



REALTOR® Secure Program

Self Review

Version 1.15

Center for REALTOR® Technology

Mar 17, 2006



Table of Contents

Table of Contents	2
Security self review for REALTOR® organizations	3
Purpose.....	3
Who should complete this form.....	3
How to use this form.....	4
Section summary.....	4
Self review summary	4
Section 1 Security Policy and Management	5
Section 1 rating	6
Section 2 Physical security and access	7
Section 2 rating	7
Section 3 Remote Access.....	8
Section 3 rating	8
Section 4 Network Access	9
Section 4 rating	10
Section 5 Intrusion detection	11
Section 5 rating	11
Section 6 Virus protection	12
Section 6 rating	12
Section 7 System security	13
Section 7 rating	13
Section 8 User management.....	14
Section 8 rating	14
Section 9 Data encryption.....	15
Section 9 rating	15
Section 10 Disaster recovery	16
Section 10 rating	16
Section 11 Development.....	17
Section 11 rating	17



Security self review for REALTOR® organizations

Purpose

The goal of the REALTOR® Secure program is to address a range of today's information technology concerns; securing networks and applications, avoiding business interruptions and securing online transactions. The program raises the security awareness of REALTOR® organizations by defining a standard of care for avoiding disruptions, protecting sensitive information and securing the technical infrastructure of participating organizations.

The REALTOR Secure program uses security industry information technology best practices that a brokerage or MLS must meet to qualify as REALTOR® Secure. The best practices are detailed in ISO standard 17799 and (ISC)² Common Body of Knowledge.

The self-review provides brokerages and MLSs with the ability to assess the effectiveness of their security measures prior to retaining a third party evaluator. Successful completion of the self-review yields two benefits. First it allows the participant understand their current security status. Secondly it allows the participant to determine if work is needed before engaging a third party evaluator.

This self-review provides a tool to help participants. It is one component of the REALTOR® Secure program. It provides a self-rating mechanism to help participants determine if their security measures meet the industry guidelines.

For more information about the REALTOR® Secure program, please visit the program web site at www.REALTOR.org/secure.

Who should complete this form

The person who is responsible for information security in the REALTOR® organization should complete this form. Depending on the size and structure of the organization, this person may be the MIS Manager, Information Security Officer, Network Administrator, Managing Broker or lead programmer.



How to use this form

This form is divided into six sections. Each section focuses on a specific area of security. Within each section, the security severity of each question is indicated as a **1** or **2**.

Rating	Security meaning
1	Indicates a critical security requirement. If this requirement is not followed, information may be at risk or the site compromised.
2	A recommended security industry best practice. The Center for REALTOR® Technology recommends this practice to reduce the risk of a security breach.

Section summary

A summary follows each section. After completing each section, fill in the rating as follows:

If	Section summary rating is
All category 1 and 2 questions are answered 'Yes'	1 - you are following security industry best practices.
All category 1 questions are answered 'Yes' Some category 2 questions are answered 'No'	2 - your organization does not follow some security industry best practice. There are some items that need further examination or changes.
Any category 1 question is answered 'No'.	3 - you have a serious information security risk. It should be fixed before proceeding with the certification process.

Self review summary

If	The self-review summary is
All sections are '1'	Proceed with the third party-evaluation.
One or more sections are '2'	You may proceed with the third-party. However there may be items that require remediation as a part of the REALTOR® Secure program.
One or more sections are '3'	You should fix or change the security risk before engaging the third-party evaluator or proceeding with the REALTOR® Secure program.

Section 1 Security Policy and Management

Risk Level	Item		
1	Does a security policy exist with in the organization?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the policy documented?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does management approve the security policy?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the policy published and communicated to all employees?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the policy state management's commitment to security?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the policy discuss the approach to managing security?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the security policy contain a definition of information security, it objectives and scope?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the policy contain a statement of management intent and support the goals of information security?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the policy contain an explanation of each principle, standard and compliance requirement of importance to the organization?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does a management process exist to identify security risks and threats?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the security policy updated when the environment changes?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the security policy reviewed at least once a year?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Have you made a formal risk analysis of your information infrastructure in the past year?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there an information security awareness program in your office?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the information security awareness program regularly updated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there a documented security incident response plan?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Do you have someone responsible for information security in your organization?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are the information security responsibilities clearly defined?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

2	Is compliance to the security policy assessed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Do all contracts with vendors contain a clause that specifies information must be kept confidential?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there a documented privacy policy?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the privacy policy made available to consumers as part of the web presence?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the privacy policy communicated to all employees?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are all changes to the environment formally authorized and logged before being implemented?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 1 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 2 Physical security and access

Risk Level	Item	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the security perimeter clearly defined and the facilities physically sound?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the perimeter void of any areas where a break-in could occur?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are the walls of solid construction?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are external doors protected against unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there a manned reception area?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is there a visitor log for restricted areas?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are access badges or proximity cards used for access to restricted areas?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Do personnel in restricted areas wear visible identification?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are access rights to secure areas regularly review and updated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are access rights to secure areas removed when personnel changes?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is key storage physically protected?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is sensitive information deleted or destroyed before physically being disposed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are privileged user who have access to sensitive or processing platforms required to use an ID card, or some other two-factor or token-based authentication method?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is sensitive information physically separated from other stored data in the e-commerce environment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is media containing sensitive information protected against unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is sensitive data encrypted in databases and in backup media?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are audit logs regularly reviewed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is information printed on paper or received by fax adequately protected against unauthorized access?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are procedures in place to handle secure disposal of backup media and other media containing sensitive information?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 2 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 3 Remote Access

Risk Level	Item	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are only users with a specific business requirement are granted remote access capabilities.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Users are authenticated prior to accessing corporate network resources.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Authentication is in the form of a unique username and password.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Data encryption is used when corporate data is accessed over public networks.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	When customers, employees, or business partners remotely access systems via the Internet, is encryption used to protect from eavesdropping?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is secure encrypted communications used for remote administration of production systems and applications?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is strong two-factor authentications used for remote administration of production systems and applications?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 3 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 4 Network Access

1	Is there a formal process for approving all external network connections (physical or virtual circuits), including documentation referencing the business case for each connection.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are access control devices such as a firewall used to separate public, 3 rd party, and corporate networks?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are users located on separate network segments from those containing servers?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are users segments separated from server segments by a firewall or equivalent access control device?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Do network access policies disallow all access by default?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is network address masquerading used to prevent internal (corporate) addresses from being translated and revealed on public networks?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are access policies audited to identify out dated policy rules.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are access control logs regularly reviewed, and do they contain both successful and unsuccessful login attempts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Do access control measures include username and password authentication?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is user access restricted on a need-to-know basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are maintenance accounts and remote support access disabled if they are not required?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is there a password policy that enforces the use of strong passwords for both employees and customers?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are users required to change their password on a regular basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are privileged and administrative accounts strictly controlled?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are password protected screen-savers used on systems and consoles that provide access to sensitive information and critical systems?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are security incidents reported for investigation?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is separation of duties enforced to prevent developers from accessing the production system and installing modified software without authorization?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is separation of duties enforced and does it prevent backup operators from being actively involved in the operations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are vendor default security settings changed on production systems before the system goes into production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all production systems hardened by removing all unnecessary tools installed by the default configuration?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all production systems updated with the latest security related patches released by the vendors of various components?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

2	Are production system and application modifications planned, authorized, and traced?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the router configuration secured?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are egress and ingress filters installed on all border routers to prevent impersonation with spoofed IP addresses?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	If routers and other network devices are configured remotely, is a secure communication protocol used to protect the communication channel from eavesdropping?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are routers configured to drop any unauthorized packets?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are the router logs regularly reviewed for unauthorized traffic?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are routers configured to prevent remote probing?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is a firewall used to protect the network, and to limit traffic to only that required for business?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Do changes to the firewall need authorization, and are the changes logged?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are firewall logs regularly reviewed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is the network segment containing the servers for the Web presence separated from the Internet with a firewall?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the network segment containing the servers for the Web presence separated from the network segment containing the internal servers with a firewall?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the firewall configured to translate the IP addresses used on the internet to different internal IP addresses (for example, using network address translation, NAT)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does the network configuration prevent network mapping from the outside (for example, ping, trace route)?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all Internet accessible hosts (for example, firewall, Web server, router, etc.) periodically updated and patched for security vulnerabilities?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is a network based intrusion detection system (IDS) used on your network?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are transmissions of data encrypted through the use of SSL or other industry acceptable methods?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 4 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 5 Intrusion detection

2	Is there an account lockout mechanism that blocks a user from obtaining access to an account by multiple password retries or brute force?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is a security assessment and/or penetration test performed on your environment at regularly?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is an intrusion detection device installed and operational where network access control devices separate trusted from untrusted networks?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the intrusion detection devices alert security personal in the event that unauthorized access is detected?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the intrusion detection device frequently updated from a software and attack signature standpoint?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is the intrusion detection device monitored on a 24/7 basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 5 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 6 Virus protection

1	Are users educated on detection and prevention of viruses?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Do all computers have virus protection installed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are regular reviews conducted on software and data content for systems that support critical business processes?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all files on electronic media of uncertain or unauthorized origin checked for viruses before use?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all e-mail attachments and downloads checked for malicious software or viruses before use?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is a virus scanner installed on all servers and workstations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are virus scanning tools and applications regularly updated?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Do all workstations have a personal firewall installed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are virus checks done at the gateway?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are virus checks done at the e-mail server?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are virus checks done on the desktop?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 6 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 7 System security

1	Are vendor-supplied defaults changed before a system is placed into production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Do standard builds for each system class exist?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Do server builds take into account all known security vulnerabilities and industry best practices?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is only one application or primary function per server in production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are systems configured to only run necessary services?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are vendor-supplied security patches installed within one month of release?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are security patches tested before they are deployed to production systems?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are change control procedures followed for system configuration modification?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does a process exist to identify newly discovered security vulnerabilities applicable to the environment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 7 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 8 User management

2	Do users have an individual username and password that is not shared?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	When an employee leaves the company, is the user account and password immediately revoked?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all user accounts reviewed on a yearly basis to ensure that out-of-date or unknown accounts do not exist?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are accounts that are not used for a pre-defined length of time automatically disabled in the system?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all users uniquely identified before being granted access system and network resources.	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is a unique username and password used to authenticate internal and external users?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is 2-factor (e.g. tokens or certificates) used to authenticate internal and external users?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is biometrics used to authenticate internal and external users?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management control the addition, deletion, and modification of user IDs?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management immediately revokes access of terminated users?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management distributes password policies, procedures and guidelines to users?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management not permit group passwords?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management requires the changing of user passwords ever 90 days?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Does information security management requires the minimum length of at least 7 characters?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does information security management require that passwords not be found in any commonly used dictionary?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does information security management requires password choice to contain at least 1 number and 1 symbol?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does information security management monitors access attempts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does information security management locks out users after repeated failed authentication attempts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 8 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 9 Data encryption

1	Is the cryptographic solution data isolated so that secret data is not disclosed?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does the data encryption conform to applicable international and national standards?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are encryption keys protected against both disclosure and misuse by allowing access to keys by the fewest individuals and storing keys securely in the fewest possible locations?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all key management processes and procedures fully documented?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is confidential data that is transmitted over public networks done in a manner that can only be decrypted by the recipient?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is confidential data always stored in an encrypted form?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	If SSL is used for transmission of data, is it using version 3.0 with 128-bit encryption?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	If wireless access is used, is the communication encrypted?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	If wireless access is used, is network access limited to only know network cards?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are personal modems configured to only allow dial-out connections?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 9 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 10 Disaster recovery

1	Are backups of data on business critical systems made daily?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is at least one backup per week stored at an offsite storage facility?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are restoration tests of backed up data performed on a regular basis?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are data connections highly available?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are firewalls highly available?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are servers (database, application, web, mail, DNS, authentication, etc.) highly available?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there an incident response team in case of a compromise?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 10 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------

Section 11 Development

Note - If your organization does not do internal development, this section may not apply.

Risk Level	Item	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is information security included throughout the development life cycle process?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is your software and application development process based on an industry standard?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is a security assessment and/or penetration test performed on all of your e-commerce applications before they go into production?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is non-production data used for testing and development purposes?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is there a dedicated and separate test environment?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is sensitive information stored in databases encrypted with sufficient strength keys?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are data and communication encryption keys stored in a hardware device or tamper resistant security module?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Does encryption and decryption of data occur within a secure hardware device?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Are key manipulations on the secure hardware device done under dual control?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
2	Is there a separation of duties between the development, production, and test staff?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Is there a separation between the development, production, and test environments?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are all input controls implemented at the server side to prevent the bypassing of client side input controls?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are controls implemented at the server side to prevent SQL injection?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	When authenticating over the Internet, is the application designed to prevent data harvesting by malicious users trying to determine existing user accounts?	Yes <input type="checkbox"/>	No <input type="checkbox"/>
1	Are cookies secured or encrypted?	Yes <input type="checkbox"/>	No <input type="checkbox"/>

Section 11 rating

Level 1 <input type="checkbox"/>	Level 2 <input type="checkbox"/>	Level 3 <input type="checkbox"/>
----------------------------------	----------------------------------	----------------------------------