



Information Shield NIST/FISMA Policy Mapping Table

The following table illustrates how the policy categories of ISO 27002 ^[4] (PolicyShield) map to the 17 specific high-level control requirements outlined in NIST Special Publication NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. ^[1]

Specific Control Objectives and Techniques	ISO Category
Management Controls	Management controls focus on the management of the IT security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.
1. Risk Assessment (RA) <i>Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.</i>	6.1.2 Information Security Coordination 6.1.1- 2. Risk Assessments 6.2.1 Identification of risks related to external parties 14.1.2 Business continuity and risk assessment 15.1.1- 6. System Risk Assessments
2. System and Services Acquisition (SA) <i>Organizations must: (i) allocate sufficient resources to adequately protect organizational information systems; (ii) employ system development life cycle processes that incorporate information security considerations; (iii) employ software usage and installation restrictions; and (iv) ensure that third-party providers employ adequate security measures to protect outsourced organizational information, applications, and/or services.</i>	12 INFORMATION SYSTEMS ACQUISITION, DEVELOPMENT AND MAINTENANCE 12.5 SECURITY IN DEVELOPMENT AND SUPPORT PROCESSES
3. Certification, Accreditation, and Security Assessments (CA) <i>Organizations must: (i) periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; (ii) develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; (iii) authorize the operation of organizational information systems and any associated information system connections; and (iv) monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.</i>	10.3 SYSTEM PLANNING AND ACCEPTANCE. 10.3.1 Capacity management 10.3.2 System acceptance 15.2.1 Compliance with security policies and standards. 15.2.2 Technical compliance checking
4. Security Planning (PL) <i>Organizations must develop, document, periodically update, and implement security plans for organizational information systems that describe the security controls in place or planned for the information systems and the rules of behavior for individuals accessing the information systems.</i>	6 ORGANIZATION OF INFORMATION SECURITY 7 ASSET MANAGEMENT 15.1 COMPLIANCE WITH LEGAL REQUIREMENTS
Operational Controls	The operational controls address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems).
5. Personnel Security (PS) <i>Organizations must: (i) ensure that individuals occupying positions of responsibility within organizations (including third-party service providers) are trustworthy and meet established security criteria for those positions; (ii) ensure that</i>	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

Specific Control Objectives and Techniques	ISO Category
<p><i>organizational information and information systems are protected during personnel actions such as terminations and transfers; and (iii) employ formal sanctions for personnel failing to comply with organizational security policies and procedures.</i></p>	8.3 TERMINATION OR CHANGE OF EMPLOYMENT
<p>6. Physical and Environmental Protection (PE) <i>Organizations must: (i) limit physical access to information systems, equipment, and the respective operating environments to authorized individuals; (ii) protect the physical plant and support infrastructure for information systems; (iii) provide supporting utilities for information systems; (iv) protect information systems against environmental hazards; and (v) provide appropriate environmental controls in facilities containing information systems.</i></p>	9 PHYSICAL AND ENVIRONMENTAL SECURITY 9.1 SECURE AREAS 9.2 EQUIPMENT SECURITY
<p>7. Media Protection (MP) <i>Organizations must: (i) protect information contained in organizational information systems in printed form or on digital media; (ii) limit access to information in printed form or on digital media removed from organizational information systems to authorized users; and (iii) sanitize or destroy digital media before disposal or release for reuse.</i></p>	10.7 MEDIA HANDLING 10.7.1 Management of removable media 10.7.2 Disposal of media 10.7.3 Information handling procedures
<p>8. Contingency Planning (CP) <i>Organizations must establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.</i></p>	14 BUSINESS CONTINUITY MANAGEMENT
<p>9. Configuration Management (CM) <i>Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems; (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems; and (iii) monitor and control changes to the baseline configurations and to the constituent components of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.</i></p>	10.1 OPERATIONAL PROCEDURES AND RESPONSIBILITIES 10.1.2 Change management 10.1.3 Segregation of duties 10.1.4 Separation of development, test, and operational facilities
<p>10. System and Information Integrity (SA) <i>Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.</i></p>	10.4 PROTECTION AGAINST MALICIOUS AND MOBILE CODE 10.6.2 Security of network services 10.10.1 Audit logging 12.2 CORRECT PROCESSING IN APPLICATIONS
<p>11. Maintenance (MA) <i>Organizations must: (i) perform periodic and timely maintenance on organizational information systems; and (ii) provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.</i></p>	9.2.4 Equipment maintenance 10.1.1 Documented operating procedures 10.7.4 Security of system documentation
<p>12. Awareness and Training (AT) <i>Organizations must: (i) ensure that managers and users of organizational information systems are made aware of the security risks associated with their activities and of the applicable laws, Executive Orders, directives, policies, standards, instructions, regulations, or procedures related to the security of organizational information systems; and (ii) ensure that organizational personnel are adequately trained to carry out their assigned information security-related duties and responsibilities.</i></p>	8.2.2 Information security awareness, education, and training

Specific Control Objectives and Techniques	ISO Category
<p>13. Incident Response (IR) <i>Organizations must: (i) establish an operational incident handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and (ii) track, document, and report incidents to appropriate organizational officials and/or authorities.</i></p>	<p>13 INFORMATION SECURITY INCIDENT MANAGEMENT</p>
<p style="text-align: center;">Technical Controls</p>	<p>Technical controls focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.</p>
<p>14. Identification and Authentication (IA) <i>Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.</i></p>	<p>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</p> <p>11.3 USER RESPONSIBILITIES 11.3.1 Password use. 11.3.2 Unattended user equipment 11.3.3 Clear desk and clear screen policy</p>
<p>15. Access Controls (AC) <i>Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.</i></p>	<p>11 ACCESS CONTROL 11.1 BUSINESS REQUIREMENT FOR ACCESS CONTROL 11.1.1 Access control policy 11.4 NETWORK ACCESS CONTROL. 11.5 OPERATING SYSTEM ACCESS CONTROL 11.6 APPLICATION AND INFORMATION ACCESS CONTROL</p>
<p>16. System and Communications Protection (SC) <i>Organizations must: (i) monitor, control, and protect organizational communications at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.</i></p>	<p>10 COMMUNICATIONS AND OPERATIONS MANAGEMENT 10.6 NETWORK SECURITY MANAGEMENT 10.8 EXCHANGE OF INFORMATION 10.9 ELECTRONIC COMMERCE SERVICES 11.4 NETWORK ACCESS CONTROL</p>
<p>17. Audit and Accountability (AU) <i>Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.</i></p>	<p>10.10 MONITORING 10.10.1 Audit logging 10.10.2 Monitoring system use 10.10.3 Protection of log information 10.10.4 Administrator and operator logs 10.10.5 Fault logging 10.10.6 Clock synchronization 15.3 INFORMATION SYSTEMS AUDIT CONSIDERATIONS</p>

References:

[1] National Institute of Standards and Technology Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, December 2007

[2] National Institute of Standards and Technology Special Publication 800-53A - *Guide for Assessing the Security Controls in Federal Information Systems*, July 2008.

[3] FIPS Publication 200 - *Minimum Security Requirements for Federal Information and Information Systems*.

[4] ISO/IEC 17799:2005 (ISO 27002) – *Code of practice for information security management* - Published by ISO and available at BSI [<http://www.bsi-global.org/>]