

Achieving Best Security Practices Utilizing ISO 17799 Standards



ISS Solutions

for Achieving ISO 17799 Security Standards

The ISO/IEC 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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Information security policy document Section A.3.1.1	A policy document shall be approved by management, published and communicated, as appropriate, to all employees	Assess and Design	X-Force™ Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practice · Documentation · ISO-17799 Gap Analysis · Security Awareness Program
Review and evaluation Section A.3.1.2	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Management information security forum Section A.4.1.1	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.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practice · Documentation · Incident Response Plan · Security Awareness Program · Security Strategy Workshop
Information security coordination Section A.4.1.2	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.		

Continued

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Allocation of information security responsibilities Section A.4.1.3	Responsibilities for the protection of individual assets and for carrying our specific security processes shall be clearly defined	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practice · Documentation · Incident Response Plan · Security Awareness Program · Security Strategy Workshop
Authorization process for information processing facilities Section A.4.1.4	A management authorization process for new information processing facilities shall be established..		
Specialist information security advice Section A.4.1.5	Specialist advice on information security shall be sought from either internal or external advisors and coordinated throughout the organization		
Cooperation between organizations Section A.4.1.6	Appropriate contacts with law enforcement authorities, regulatory bodies, information service providers and telecommunications operators shall be maintained.		
Independent review of information security Section A.4.1.7	The implementation of the information security policy shall be reviewed independently.	Assess	X-Force Professional Services: <ul style="list-style-type: none"> · ISO-17799 Gap Analysis · Vulnerability Assessment · Penetration Test · Wireless Assessment

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Identification of risks from third-party access Section A 4.2.1	The risks associated with access to organizational information processing facilities by third parties shall be assessed and appropriate security controls implemented.	Assess and Design	X-Force Professional Services: <ul style="list-style-type: none"> · Information Security Assessment · Application Security Assessment · Penetration Test · Vulnerability Assessment
Security requirements in third-party contracts Section A 4.2.2	Arrangements involving third-party access to organizational information processing facilities shall be based on a formal contract containing all necessary security requirements.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Inventory of assets Section A.5.1.1	An inventory of all important assets associated with each information system shall be drawn up and maintained.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program
Classification guidelines Section A.5.2.1	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.		
Information labeling and handling Section A.5.2.2	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Including security in job responsibilities Section A.6.1	Security roles and responsibilities, as laid down in the organization's information security policy shall be documented in job definitions.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program
Personnel screening and policy Section A.6.1.2	Verification checks on permanent staff, contractors, and temporary staff shall be carried out at the time of job applications.		
Confidentiality agreements Section A.6.1.3	Employees shall sign a confidentiality agreement as part of their initial terms and conditions of employment.		
Terms and conditions of employment Section A.6.1.4	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Information security education and training Section A.6.2.1	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 X-Force Professional Services: <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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Reporting security incidents Section A.6.3.1	Security incidents shall be reported through appropriate management channels as quickly as possible.	Design Manage and Support	Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings. X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Incident Response Plan · Emergency Response Services
Reporting security weaknesses Section A.6.3.2	Users of information services shall be required to note and report any observed or suspected security weaknesses in, or threats to, systems and services.		
Reporting software malfunctions Section A.6.3.3	Procedures shall be established for reporting software malfunctions.		
Learning from incidents Section A.6.3.4	Mechanisms shall be put into place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.		
Disciplinary process Section A.6.3.5	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

Currently not offered by 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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Documented operating procedures Section A.8.1.1	The operating procedures identified in the security policy shall be documented and maintained.		
Operational change controls Section A.8.1.2	Changes to information processing facilities and systems shall be controlled.		
Incident management procedures Section A.8.1.3	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.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices- Documentation · Security Awareness Program · Incident Response Plan · Emergency Response Services
Segregation of duties Section A.8.1.4	Development and testing facilities shall be separated in order to reduce opportunities for unauthorized modification or misused of information and services.	Manage and Support	Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Separation of development and operational facilities Section A.8.1.5	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.		
External facilities management Section A.8.1.6	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Capacity planning Section A.8.2.1	Capacity demands shall be monitored and projection of future capacity requirements made to enable adequate processing power and storage to be made available.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation
System Acceptance Section A.8.2.2	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	Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings. Dynamic Threat Protection™ Platform: <ul style="list-style-type: none"> · RealSecure® System Scanner · RealSecure Internet Scanner

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Network controls Section A.8.5.1	A range of controls shall be implemented to achieve and maintain security in networks.	Deploy Design	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector™ Proventia™ X-Force Professional Services: <ul style="list-style-type: none"> · ISO-17799 Gap Analysis · Information Security Assessment · Application Security Assessment · Vulnerability Assessment

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

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Management of removable computer media Section A.8.6.1	The management of removable computer media, such as tapes, disks, cassettes and printed reports shall be controlled.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program
Disposal of media Section A.8.6.2	Media shall be disposed of securely and safely when no longer required.		
Information handling procedures Section A.8.6.3	Procedures for the handling and storage of information shall be established in order to protect such information from unauthorized disclosure or misuse.		
Security of system documentation Section A.8.6.4	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Information and software exchange agreements Section A.8.7.1	Agreements, some of which may be formal, shall be established for the exchange of information and software (whether electronic or manual) between organizations.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation
Security of media in transit Section A.8.7.2	Media being transported shall be protected from unauthorized access, misuse or corruption.	Assess Deploy	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia
Electronic commerce security Section A.8.7.3	Electronic commerce shall be protected against fraudulent activity, contract dispute and disclosure or modification of information.		
Security of electronic mail Section A.8.7.4	A policy for the use of electronic mail shall be developed and controls put into place to reduce security risk created by electronic mail		
Security of electronic office systems Section A.8.7.5	Policies and guidelines shall be prepared and implemented to control the business and security risks associated with electronic office systems.		
Publicly available systems Section A.8.7.6	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	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Other forms of information exchange A.8.7.7	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Access control policy Section A.9.1	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	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Information Security Assessment · Application Security Assessment · Vulnerability Assessment

Section A.9.2: Communications and Operations Management - Exchanges of Information and Software

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
User registration Section A.9.2.1	There shall be a formal user registration and de-registration procedure for granting access to all multi-user information systems and services.	Deploy	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS)
Privilege management Section A.9.2.2	The allocation and use of privileges shall be restricted and controlled.		
User password management Section A.9.2.3	The allocation of passwords shall be controlled through a formal management process.	Assess and Design	SiteProtector Proventia
Review of user access right Section A.9.2.4	Management shall conduct a formal process at regular intervals to review users; access rights.	Manage and Support	X-Force Professional Services:

Section A.9.3: Access Control - User Responsibilities

Objective: To prevent unauthorized user access.

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Password use Section A.9.3.1	Users shall be required to follow good security practices in the selection and use of passwords.	Assess and Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Unattended user equipment Section A.9.3.2	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Policy on use of network services Section A.9.4.1	Users shall have only direct access to the services that they have been specifically authorized to use.	Deploy Assess and Design	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Security Awareness Program · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Enforced path Section A.9.4.2	The path from the user terminal to the computer service shall be controlled.		
User authentication for external connections Section A.9.4.3	Access by remote users shall be subject to authentication.		
Node authentication Section A.9.4.4	Connections to remote computer systems shall be authenticated.		
Remote diagnostic port protection Section A.9.4.5	Access to diagnostic ports shall be securely controlled.		
Segregation in networks Section A.9.4.6	Controls shall be introduced in networks to segregate groups of information services, users and information systems.		
Network connection control Section A.9.4.7	The connection capability of users shall be restricted in shared networks, in accordance with the access control policy.		
Network routing control Section A.9.4.8	Shared networks shall have routing controls to ensure that computer connections and information flows do not breach the access policy of the business applications.		
Security of network services Section A.9.4.9	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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Automatic terminal identification Section A.9.5.1	Automatic terminal identification shall be considered to authenticate connections to specific locations and to portable equipment.	Deploy Design	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia
Terminal log-in procedures Section A.9.5.2	Access to information services shall use a secure log-on process.		
User identification and authentication Section A.9.5.3	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.		

Continued

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Password management system Section A.9.5.4 Use of system utilities Section A.9.5.5 Duress alarm to safeguard users Section A.9.5.6 Terminal time-out Section A.9.5.7	Password management systems shall provide an effective, interactive facility which aims to ensure quality passwords. Use of system utility programs shall be restricted and tightly controlled. Duress alarms shall be provided for users who might be the target of coercion. 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.	Deploy Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Security Awareness Program · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Limitation of connection time Section A.9.5.8	Restrictions on connection times shall be used to provide additional security for high-risk applications.	N/a	N/a

Section A.9.6: Access Control - Application Access Control

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Information access restriction Section A.9.5.1	Access to information and application system functions shall be restricted in accordance with the access control policy.	Deploy Design	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Security Awareness Program · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Sensitive system isolation Section A.9.6.2	Sensitive systems shall have a dedicated (isolated) computing environment	N/a	N/a

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

Objective: To control access to information.

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Event logging Section A.9.7.1	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.		Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Monitoring system use Section A.9.7.2	Procedures for monitoring the use of information processing facilities shall be established and the result of the monitoring activities reviewed regularly.	Manage and Support Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program · Information Security Assessment · Application Security Assessment · Vulnerability Assessment · Incident Response Plan
Clock synchronization Section A.9.7.3	Computer clocks shall be synchronized for accurate recording.	N/a	N/a

Section A.9.8: Access Control - Mobile Computing and Telecommuting

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Mobile computing Section A.9.8.1	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.		X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Information Security Assessment · Application Security Assessment · Vulnerability Assessment
Telecommuting Section A.9.8.2	Policies, procedures and standards shall be developed to authorize and control telecommuting activities.	Assess and Design	<ul style="list-style-type: none"> · Wireless Assessment

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

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Security requirements analysis and specifications Section A.10.1.1	Business requirements for new systems, or enhancements to existing systems shall specify the requirements for controls.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · 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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Input data validation Section A.10.2.1	Data input to application systems shall be validated to ensure that it is correct and appropriate.		Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Security Awareness Program
Control of internal processing Section A.10.2.2	Validation checks shall be incorporated into systems to detect any corruption of the data processed.	Deploy	
Message authentication Section A.10.2.3	Message authentication shall be used for application where there is a security requirement to protect the integrity of the message content	Design	
Output data validation Section A.10.2.4	Data output from an application system shall be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.	Assess	

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

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

ISO/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Policy on the use of cryptographic controls Section A.10.3.1	A policy on the use of cryptographic controls for the protection of information shall be developed.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation
Encryption Section A.10.3.2	Encryption shall be applied to protect the confidentiality of sensitive or critical information.	Deploy	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia
Digital signatures Section A.10.3.3	Digital signatures shall be applied to protect the authenticity and integrity of electronic information.		
Non-repudiation services Section A.10.3.4	Non-repudiation services shall be used to resolve disputes about occurrence or non-occurrence of an event of action.	Manage and Support	Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Key management Section A.10.3.5	A key management system based on an agreed set of standards, procedures and methods shall be used to support the use of cryptographic techniques.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Control of operational software Section A.10.4.1	Procedures shall be in place to control the implementation of software on operations systems.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation
Protection of system test data Section A.10.4.2	Test data shall be protected and controlled.	Deploy	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Guard · RealSecure Desktop · RealSecure Server Sensor · RealSecure System Scanner · VPN Enforcer · Dual authentication · Intrusion Protection Systems (IPS) SiteProtector Proventia
Access control to program source library Section A.10.4.3	Strict control shall be maintained over access to program source libraries.	Assess and Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Application Security Assessment

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Change control procedures. Section A.10.5.2	The implementation of changes shall be strictly controlled by the use of formal change control procedures.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Application Security Assessment
Technical review of operating system changes Section A.10.5.3	Application systems shall be reviewed and tested when changes occur.	Manage and Support	Dynamic Threat Protection Platform: <ul style="list-style-type: none"> · RealSecure Server Sensor · RealSecure System Scanner
Restrictions on changes to software packages Section A.10.5.3	Modifications to software packages shall be discouraged and essential changes strictly controlled.		Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Convert channels and Trojan code Section A.10.5.4	The purchase, use and modification of software shall be controlled and checked to protect against possible convert channels and Trojan code.		
Outsourced software development Section A.10.5.5	Controls shall be applied to secure outsourced software development.	Assess and Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation · Application Security Assessment

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/IEC 17799 Requirements	Description	ISS Program Phase	ISS Solutions to Achieve ISO/IEC 17799 Compliance
Business continuity management process Section A.11.1.1	There shall be a managed process in place for developing and maintaining business continuity throughout the organization.	Manage and Support	Managed Protection Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Business continuity and impact analysis Section A.11.1.2	A strategy plan, based upon appropriate risk assessment, shall be developed for the overall approach to business continuity.	Design	X-Force Professional Services: <ul style="list-style-type: none"> · Policy Design · Best Practices · Documentation
Writing and implementing continuity plans Section A.11.1.3	Plans shall be developed to maintain or restore business operations in a timely manner following interruption to, or failure of, critical business processes.		
Business continuity planning framework Section A.11.1.4	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.	Manage and Support	Managed Security Services: <ul style="list-style-type: none"> · On-going monitoring and reporting · Outsourced solution to provide a significant cost savings.
Testing, maintaining and re-assessing business continuity plans Section A.11.1.5	Business continuity plans shall be tested regularly and maintained by regular reviews to ensure they are up to date and effective.		