ISO 27002:2013 Version Change Summary

This table highlights the control category changes between ISO 27002:2005 and the 2013 update. Changes are color coded.

### Control Category Change Key
- **Control Removed**
- **Control Moved or Renamed**
- **Control Added (new outline)**

### Change Map Key
- **Minimum Changes to Domain**
- **Several key changes to Domain**
- **Major changes to Domain**

<table>
<thead>
<tr>
<th>Change</th>
<th>2005 Control Category</th>
<th>2013 Control Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOW</td>
<td>5 SECURITY POLICY</td>
<td>5 INFORMATION SECURITY POLICIES</td>
</tr>
<tr>
<td></td>
<td>5.1 INFORMATION SECURITY POLICY</td>
<td>5.1 Management direction for information security</td>
</tr>
<tr>
<td></td>
<td>5.1.1 Information security policy document</td>
<td>5.1.1 Policies for information security</td>
</tr>
<tr>
<td></td>
<td>5.1.2 Review of the information security policy</td>
<td>5.1.2 Review of the policies for information security</td>
</tr>
<tr>
<td>MED</td>
<td>6 ORGANIZATION OF INFORMATION SECURITY</td>
<td>6 ORGANIZATION OF INFORMATION SECURITY</td>
</tr>
<tr>
<td></td>
<td>6.1 INTERNAL ORGANIZATION</td>
<td>6.1 Internal organization</td>
</tr>
<tr>
<td></td>
<td>6.1.1 Management commitment to information security (Removed)</td>
<td>6.1.1 Information security roles and responsibilities</td>
</tr>
<tr>
<td></td>
<td>6.1.2 Information security co-ordination (removed)</td>
<td>6.1.2 Segregation of duties (Moved)</td>
</tr>
<tr>
<td></td>
<td>6.1.3 Allocation of information security responsibilities.</td>
<td>6.1.3 Contact with authorities</td>
</tr>
<tr>
<td></td>
<td>10.1.3 Segregation of duties (moved)</td>
<td>6.1.4 Contact with special interest groups</td>
</tr>
<tr>
<td></td>
<td>6.1.6 Contact with authorities</td>
<td>6.1.5 Information security in project management (New)</td>
</tr>
<tr>
<td></td>
<td>6.1.7 Contact with special interest groups</td>
<td></td>
</tr>
</tbody>
</table>
11.7 MOBILE COMPUTING AND TELEWORKING (Moved)
11.7.1 Mobile computing and communications
11.7.2 Teleworking

6.2 Mobile devices and teleworking
6.2.1 Mobile device policy
6.2.2 Teleworking

8 Human Resource Security
8.1 PRIOR TO EMPLOYMENT
8.1.2 Screening
8.1.3 Terms and conditions of employment
8.2 DURING EMPLOYMENT
8.2.1 Management responsibilities
8.2.2 Information security awareness, education, and training
8.2.3 Disciplinary process
8.3 TERMINATION OR CHANGE OF EMPLOYMENT
8.3.1 Termination responsibilities

7 Human Resource Security
7.1 Prior to employment
7.1.2 Terms and conditions of employment
7.2 During employment
7.2.1 Management responsibilities
7.2.2 Information security awareness, education and training
7.2.3 Disciplinary process
7.3 Termination and change of employment
7.3.1 Termination or change of employment responsibilities

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
8.3.2 Return of assets (moved)

7.2 INFORMATION CLASSIFICATION
7.2.1 Classification guidelines
7.2.2 Information labeling and handling

10.7 MEDIA HANDLING (Moved)
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 (Removed)
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 (moved)
11.2.4 Review of user access rights

8.3.3 Removal of access rights (Moved)

11.3 USER RESPONSIBILITIES
11.3.1 Password use.

11.5 OPERATING SYSTEM ACCESS CONTROL
11.6.1 Information access restriction
11.5.1 Secure log-on procedures
11.5.2 User identification and authentication
11.5.3 Password management system
11.5.4 Use of system utilities
12.4.3 Access control to program source code (moved)

11.5.5 Session time-out (Removed)
11.5.6 Limitation of connection time

11.6 APPLICATION AND INFORMATION ACCESS CONTROL
11.6.2 Sensitive system isolation

12.3 CRYPTOGRAPHIC CONTROLS
12.3.1 Policy on the use of cryptographic controls
12.3.2 Key management

9 PHYSICAL AND ENVIRONMENTAL SECURITY
9.1 SECURE AREAS

10 Cryptography (NEW)
10.1.1 Policy on the use of cryptographic controls
10.1.2 Key management

11 PHYSICAL AND ENVIRONMENTAL SECURITY
11.1 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
9.2.7 Removal of property (Moved)
9.2.5 Security of equipment off-premises

9.3.2 Unattended user equipment (Moved)
9.3.3 Clear desk and clear screen policy (Moved)

10. OPERATIONS SECURITY
10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES
10.1.1 Documented operating procedures
10.1.2 Change management
10.3.1 Capacity management
10.1.4 Separation of development, test, and operational facilities

10.3 SYSTEM PLANNING AND ACCEPTANCE.
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 (combined)

10.5 BACK-UP
10.5.1 Information back-up

10.10 MONITORING
10.10.1 Audit logging

11.1.1 Physical security perimeter
11.1.2 Physical entry controls
11.1.3 Securing offices, rooms and facilities
11.1.4 Protecting against external and environmental threats
11.1.5 Working in secure areas
11.1.6 Delivery and loading areas

11.2 Equipment
11.2.1 Equipment siting and protection
11.2.2 Supporting utilities
11.2.3 Cabling security
11.2.4 Equipment maintenance
11.2.5 Removal of assets (moved)
11.2.6 Security of equipment and assets off premises
11.2.7 Secure disposal or re-use of equipment
11.2.8 Unattended user equipment
11.2.9 Clear desk and clear screen policy

12 OPERATIONS SECURITY
12.1 Operational procedures and responsibilities
12.1.1 Documented operating procedures
12.1.2 Change management
12.1.3 Capacity management

12.2 Protection from malware
12.2.1 Controls against mal-Ware

12.3 Backup
12.3.1 Information backup

12.4 Logging and monitoring
12.4.1 Event logging
10.10.2 Monitoring system use (combined)
10.10.3 Protection of log information
10.10.4 Administrator and operator logs
10.10.5 Fault logging (Removed)
10.10.6 Clock synchronization

12.4 SECURITY OF SYSTEM FILES
12.4.1 Control of operational software

12.6 TECHNICAL VULNERABILITY MANAGEMENT
12.6.1 Control of technical vulnerabilities

15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS (Moved)
15.3.1 Information systems audit controls
15.3.2 Protection of information systems audit tools

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

10.8 EXCHANGE OF INFORMATION (Moved)
10.8.1 Information exchange policies and procedures
10.8.2 Exchange agreements
10.8.3 Physical media in transit (removed)
10.8.4 Electronic messaging
10.8.5 Business information systems (removed)

12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE
12.1 SECURITY REQUIREMENTS OF INFORMATION SYSTEMS

12.5 Control of operational software
12.5.1 Installation of soft-ware on operational systems

12.6 Technical vulnerability management
12.6.1 Management of technical vulnerabilities
12.6.2 Restrictions on software installation

12.7 Information systems audit considerations
12.7.1 Information systems audit controls

13 Communications security
13.1 Network security management
13.1.1 Network controls
13.1.2 Security of network services
13.1.3 Segregation in networks

13.2 Information transfer
13.2.1 Information transfer policies and procedures
13.2.2 Agreements on information transfer
13.2.3 Electronic messaging
13.2.4 Confidentiality or non-disclosure agreements

14 System acquisition, development and maintenance
14.1 Security requirements of information systems
12.1.1 Security requirements analysis and specification
12.2 CORRECT PROCESSING IN APPLICATIONS (Removed)
12.2.1 Input data validation
12.2.2 Control of internal processing
12.2.3 Message integrity
12.2.4 Output data validation
12.4 SECURITY OF SYSTEM FILES (Moved)
12.4.1 Control of operational software
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 applications after operating system changes
12.5.3 Restrictions on changes to software packages
12.5.4 Information leakage (Removed)
12.5.5 Outsourced software development

12.4.2 Protection of system test data

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

10.2 THIRD PARTY SERVICE DELIVERY MANAGEMENT
10.2.1 Service delivery
10.2.2 Monitoring and review of third party services
10.2.3 Managing changes to third party services

13 INFORMATION SECURITY INCIDENT MANAGEMENT

14.1.1 Information security requirements analysis and specification
14.1.2 Securing application services on public networks
14.1.3 Protecting application services transactions

14.2 Security in development and support processes
14.2.1 Secure development policy
14.2.2 System change control procedures
14.2.3 Technical review of applications after operating platform changes
14.2.4 Restrictions on changes to software packages
14.2.5 Secure system engineering principles
14.2.6 Secure development environment
14.2.7 Outsourced development
14.2.8 System security testing
14.2.9 System acceptance testing
14.3 Test data (New)
14.3.1 Protection of test data

15 Supplier relationships
15.1 Information security in supplier relationships
15.1.1 Information security policy for supplier relationships
15.1.2 Addressing security within supplier agreements
15.1.3 Information and communication technology supply chain (New)
15.2 Supplier service delivery management
15.2.1 Monitoring and review of supplier services
15.2.2 Managing changes to supplier services
13.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

13.2.1 Responsibilities and procedures
13.1.1 Reporting information security events
13.1.2 Reporting security weaknesses

13.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES.

13.2.2 Learning from information security incidents
13.2.3 Collection of evidence

14 BUSINESS CONTINUITY MANAGEMENT

14.1 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT
14.1.1 Including information security in the business continuity management process
14.1.2 Business continuity and risk assessment
14.1.3 Developing and implementing continuity plans including information security
14.1.4 Business continuity planning framework
14.1.5 Testing, maintaining and re-assessing business continuity plans

17 INFORMATION SECURITY ASPECTS OF BUSINESS CONTINUITY MANAGEMENT

17.1 Information security aspects of business continuity management
17.1.1 Planning information security continuity
17.1.2 Implementing information security continuity
17.1.3 Verify, review and evaluate information security continuity
17.2 Redundancies (new)
17.2.1 Availability of information processing facilities

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
15.1.5 Prevention of misuse of information processing facilities (Removed)
15.1.6 Regulation of cryptographic controls

15.2 COMPLIANCE WITH SECURITY POLICIES AND STANDARDS, AND TECHNICAL COMPLIANCE

15.2.1 Compliance with legal and contractual requirements
15.2.2 Identification of applicable legislation and contractual requirements
15.2.3 Intellectual property Rights
15.2.4 Protection of records
15.2.5 Privacy and protection of personally identifiable information
15.2.6 Regulation of cryptographic controls
15.2.7 Information security reviews (New)
6.1.8 Independent review of information security (moved)
15.2.1 Compliance with security policies and standards.
15.2.2 Technical compliance checking

18.2.1 Independent review of information security
18.2.2 Compliance with security policies and standards
18.2.3 Technical compliance review