

# Implementing ISO 17799

now from Symantec™

Enabling you to implement ISO 17799 for multiple regulations.

## Overview

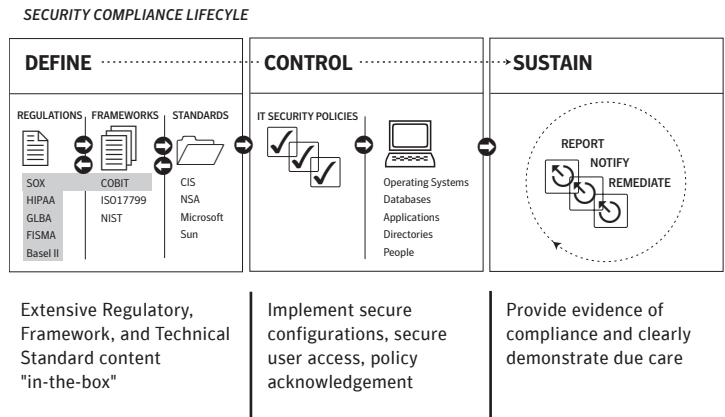
As a global framework for best practices in information security, ISO 17799 has become the optimum choice for meeting the needs of regulatory compliance in many organizations. Implementing ISO 17799, however, can be extremely difficult and expensive to achieve due to the complexity, scope and knowledge required. Symantec can help.

Symantec offers IT security solutions that help you to:

- Define regulations, frameworks and standards that apply to your organization.
- Implement standards to support policies and apply specific IT technical controls to achieve compliance.
- Demonstrate due care and sustain compliance by showing that IT controls are in effect and working properly.

## Meeting the Challenge of Complying with Multiple Regulations

The challenge of dealing with the general controls requirement for even one regulation can be intimidating and cost prohibitive. Multiply that by two or even three regulations and the complexity grows exponentially. How are mature organizations managing the challenge of demonstrating compliance with multiple regulations?



The key to success stems from identifying a common framework for implementation and mapping the regulatory requirements to that framework. ISO 17799 is quickly becoming that common framework.

In reviewing recent regulations such as HIPAA, GLBA, Sarbanes-Oxley and others, there are several consistent elements common to all these regulations. These common elements shown in Table 1 are comprehensively addressed by ISO 17799.

### Here's How Symantec Solutions Can Help

- Provides "context mapping" of industry-accepted frameworks, including ISO 17799, to a set of technical controls and policies for implementation and enforcement.
- Enables you to implement specific technical controls and customizable policies across your heterogeneous IT infrastructure.
- Assists in securing personnel acknowledgment and agreement to security and compliance policies.
- Automates procedures to continuously monitor and report on your compliance posture.
- Provides recommendations for remediating risks or gaps in your security posture.
- Integrates with leading help desk and operational monitoring solutions such as Remedy®, HP® Service Desk and HP® OpenView® so that you can leverage existing technology.

---

### ISO 17799 Provides an Ideal Framework for Compliance

ISO 17799 is an international security standard or "code of practice for information security management" that has been published by the ISO (International Organization for Standardization) and the IEC (International Electrotechnical Commission). ISO and the IEC are international standards organizations whose membership includes the standards bodies from many countries. ISO 17799 is generally accepted as the replacement for the earlier BS 7799 standard, which was published by the British Standards Institute.

Since its publication in 2000, ISO 17799 has gained wide acceptance, including recognition by leading research firms.

Gartner, for example, forecasts that by 2006, ISO 17799 will be the most common standard used to judge the information security posture of an organization. The goal of ISO 17799 is to provide a comprehensive security framework. As such, its requirements are very broad in their impact, typically affecting all aspects of your IT organization.

ISO 17799 was updated in June 2005 and in the update, 36 control areas and controls were either deleted or moved. Additionally, 46 new control areas and controls were added, including those that were deleted and modified into new sections. The net of these changes resulted in seven new controls existing within ISO 17799 for a total of 134 controls, residing within 11 security control clauses and 39 main security categories.

---

### ISO 17799 In Sync with Other Leading Compliance Frameworks

ISO 17799 is complementary to frameworks published by other organizations. For example, the United States National Institute of Standards and Technology (NIST) published its own "Recommended Security Controls for Federal Information Systems" as Special Publication 800-53 to address FISMA compliance. ISO 17799 and SP 800-53 are so complementary, that there is even an appendix in SP 800-53 that maps the sections within SP 800-53 back to ISO 17799. Additionally, other well-known research firms advise that ISO 17799 can be used to support higher level IT and security frameworks such as the Control Objectives for Information and related Technology (COBIT), which is frequently used to show compliance with the general controls requirements implied by the Sarbanes-Oxley Act of 2002.

Symantec's security compliance solutions have been helping large and small companies manage compliance issues for over 15 years. Symantec's solutions remove the barriers limiting your company's ability to demonstrate and maintain compliance with policies and regulations such as Sarbanes-Oxley, HIPAA, and GLBA.

### Make Symantec Solutions Work For You

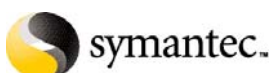
- **bv-Control®** allows administrators to efficiently identify and eliminate IT infrastructure vulnerabilities and their associated operational risk.
- **BindView® Compliance Center** now from Symantec allows security and audit professionals to continuously measure and manage compliance of systems to external standards such as the Center for Internet Security (CIS) benchmarks and Sun BluePrints®.
- **BindView Policy Operations Center®** now from Symantec automates the process of defining, documenting, tracking user acceptance and promoting awareness of security policies to employees across the organization.
- **bv-Admin®** allows administrators to cost-effectively manage user accounts, privileges, and access controls to ensure that confidential information is available only on a need to know basis.

#### REGULATORY REQUIREMENTS COMMON TO SEVERAL RECENT REGULATIONS

COMMON REGULATORY ELEMENT	DETAILS
Develop an information security policy document	<ul style="list-style-type: none"> <li>- Management commitment</li> <li>- Owner who reviews and maintains</li> <li>- Effective consensus process across departments</li> </ul>
Perform Risk Analysis and Risk Management	<ul style="list-style-type: none"> <li>- Understand your organization's risk posture</li> <li>- Keep requirements current; periodic review</li> </ul>
Train employees on security	<ul style="list-style-type: none"> <li>- Job screening</li> <li>- Supervision by a knowledgeable person</li> <li>- Users understand their responsibilities in maintaining security</li> </ul>
Develop procedures and reporting for Security Incident Response	<ul style="list-style-type: none"> <li>- Speed</li> <li>- Communication through appropriate management channels</li> </ul>
Develop a contingency plan	<ul style="list-style-type: none"> <li>- Cover natural disasters, accidents, equipment failures, and deliberate actions</li> <li>- Include preventative and recovery controls</li> <li>- Capability to restore within required time-scales</li> <li>- Test and update the plan periodically</li> </ul>
Manage access control	<ul style="list-style-type: none"> <li>- Match business process requirements to granting/revoking access to information</li> <li>- Users understand their responsibility for security</li> <li>- Access controls enforced</li> <li>- Capability to detect failure of access control</li> </ul>
Maintain audit controls	<ul style="list-style-type: none"> <li>- Only competent, technical professionals acceptable</li> <li>- Scope of controls should be agreed and controlled</li> <li>- Limit to read-only access</li> </ul>
Engage in a continuous evaluation model	<ul style="list-style-type: none"> <li>- Continuous monitoring for controls effectiveness</li> </ul>

#### ISO 17799: 2005 SECURITY CATEGORIES ADDRESSED BY BINDVIEW SOLUTIONS

SECURITY CONTROL CLAUSES	SECURITY CATEGORIES	SYMANTEC HELPS
5 - Security Policy	5.1 - Information security policy	✓
6 - Organizing Information Security	6.1 - Internal organization 6.2 - External parties	✓
7 - Asset Mgmt	7.1 - Responsibility for assets 7.2 - Information classification	✓
8 - Human Resources Security	8.2 - During employment 8.3 - Termination/change employment	✓
9 - Physical & Environmental Security	9.1 - Secure areas 9.2 - Equipment security	✓
10 - Communications & Ops Mgmt	10.1 - Operational procedures and responsibilities 10.2 - Third party service delivery management 10.3 - System planning and acceptance 10.4 - Protection against malicious and mobile code 10.5 - Back-up 10.6 - Network security management 10.7 - Media handling 10.8 - Exchange of information 10.9 - Electronic commerce services 10.10 - Monitoring	✓
11 - Access Control	11.1 - Business requirement for access control 11.2 - User access management 11.3 - User responsibilities 11.4 - Network access control 11.5 - Operating system access control 11.6 - Application and information access control 11.7 - Mobile computing and teleworking	✓
12 - Information Systems Acquisition, Development and Maintenance	12.1 - Security requirements of information systems 12.2 - Correct processing in applications 12.3 - Cryptographic controls 12.4 - Security of system files 12.5 - Security in development and support processes 12.6 - Technical Vulnerability Management	✓
13 - Information Security Incident Mgmt	13.1 - Reporting information security events & weaknesses 13.2 - Management of information security incidents and improvements	✓
14 - Business Continuity Mgmt	14.1 - Information security aspects of business continuity management	✓
15 - Compliance	15.1 - Compliance with legal requirements 15.2 - Compliance with security policies and standards, and technical compliance 15.3 - Information systems audit considerations	✓



Data Sheet: Regulation Solutions  
Implementing ISO 17799 *now from Symantec™*

**More information**

*Visit our Web site*

<http://enterprisesecurity.symantec.com>

*To speak with a Product Specialist in the U.S.*

Call toll-free (800) 745-6054

*To speak with a Product Specialist outside the U.S.*

Symantec has operations in 40 countries. For specific country offices and contact numbers, please visit our Web site.

*About Symantec*

Symantec is the world leader in information security providing a broad range of software, appliances and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions providing solutions to help individuals and enterprises assure the security, availability, and integrity of their information. Headquartered in Cupertino, California, Symantec has operations in 40 countries. More information is available at [www.symantec.com](http://www.symantec.com).

*Symantec Corporation World Headquarters*

20330 Stevens Creek Blvd.

Cupertino, CA 95014 USA

(408) 517-8000

(800) 721-3934

[www.symantec.com](http://www.symantec.com)

