1 Inventory of assets		
7.1.2 Ownership of assets		
7.1.3 Acceptable use of assets		
7.2 Information classification		
7.2.1 Classification guidelines		
7.2.2 Information labeling and handling		
Total (sum columns and divide by 2)		

7.3.2.1.5 Human resources security

Area	Rate	Goal
8 - Human resources security		
8.1 Prior to employment		
8.1.1 Roles and responsibilities		
8.1.2 Screening		
8.1.3 Terms and conditions of employment		
8.2 During employment		
8.2.1 Management		
8.2.2 Information security education, awareness, and training		
8.2.3 Disciplinary process		
8.3 Termination or change of employment		
8.3.1 Termination responsibility		

Area	Rate	Goal
8.3.2 Return of assets		
8.3.3 Removal of access rights		
Total (sum columns and divide by 3)		

7.3.2.1.6 Physical and environmental security

Area	Rate	Goal
9 - Physical and environmental security		
9.1 Secure areas		
9.1.1 Physical security perimeter		
9.1.2 Physical entry controls		
9.1.3 Securing offices, rooms, and facilities		
9.1.4 Protecting against external and environmental threats		
9.1.5 Working in secure areas		
9.1.6 Public access, delivery, and loading areas		
9.2 Equipment security		
9.2.1 Equipment siting and protection		
9.2.2 Supporting utilities		
9.2.3 Cabling security		
9.2.4 Equipment maintenance		
9.2.5 Security of equipment off-premises		
9.2.6 Secure disposal or reuse of equipment		
9.2.7 Removal of property		
Total (sum columns and divide by 2)		

7.3.2.1.7 Communications and operations management

Area	Rate	Goal
10 - Communications and operations management		
10.1 Operational procedures and responsibilities		
10.1.1 Documented operating procedures		
10.1.2 Change management		
10.1.3 Segregation of duties		
10.1.4 Separation of development, test, and operating facilities		
10.2 Third party service delivery management		

Area	Rate	Goal
10.2.1 Service delivery		
10.2.2 Monitoring and review of third party services		
10.2.3 Managing changes to third party services		
10.3 System planning and acceptance		
10.3.1 Capacity management		
10.3.2 System acceptance		
10.4 Protection against malicious and mobile code		
10.4.1 Controls against malicious code		
10.4.2 Controls against mobile code		
10.5 Backup		
10.5.1 Information backup		
10.6 Network security management		
10.6.1 Network controls		
10.6.2 Security of network services		
10.7 Media handling		
10.7.1 Management of removable media		
10.7.2 Disposal of media		
10.7.3 Information handling procedures		
10.7.4 Security of system documentation		
10.8 Exchange of information		
10.8.1 Information exchange policies and procedures		
10.8.2 Exchange agreements		
10.8.3 Physical media in transit		
10.8.4 Electronic messaging		
10.8.5 Business information systems		
10.9 Electronic commerce services		
10.9.1 Electronic commerce		
10.9.2 On-0line transactions		
10.9.3 Publicly available information		
10.10 Monitoring		
10.10.1 Audit logging		
10.10.2 Monitoring system use		
10.10.3 Protection of log information		

Area	Rate	Goal
10.10.4 Administrator and operator logs		
10.10.5 Fault logging		
10.10.6 Clock synchronization		
Total (sum columns and divide by 10)		

7.3.2.1.8 Access control

Area	Rate	Goal
11 - Access control		
11.1 Business requirement for access control		
11.1.1 Access control policy		
11.2 User access management		
11.2.1 User registration		
11.2.2 Privilege management		
11.2.3 User password management		
11.2.4 Review of user access rights		
11.3 User responsibilities		
11.3.1 Password use		
11.3.2 Unattended user equipment		
11.3.3 Clear desk and clear screen policy		
11.4 Network access control		
11.4.1 Policy on use of network services		
11.4.2 User authentication for external connections		
11.4.3 Equipment identification in networks		
11.4.4 Remote diagnostic and configuration port protection		
11.4.5 Segregation in networks		
11.4.6 Network connection control		
11.4.7 Network routing control		
11.5 Operating system access control		
11.5.1 Server login control		
11.5.2 User identification and authenticaiton		
11.5.3 Password management system		
11.5.4 Use of system utilities		
11.5.5 Session time-out		

Area	Rate	Goal
11.5.6 Limitation of connection time		
11.6 Application and information access control		
11.6.1 Information access restriction		
11.6.2 Sensitive system isolation		
11.7 Mobile computing and teleworking		
11.7.1 Mobile computing and communications		
11.7.2 Teleworking		
Total (sum columns and divide by 11)		

7.3.2.1.9 Information system acquisition, development, and maintenance

Area	Rate	Goal
12 Information system acquisition, development, and maintenance		
12.1 Security requirements of information systems		
12.1.1 Security requirements analysis and specification		
12.2 Correct processing in applications		
12.2.1 Input data validation		
12.2.2 Control of internal processing		
12.2.3 Message integrity		
12.2.4 Output data validation		
12.3 Cryptographic controls		
12.3.1 Policy on the use of cryptographic controls		
12.3.2 Key management		
12.4 Security of system files		
12.4.1 Control of operational software		
12.4.2 Protection of system test data		
12.4.3 Access control to program source code		
12.5 Security in development and support processes		
12.5.1 Change control procedures		
12.5.2 Technical review of application after system changes		
12.5.3 Restrictions on changes to software packages		
12.5.4 Information leakage		
12.5.5 Outsourced software development		
12.6 Technical vulnerability management		

Area	Rate	Goal
12.6.1 Control of technical vulnerabilities		
Total (sum columns and divide by 6)		

7.3.2.1.10 Information security incident management

Area	Rate	Goal
13 Information security incident management		
13.1 Reporting information security events and weaknesses		
13.1.1 Reporting information security events		
13.1.2 Reporting information security weaknesses		
13.2 Management of security incidents and improvements		
12.2.1 Responsibilities and procedures		
13.2.2 Learning from information security incidents		
13.2.3 Collection of evidence		
Total (sum columns and divide by 2)		

7.3.2.1.11 Business continuity management

Area	Rate	Goal
14 Business continuity management (BCM)		
14.1 Information security aspects of BCM		
14.1.1 Including information security in the BCM process		
14.1.2 Business continuity and risk management		
14.1.3 Developing and implementing BCPs with information security		
14.1.4 Business continuity planning framework		
14.1.5 Testing, maintaining & re-assessing business continuity plans		
Total (sum columns)		

7.3.2.1.12 Compliance

Area	Rate	Goal
15 Compliance		
15.1 Compliance with legal requirements		
15.1.1 Identification of applicable legislation		
15.1.2 Intellectual property rights (IPR)		
15.1.3 Protection of organizational records		
15.1.4 Data protection and privacy of personal information		

Area	Rate	Goal
15.1.5 Prevention of misuse of information processing facilities		
15.1.6 Regulation of cryptographic controls		
15.2 Compliance with policies, standards, and technical compliance		
15.2.1 Compliance with security policy		
15.2.2 Technical compliance checking		
15.3 Information security audit controls		
15.3.1 Information system audit controls		
15.3.2 Protection of system audit tools		
Total (sum columns and divide by 3)		

7.3.2.1.13 ISO 17799-2005 roll-up

Area	Rate	Goal
TOTAL for 4: Risk assessment and treatment		
TOTAL for 5: Security Policy		
TOTAL for 6: Organization of information security		
TOTAL for 7: Asset management		
TOTAL for 8: Human resources security		
TOTAL for 9: Physical and environmental security		
TOTAL for 10: Communications and operations management		
TOTAL for 11: Access control		
TOTAL for 12: System acquisition, development, and maintenance		
TOTAL for 13: Incident management		
TOTAL for 14: Business continuity management		
TOTAL for 15: Compliance		
Grand total (sum the totals and divide by 12)		

Due diligence, startup programs with no historical program, common ratings for programs that have been underway for a few years, and mature program levels for each of the areas of ISO 17799 are provided here. They are reasonable as a guide to understanding your ratings and working toward reasonable and attainable goals over time.

Area	*Diligent*	*Startup*	*Typical*	*Excel*	*Best*
4 - Risk assessment and treatment	5	1	3	7	10
5 - Security Policy	5	3	7.5	9	10
6 - Organization of information security	5	0	7.5	8	10
7 - Asset management	5	1	5	7	10
8 - Human resources security	5	3	6.5	8	9
9 - Physical and environmental	5	1	6.2	8	9
10 - Communications and operations	5	2	6.4	7	9
11 - Access control	5	2	6.9	8	9
12 - System acquisition, develop, maintain	5	2	6	8	9
13 - Incident management	5	2	4	6	9
14 - Business continuity management	5	2	9	10	10
15 - Compliance	5	2	6.4	8	9
Total / 12	5	1.75	6.2	7.83	9.4

Due diligence levels indicate at least a Fair in every area. Startup ratings are really not acceptable in the areas covered by ISO 17799. Startup ratings are often low because many elements of the protection process were never considered and the areas where they are considered are out of business necessity in response to events or based on general sensibilities of owners and managers, not as a result of some sort of a plan. From startup to diligent level typically takes 18 months of concerted effort. Programs reach the typical level in 3-5 years by selectively going beyond the diligent level in areas they consider important. Programs that reach the excellent level typically get there as a result of systemic programs over periods of 5 or more years.

ISO 17799-2005 is a new standard, however, it is closely related to its previous version - ISO17799 and as such the ratings provided are reasonably reflective of the standard as it exists today.