

Sarbanes-Oxley Act Compliance Utilizing ISO 17799 Best Security Practices *matrix*



ISS Solutions for Security Best Practices for the Sarbanes-Oxley Act Utilizing the ISO 17799 standard

The ISO 17799 standard gives recommendations for information security management for use by those who are responsible for initiating, implementing or maintaining security in their organization. ISO 17799 is "*a comprehensive set of controls comprising best practices in information security*", and is essentially an internationally recognized generic information security standard.

For more information on ISO/IEC 17799, please visit <http://www.iso-17799.com/>

Source: ISO 17799 Directory

Section A.3.1: Security Policy

Objective: To provide management direction and support for information security.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.3.1.1 Information security policy document	A policy document shall be approved by management, published and communicated, as appropriate, to all employees	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • ISO-17799 Gap Analysis • Security Awareness Program • Documentation
Section A.3.1.2 Review and evaluation	The policy shall be reviewed regularly, and in case of influencing changes, to ensure it remains appropriate.		

Section A.4: Information Security Infrastructure

Objective: To manage information security within the organization.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.4.1.1 Management information security forum	A management forum to ensure that there is clear direction and visible management support for security initiatives shall be in place. The management forum shall promote security through appropriate commitment and adequate resourcing.	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Collaborative Business Case Assessment • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • ISO-17799 Gap Analysis • Incident Response Plan • Security Awareness Program • Security Strategy Workshop • Documentation Managed Services: <ul style="list-style-type: none"> • Detailed reports and remediation advice provided for escalated security incidents
Section A.4.1.2 Information security coordination	In large organizations, a cross-functional forum of management representatives from relevant parts of the organization shall be used to coordinate the implementation of information security controls.		
Section A.4.1.3 Allocation of information security responsibilities	Responsibilities for the protection of individual assets and for carrying out specific security processes shall be clearly defined		
Section A.4.1.4 Authorization process for information processing facilities	A management authorization process for new information processing facilities shall be established.		
Section A.4.1.5 Specialist information security advice	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization		

Section A.4.1.6 Cooperation between organizations	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.		
Section A.4.1.7 Independent review of information security	The implementation of the information security policy shall be reviewed independently.		

Section A.4.2: Information Security Infrastructure -Security of Third-Party Access

Objective: To maintain the security of organizational information processing facilities and information assets accessed by third parties.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A 4.2.1 Identification of risks from third-party access	The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Information, Policy, Application and Vulnerability Security Assessments • Penetration Test • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • ISO-17799 Gap Analysis • Security Strategy Workshop • Documentation Managed Services: <ul style="list-style-type: none"> • Vulnerability Management
Section A 4.2.2 Security requirements in third-party contracts	Arrangements involving third-party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.		

Section A.4.3: Information Security Infrastructure - Outsourcing

Not applicable to ISS.

Section A.5: Asset Clarification and Control

Objective: To maintain the appropriate protection of all organizational assets and to ensure that information assets receive an appropriate level of protection.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.5.1.1 Inventory of assets	An inventory of all important assets associated with each information system shall be drawn up and maintained.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • ISO-17799 Gap Analysis • Security Awareness Program • Documentation
Section A.5.2.1 Classification guidelines	Classifications and associated protective controls for information shall take account of business needs for sharing or restricting information, and the business impacts associated with such needs.		
Section A.5.2.2 Information labeling and handling	A set of procedures shall be defined for information labeling and handling in accordance with the classification scheme adopted by the organization.		

Section A.6.1: Personnel Security- Security in Job Definition and Resourcing

Objective: To reduce the risks of human error, theft, fraud or misuse of facilities.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.6.1 Including security in job responsibilities	Security roles and responsibilities, as laid down in the organization's information security policy shall be documented in job definitions.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • ISO-17799 Gap Analysis • Security Awareness Program • Documentation
Section A.6.1.2 Personnel screening and policy	Verification checks on permanent staff, contractors, and temporary staff shall be carried out at the time of job applications.		
Section A.6.1.3 Confidentiality agreements	Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.		
Section A.6.1.4 Terms and conditions of employment	The terms and conditions of employment shall state the employee's responsibility for information security.		

Section A.6.2: Personnel Security- User Training

Objective: To ensure that users are aware of information security threats and concerns, and are equipped to support organizational security policy in the course of their normal work.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.6.2.1 Information security education and training	All employees of the organization and, where relevant, third-party users, shall receive appropriate training and regular updates in organizational policies and procedures.	Education	X-Force® Education Services Professional Security Services (PSS): <ul style="list-style-type: none"> • Security Awareness Program

Section A.6.3: Personnel Security- Responding to Security Incidents and Malfunctions

Objective: To minimize the damage from security incidents and malfunction, and to monitor and learn from such incidents.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.6.3.1 Reporting security incidents	Security incidents shall be reported through appropriate management channels as quickly as possible.	Design	Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Intrusion Detection and Prevention Services • Customer Portal Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Incident Response Plan • Emergency Response Services • Documentation
Section A.6.3.2 Reporting security weaknesses	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems and services.	Manage and Support	
Section A.6.3.3 Reporting software malfunctions	Procedures shall be established for reporting software malfunctions.		
Section A.6.3.4 Learning from incidents	Mechanisms shall be put into place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.		
Section A.6.3.5 Disciplinary process	The violation of organizational security policies and procedures by employees shall be dealt with through a formal disciplinary process.		

Section A.7: Physical and Environmental Security

Not applicable to ISS.

Section A.8.1: Communications and Operations Management- Operational Procedures and Responsibilities

Objective: To ensure the correct and secure operation of information processing facilities.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.1.1 Documented operating procedures	The operating procedures identified in the security policy shall be documented and maintained.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Incident Response Plan • Emergency Response Services • Documentation Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Intrusion Detection and Prevention Services • Customer Portal
Section A.8.1.2 Operational change controls	Changes to information processing facilities and systems shall be controlled.	Manage and Support	
Section A.8.1.3 Incident management procedures	Incident management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to security incidents and to collect incident related data such as audit trails and logs.		
Section A.8.1.4 Segregation of duties	Development and testing facilities shall be separated in order to reduce opportunities for unauthorized modification or misused of information and services.		
Section A.8.1.5 Separation of development and operational facilities	Development and testing facilities shall be separated from operational facilities. Rules for the migration of software from development to operational status shall be defined and documented.		
Section A.8.1.6 External facilities management	Prior to using external facilities management services, the risks shall be identified and appropriate controls agreed with the contractor, and incorporated into a contract.		

Section A.8.2: Communications and Operations Management- System Planning and Acceptance

Objective: To minimize the risk of systems failure

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.2.1 Capacity planning	Capacity demands shall be monitored and projection of future capacity requirements made to enable adequate processing power and storage to be made available.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Network Architecture Review and Design • Best Practices for Sarbanes-Oxley • Documentation
Section A.8.2.2 System Acceptance	Acceptance criteria for new information systems, upgrades and new versions shall be established and suitable tests of the system carried out prior to acceptance.	Manage and Support	

Section A.8.3: Communications and Operations Management- Protection Against Malicious Software

Objective: To protect the integrity of software and information from damage by malicious software

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.3.1 Controls against malicious software	Detection and prevention controls to protect against malicious software and appropriate user awareness procedures shall be implemented.	Deploy Design	Proventia™ Integrated Security Appliances: Single, all-in-one protection for networks, servers and desktops combining: <ul style="list-style-type: none"> • Stateful Inspection Firewall • VPN • Antivirus • Intrusion Detection and Prevention • Content Filtering • Anti-spam • Application Protection SiteProtector™ Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy Design • Best Practices • Documentation

Section A.8.4: Communications and Operations Management- Housekeeping

Objective: To maintain the integrity and availability of information processing and communication services

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.4.1 Information back-up	Back-up copies of essential business information and software shall be taken and test regularly.	Manage and Support	Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Firewall Service • Managed Intrusion Detection and Prevention Services • Vulnerability Management • Customer Portal
Section A.8.4.2 Operator logs	Operational staff shall maintain a log of their activities. Operator logs shall be subject to regular, independent checks.		
Section A.8.4.3 Fault logging	Faults shall be reported and corrective action taken.		

Section A.8.5: Communications and Operations Management- Network Management

Objective: To ensure the safeguarding of information in networks and the protection of the supporting infrastructure

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.5.1 Network controls	A range of controls shall be implemented to achieve and maintain security in networks.	Deploy Design	Proventia Integrated Security Appliances SiteProtector Professional Security Services (PSS): <ul style="list-style-type: none"> • Information, Policy, Application and Vulnerability Security Assessments • ISO 17799 Gap Analysis

Section A.8.6: Communications and Operations Management- Media Handling and Security

Objective: To prevent damage to assets and interruptions to business activities

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.6.1 Management of removable computer media	The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.8.6.2 Disposal of media	Media shall be disposed of securely and safely when no longer required.		
Section A.8.6.3 Information handling procedures	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.		
Section A.8.6.4 Security of system documentation	System documentation shall be protected from unauthorized access.		

Section A.8.7: Communications and Operations Management- Exchanges of Information and Software

Objective: To prevent damage to assets and interruptions to business activities

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.8.7.1 Information and software exchange agreements	Agreements, some of which may be formal, shall be established for the exchange of information and software (whether electronic or manual) between organizations.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation Proventia Integrated Security Appliances SiteProtector
Section A.8.7.2 Security of media in transit	Media being transported shall be protected from unauthorized access, misuse or corruption.	Assess and Deploy	
Section A.8.7.3 Electronic commerce security	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.		
Section A.8.7.4 Security of electronic mail	A policy for the use of electronic mail shall be developed and controls put into place to reduce security risk created by electronic mail		

Section A.8.7.5 Security of electronic office systems	Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.		
Section A.8.7.6 Publicly available systems	There shall be a formal authorization process before information is made publicly available and the integrity of such information shall be protected to prevent unauthorized modification.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation
Section A.8.7.7 Other forms of information exchange	Policies, procedures and controls shall be in place to protect the exchange of information through the use of voice, facsimile and video communications facilities.		

Section A.9: Access Control- Business Requirement for Access Control

Objective: To control access to information.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.1 Access control policy	Business requirements for access control shall be defined and documented, and access shall be restricted to what is defined in the access control policy.	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation

Section A.9.2: Access Control- User Access Management

Objective: To ensure that access rights to information systems are appropriately authorized, allocated and maintained.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.2.1 User registration	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation
Section A.9.2.2 Privilege management	The allocation and use of privileges shall be restricted and controlled.		
Section A.9.2.3 User password management	The allocation of passwords shall be controlled through a formal management process.		
Section A.9.2.4 Review of user access right	Management shall conduct a formal process at regular intervals to review users; access rights.		

Section A.9.3: Access Control- User Responsibilities

Objective: To prevent unauthorized user access.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.3.1 Password use	Users shall be required to follow good security practices in the selection and use of passwords.	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.9.3.2 Unattended user equipment	Users shall be required to ensure that unattended equipment is given appropriate protection.		

Section A.9.4: Access Control- Network Access Control

Objective: Protection of networked services.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.4.1 Policy on use of network services	Users shall have only direct access to the services that they have been specifically authorized to use.	Deploy	Proventia Integrated Security Appliances SiteProtector X-Force Professional Services: <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.9.4.2 Enforced path	The path from the user terminal to the computer service shall be controlled.		
Section A.9.4.3 User authentication for external connections	Access by remote users shall be subject to authentication.		
Section A.9.4.4 Node authentication	Connections to remote computer systems shall be authenticated.		
Section A.9.4.5 Remote diagnostic port protection	Access to diagnostic ports shall be securely controlled.		
Section A.9.4.6 Segregation in networks	Controls shall be introduced in networks to segregate groups of information services, users and information systems.		
Section A.9.4.7 Network connection control	The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.		

Section A.9.4.8 Network routing control	Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access policy of the business applications.		
Section A.9.4.9 Security of network services	A clear description of the security attributes of all network services used by the organization shall be provided.		

Section A.9.5: Access Control- Operating System Access Control

Objective: To prevent unauthorized computer access.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.5.1 Automatic terminal identification	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	Deploy	Proventia Integrated Security Appliances SiteProtector Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.9.5.2 Terminal log-in procedures	Access to information services shall use a secure log-on process.	Design	
Section A.9.5.3 User identification and authentication	All users shall have a unique identifier (User ID) for their personal and sole use so that activities can be traced to the responsible individual.		
Section A.9.5.4 Password management system	Password management systems shall provide an effective, interactive facility which aims to ensure quality passwords.		
Section A.9.5.5 Use of system utilities	Use of system utility programs shall be restricted and tightly controlled.		
Section A.9.5.6 Duress alarm to safeguard users	Duress alarms shall be provided for users who might be the target of coercion.		
Section A.9.5.7 Terminal time-out	Inactive terminals in high risk locations or serving high risk systems shall be shut down after a defined period of inactivity to prevent access by unauthorized persons.		
Section A.9.5.8 Limitation of connection time	Restrictions on connection times shall be used to provide additional security for high-risk applications.		

Section A.9.6: Access Control- Application Access Control

Objective: To prevent unauthorized access to information held in information systems.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.5.1 Information access restriction	Access to information and application system functions shall be restricted in accordance with the access control policy.	Deploy	Proventia Integrated Security Appliances SiteProtector Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.9.6.2 Sensitive system isolation	Sensitive systems shall have a dedicated (isolated) computing environment	Design	

Section A.9.7: Access Control- Monitoring System Access and Use

Objective: To control access to information.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.7.1 Event logging	Audit logs recording exceptions and other security-relevant events shall be produced and kept for an agreed period to assist in future investigations and access-control monitoring.	Manage and Support	Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Firewall Service • Managed Intrusion Detection and Prevention Services • Vulnerability Management • Customer Portal Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Security Awareness Program • Documentation
Section A.9.7.2 Monitoring system use	Procedures for monitoring the use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.	Design	
Section A.9.7.3 Clock synchronization	Computer clocks shall be synchronized for accurate recording.		

Section A.9.8.1: Access Control- Mobile Computing and Telecommuting

Objective: To ensure information security when using mobile computing and telecommuting facilities.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.9.8.1 Mobile computing	A formal policy shall be in place and appropriate controls shall be adopted to protect against the risks of working with mobile computing facilities, in particular in unprotected environments.	Assess and Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley Security Awareness Program • Documentation
Section A.9.8.2 Telecommuting	Policies, procedures and standards shall be developed to authorize and control telecommuting activities.		

Section A.10: System Development and Maintenance- Security Requirements of Systems

Objective: To ensure that security is built into information systems.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.10.1.1 Security requirements analysis and specifications	Business requirements for new systems or enhancements to existing systems shall specify the requirements for controls.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Network Architecture Review and Design • Documentation

Section A.10.2: System Development and Maintenance- Security in Application Systems

Objective: To prevent loss, modification or misuse of user data in application systems.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.10.2.1 Input data validation	Data input to application systems shall be validated to ensure that it is correct and appropriate.	Deploy	Proventia Integrated Security Appliances SiteProtector Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Network Architecture Review and Design • Documentation
Section A.10.2.2 Control of internal processing	Validation checks shall be incorporate into systems to detect any corruption of the data processed.	Design	
Section A.10.2.3 Message authentication	Message authentication shall be used for application where there is a security requirement to protect the integrity of the message content		
Section A.10.2.4 Output data validation	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.		

Section A.10.3: System Development and Maintenance- Cryptographic Controls

Objective: To prevent loss, modification or misuse of user data in application systems.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.10.3.1 Policy on the use of cryptographic controls	A policy on the use of cryptographic controls for the protection of information shall be developed.	Design	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation Proventia Integrated Security Appliances Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Firewall Service • Managed Intrusion Detection and Prevention Services • Vulnerability Management • Customer Portal
Section A.10.3.2 Encryption	Encryption shall be applied to protect the confidentiality of sensitive or critical information.	Deploy	
Section A.10.3.3 Digital signatures	Digital signatures shall be applied to protect the authenticity and integrity of electronic information.	Manage and Support	
Section A.10.3.4 Non-repudiation services	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event of action.		
Section A.10.3.5 Key management	A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.		

Section A.10.4: System Development and Maintenance- Security of Systems Files

Objective: To ensure that IT projects and support activities and conducted in a secure manner.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.10.4.1 Control of operational software	Procedures shall be in place to control the implementation of software on operations systems.	Design and Deploy	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation Proventia Integrated Security Appliances SiteProtector
Section A.10.4.2 Protection of system test data	Test data shall be protected and controlled.		
Section A.10.4.3 Access control to program source library	Strict control shall be maintained over access to program source libraries.		

Section A.10.5: System Development and Maintenance- Security in Development and Support Processes

Objective: To maintain the security of application system software and information.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.10.5.2 Change control procedures.	The implementation of changes shall be strictly controlled by the use of formal change control procedures.	Design Manage and Support	Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Documentation Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Firewall Service • Managed Intrusion Detection and Prevention Services • Vulnerability Management • Customer Portal
Section A.10.5.3 Technical review of operating system changes	Application systems shall be reviewed and tested when changes occur.		
Section A.10.5.3 Restrictions on changes to software packages	Modifications to software packages shall be discouraged and essential changes strictly controlled.		
Section A.10.5.4 Convert channels and Trojan code	The purchase, use and modification of software shall be controlled and checked to protect against possible convert channels and Trojan code.		
Section A.10.5.5 Outsourced software development	Controls shall be applied to secure outsourced software development.		

Section A.11: Business Continuity Management- Aspects of Business Continuity Management

Objective: To counteract interruption to business activities and to protect critical business processes from the effects of major failures or disasters.

ISO 17799 Requirement	Description	ISS Program Phase	ISS Solutions to Achieve ISO 11799 Compliance
Section A.11.1.1 Business continuity management process	There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	Design	Managed Services: <ul style="list-style-type: none"> • Managed Protection Services • Managed Firewall Service • Managed Intrusion Detection and Prevention Services • Vulnerability Management • Customer Portal Professional Security Services (PSS): <ul style="list-style-type: none"> • Policy and Procedures Design • Best Practices for Sarbanes-Oxley • Emergency Response Services • Incident Response Plan • Documentation
Section A.11.1.2 Business continuity and impact analysis	A strategy plan, based upon appropriate risk assessment, shall be developed for the overall approach to business continuity.	Manage and Support	
Section A.11.1.3 Writing and implementing continuity plans	Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.		
Section A.11.1.4 Business continuity planning framework	A single framework of business continuity plans shall be maintained to ensure that all plans are consistent, and to identify priorities for testing and maintenance.		
Section A.11.1.5 Testing, maintaining and re-assessing business continuity plans	Business continuity plans shall be tested regularly and maintained by regular reviews to ensure they are up to date and effective.		

GLOBAL HEADQUARTERS

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: (404) 236 2600

REGIONAL HEADQUARTERS

Australasia

Internet Security Systems Pty Ltd.
Level 6, 15 Astor Terrace
Spring Hill Queensland 4000
Australia
Phone: +61 (0)7 3838 1555
Fax: +61 (0)7 3832 4756
e-mail: aus-info@iss.net
Support e-mail: support@iss.net

Asia Pacific

Internet Security Systems K. K.
JR Tokyu Meguro Bldg. 3-1-1
Kami-Osaki, Shinagawa-ku
Tokyo 141-0021
Japan
Phone: +81 (3) 5740-4050
Fax: +81 (3) 5487-0711
e-mail: sales@isskk.co.jp
Support e-mail: support@isskk.co.jp

Europe, Middle East and Africa

Ringlaan 39 bus 5
1853 Strombeek-Bever
Belgium
Phone: +32 (2) 479 67 97
Fax: +32 (2) 479 75 18
e-mail: isseur@iss.net

Latin America

6303 Barfield Road
Atlanta, GA 30328
United States
Phone: 404 236 2790
Fax: 404 236 2629
e-mail: isslatam@iss.net