

AIG netAdvantage[®] Suite

Information Security Self Assessment

Please complete the following informational questions before filling out the assessment. Please note that all fields are required. When you have completed the assessment, please save as a Microsoft Word file and e-mail to: netAdvantageAssessment@aig.com Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.

Primary Contact Information	
Primary Contact First Name	
Primary Contact Last Name	
Email Address	
Job Function	Other (If "Other" please fill in:)
Company	
Industry	Other (If "Other" please fill in:)
Address	
Address 2	
City	
State/Province	
Zip Code	
Country	
Name of Broker (if applicable)	
How many employees does your company have?	1 - 50 employees

Please answer all of the following questions to the best of your knowledge. You may need to refer certain sections of this questionnaire to other managers in your company for completion. For your convenience, next to each section heading we have noted the job function(s) that may be best equipped to answer the questions within that section

For each question, choose an answer of either ‘Yes’ or ‘No’. If ‘Yes’ is selected, please check all of the additional sub points that apply to your company. Please provide any relevant additional information in the space provided.

If there are any questions that you feel are not applicable to your company, please check ‘No’ and explain in the ‘Additional Information’ section at the end of each question. If the topic of any section pertains to a service that your company outsources, please answer the questions to the best of your knowledge and/or fill out the additional information section of the question. Please also enter details on the outsourcer that you use in the vendor management section of this questionnaire.

When you have completed the assessment, please save as a Microsoft Word file and e-mail to: netAdvantageAssessment@aig.com. Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.

Security Organization – (Suggested respondent: CIO, CSO, CTO, Information Security Manager)	
1. What percentage of your total global IT budget is allocated to security?	<p>Please Choose</p> <p>Additional Information:</p>
2. Does your company have an information security infrastructure and organization? <input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> There is an IT security strategy document that details the company’s security function. <input type="checkbox"/> The board of directors or audit committee provides oversight for the security function. <input type="checkbox"/> Information security roles and responsibilities are defined, documented, and address separation of duties (e.g. information security steering committee, security administrators, information owners, etc.). <input type="checkbox"/> A security contact has been designated at each company site or facility. <input type="checkbox"/> The name and contact information for the security contact has been communicated to users.

Additional information:

Security Policy and Standards – (Suggested respondent: CIO, CSO, CTO, Information Security Manager)

<p>3. Is there technical security configuration documentation for the technologies or major business applications in your company?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Technical security configuration documentation exists for:</p> <ul style="list-style-type: none"><input type="checkbox"/> Firewalls<input type="checkbox"/> Routers<input type="checkbox"/> Operating systems (Windows 2000, XP, NT, Mainframe, Unix, etc)<input type="checkbox"/> Infrastructure applications (IIS, Exchange, Websphere, Lotus Notes, Domain Controllers, etc)<input type="checkbox"/> Other major business applications (please list up to five) <p><input type="checkbox"/> Technical security configuration documentation is reviewed at least twice a year and immediately when new security vulnerabilities arise.</p> <p>Additional Information:</p>
<p>4. Does your company have information security policies?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<ul style="list-style-type: none"><input type="checkbox"/> A central person/group maintains, reviews and updates information security policies (i.e. designated security officer, security department, security steering committee.)<input type="checkbox"/> Security policies are reviewed at least annually.<input type="checkbox"/> Security policies are published and made available to all users.<input type="checkbox"/> New users must acknowledge their understanding of security policies.<input type="checkbox"/> Users must reconfirm their acknowledgement of security policies at least annually.<input type="checkbox"/> Users have undergone a security awareness-training program.<input type="checkbox"/> Internal security specialists/administrators receive additional specialized security training on an ongoing basis.

The following areas are addressed in documented security policies:

- Business Continuity Management
- Change Control
- Security Assessment and Compliance
- Computer & Network Management
- Electronic Access Control
- Email Usage and Protection
- Encryption
- Incident Response
- Information Asset Classification and Data Protection
- Internet Usage
- Password Management
- Personnel Security and Hiring Standards
- Physical Access
- Privacy & Confidentiality
- Remote Access
- Security Awareness
- Systems Development & Maintenance
- Vendor/Third Party Management
- Web Application Security
- Virus Protection

Additional Information:

Physical and Environmental Security – (Suggested respondent: Facilities manager, CSO, CIO)

5. Does your company have physical security controls in place?

Yes No

- A security perimeter has been identified and documented, which includes computer rooms, media storage rooms, data centers, etc.
- Biometric access controls are used to access company data center(s).
- Computers are physically secured with lock devices.
- Surveillance cameras and guards are in place to monitor premises.
- Departments and work areas that deal with sensitive information or systems are limited to authorized personnel.
- ID badges are required for employee, visitor and vendor access.
- ID badges are electronically verified for access.
- Computer, media storage and telecom room access is secured and restricted to authorized personnel.
- Cables and network ports are protected from unauthorized access.
- Disposal of computer systems and media storage devices (hard drives, tapes, floppies, CDs, etc) is handled in a secure fashion (i.e. de-magnetization).
- Remote locations have physical security similar to the main location.

Additional Information:

Computer and Network Management – (Suggested respondent: CTO, CIO, CSO, Information Security Manager)

6. Does your company enforce a patch management process?

Yes No

- Vulnerabilities and exploits are monitored and prioritized on a daily basis (i.e. subscriptions to security sites, vendor sites etc.)
- Security patches or workarounds are identified and prioritized on a daily basis.

Highest priority security patches or workarounds are implemented within the following timeframe of identification: Please Choose

	<p>Other security patches or workarounds are implemented within the following timeframe of identification: Please Choose</p> <p><input type="checkbox"/> Patches are tested on non-production systems before they are implemented. <input type="checkbox"/> Implementation of patches is formally documented.</p> <p>Please summarize your patch implementation process:</p> <p>Additional information:</p>
<p>7. Does your company have a virus protection program in place?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Virus protection/detection software is installed and enabled on servers, workstations and laptops. <input type="checkbox"/> Virus definition files are updated on servers, workstations and laptops at least weekly and immediately in the event of an outbreak. <input type="checkbox"/> In the event of an outbreak, the user community is alerted with actions to be taken. <input type="checkbox"/> Email attachments, downloads and other potentially malicious extensions are pre-screened for viruses by network filtering devices</p> <p>Additional information:</p>
<p>8. Are systems in your Internet/DMZ environment secured?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Internet accessible systems are tested for vulnerabilities prior to being placed in production. <input type="checkbox"/> Only services that are required by a specific business need and that have been assessed for their impact on security are enabled. <input type="checkbox"/> All essential protocols (i.e. DNS, LDAP, SMTP, FTP, etc) are securely configured. <input type="checkbox"/> Firewall(s) are configured to ensure source(s), destination(s) and protocol(s) are as specific as possible.</p>

	<input type="checkbox"/> The DMZ architecture is multi-tiered. <input type="checkbox"/> External networks and DMZ servers are monitored 24 x 7 for security violations. Additional information:
9. Are internal systems secured? <input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Applications on internal web servers run in non-privileged mode. <input type="checkbox"/> Host based firewalls are implemented between segregated networks. <input type="checkbox"/> Server performance metrics (CPU, disk, memory, hardware, etc.) are monitored. <input type="checkbox"/> Critical applications residing within the internal networks (and behind the firewall) are monitored 24 x 7 for security violations. <input type="checkbox"/> Systems are scanned for unauthorized software installations. <input type="checkbox"/> Desktop machines, laptops and servers are configured according to your company's technical security configuration standards. <input type="checkbox"/> Password protected screensavers automatically activate after a predetermined period of inactivity. Additional information:
10. Do critical systems receive full security testing before deployment? <input type="checkbox"/> Yes <input type="checkbox"/> No	<input type="checkbox"/> Security vulnerability testing is performed according to a defined and documented methodology. <input type="checkbox"/> Attack and penetration testing is performed by an independent third party. <input type="checkbox"/> Testing for web applications includes checking for session management weaknesses and cross-site scripting vulnerabilities. <input type="checkbox"/> Availability testing is conducted on redundant systems. <input type="checkbox"/> Written results are produced and retained for a minimum of 1 year. Additional information:

Access Control - (Suggested respondent: CIO, CSO, CTO, Information Security Manager)	
<p>11. Do your company's access control procedures address access to sensitive systems, files and directories?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Procedures for access to mission critical systems and sensitive data (e.g. company financial data, customer data, etc.) include user authorization and authentication.</p> <p><input type="checkbox"/> Files stored on servers are protected from unauthorized access or use.</p> <p><input type="checkbox"/> Access to system files and directories is explicitly restricted to authorized IT personnel.</p> <p>Additional information:</p>
<p>12. Does your company enforce a password management process?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Unique username and password for user authentication is required.</p> <p><input type="checkbox"/> Password complexity scheme is in place and is technically enforced where feasible or testing is performed to ensure compliance.</p> <p><input type="checkbox"/> Technology is configured to require users to change passwords at least every 180 days.</p> <p><input type="checkbox"/> Technology is configured to require <u>privileged</u> users to change passwords at least every 90 days.</p> <p><input type="checkbox"/> Passwords cannot be reused for at least 4 changes.</p> <p>Additional information:</p>

<p>13. Are controls in place to secure network access?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> There is a documented process in place to activate new network connections.</p> <p><input type="checkbox"/> Extranet connections are limited and secured (e.g. via firewall rules established as required by a documented business need).</p> <p><input type="checkbox"/> Connections to legacy systems are secured.</p> <p>Additional information:</p>
<p>14. Are connections from laptops, mobile devices, and remote users into the company's network secured?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Advanced authentication controls are in place for remote access.</p> <p><input type="checkbox"/> VPN software is configured to prohibit broad-band users from accessing the corporate network while also accessing the Internet (i.e. split tunnel)</p> <p><input type="checkbox"/> Remote user access is limited to only those applications needed.</p> <p><input type="checkbox"/> Remote users are required to have a personal firewall installed if using a VPN connection to the network.</p> <p>Additional information:</p>
<p>15. Does your company have a process for managing user accounts?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> There is a documented process to approve new accounts and modify user privileges.</p> <p><input type="checkbox"/> User privileges are based upon job function.</p> <p><input type="checkbox"/> User privileges are changed within one week for internal transfers.</p> <p><input type="checkbox"/> User privileges are revoked for terminated users within 2 business days of the termination.</p> <p><input type="checkbox"/> Users are required to verify their identity prior to a password reset.</p> <p><input type="checkbox"/> User privileges are reviewed at least annually.</p> <p>Additional information:</p>

<p>16. Is encryption used to protect sensitive information when it is transmitted over external networks?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Public/private keys are used for the encryption of sensitive information.</p> <p><input type="checkbox"/> 128-bit encryption products (e.g. SSL, RSA) and/or algorithms (e.g. Triple DES) are used.</p> <p><input type="checkbox"/> Database encryption is used for sensitive information (e.g. credit card numbers, social security numbers, etc.).</p> <p><input type="checkbox"/> Passwords are encrypted.</p> <p><input type="checkbox"/> File encryption is used for locally stored materials (e.g. on laptops, etc.)</p> <p>Additional information:</p>
<p>17. Do your company's policies address access to data based on a data classification scheme?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Data classification policies are based on risk assessments.</p> <p><input type="checkbox"/> Data protection requirements are defined and documented.</p> <p><input type="checkbox"/> Information owners are responsible for the protection of the data they own.</p> <p>Additional information:</p>

<p>System Development and Maintenance – (Suggested respondent: Development Manager, CIO, CSO, CTO, Information Security Manager)</p>	
<p>18. When a new system is developed or purchased, are security considerations taken into account?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Security requirements are an integral part of new project plans.</p> <p><input type="checkbox"/> Security is defined within the system architecture.</p> <p><input type="checkbox"/> Security coding standards for your company are defined (e.g. global variables are not used).</p> <p><input type="checkbox"/> A security expert is involved in new projects.</p> <p>Additional information:</p>

<p>19. Are staging, test, and development systems kept separate from production systems?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<ul style="list-style-type: none"><input type="checkbox"/> There is no sharing of databases and configuration files.<input type="checkbox"/> There is no sharing of accounts.<input type="checkbox"/> Developers do not have access to production.<input type="checkbox"/> Staging, test and development systems are in separate environments (i.e. separate segments, separate servers)<input type="checkbox"/> Development tools, including compilers and linkers, are not installed on production systems. <p>Additional information:</p>
<p>20. Does your company perform configuration management?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<ul style="list-style-type: none"><input type="checkbox"/> Software products are used to maintain version control and restrict access to programming libraries.<input type="checkbox"/> There is a documented process to review and approve changes to code.<input type="checkbox"/> Modifications made by individuals to code are tracked.<input type="checkbox"/> The development system has the ability to back out changes.<input type="checkbox"/> The development system is protected by appropriate security measures.<input type="checkbox"/> Developers do not have the ability to migrate code to production.<input type="checkbox"/> Change control procedures are documented.<input type="checkbox"/> Management reviews documentation of emergency changes. <p>Additional information:</p>
<p>21. Are new applications and non-cosmetic changes reviewed for security vulnerabilities prior to migration to production?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<ul style="list-style-type: none"><input type="checkbox"/> Code reviews are performed by an independent individual or third party.<input type="checkbox"/> The impact of changes to security is documented.<input type="checkbox"/> Assessments of applications are performed according to a defined procedure, which includes security guidelines.<input type="checkbox"/> Security assessments of applications are performed with automated scanning tools and manual techniques as appropriate.<input type="checkbox"/> A report documents assessment findings.<input type="checkbox"/> Data input testing standards are defined (e.g. buffer overflow check).

Additional information:

Compliance – (Suggested respondent: Compliance Officer, CIO, CSO, Information Security)

22. Does your company have a program in place to periodically test security controls?
(NOTE: This can include internal audits, external audits or security consulting engagements.)

Yes No

Security assessments are based on a risk evaluation and are performed at least once a year.

Security assessment processes and methodologies are documented.

Access to security assessment tools and utilities and the directories where they are stored are restricted to authorized personnel

Security assessments include the use of :

Outside security specialists to perform penetration testing

Automated vulnerability scanners

Policy compliance checking tools (e.g. eTrust)

Secure configuration checkers

Performance tools

Modem Sweeps

Source code comparison tools.

Security policies and controls are subject to independent reviews and audits.

All high risk vulnerabilities are remediated within 1 month.

All medium risk vulnerabilities are remediated within 3 months.

Additional information:

<p>23. Do you maintain system logs?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>System logs are maintained for the following:</p> <p><input type="checkbox"/> Internet connections</p> <p><input type="checkbox"/> Access attempts</p> <p><input type="checkbox"/> Critical Applications</p> <p><input type="checkbox"/> Internal network devices (e.g., firewalls, routers, IDS, etc.)</p> <p><input type="checkbox"/> Logs are stored securely in a central location.</p> <p><input type="checkbox"/> A copy of the logs is stored off site for at least 90 days.</p> <p>Additional information:</p>
<p>24. Are system logs reviewed for security related events?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>System log reviews:</p> <p><input type="checkbox"/> Occur at least daily</p> <p><input type="checkbox"/> Use automated tools</p> <p><input type="checkbox"/> Are performed by trained personnel</p> <p><input type="checkbox"/> System clocks are synchronized with a trusted time server.</p> <p>Additional information:</p>

<p>Vendor Management – (Suggested respondent: General Counsel, CIO, CTO, Contracts Manager)</p>	
<p>25. Does your company enforce security standards for third parties that connect to your network?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p><input type="checkbox"/> Requests for third party connectivity must be reviewed and approved by your management.</p> <p><input type="checkbox"/> Technical risk assessments are performed on third parties that request access.</p> <p><input type="checkbox"/> Third party connections are monitored for security events.</p>

Additional information:	
26. Do third party contracts include security provisions? <input type="checkbox"/> Yes <input type="checkbox"/> No	Third party contracts include: <input type="checkbox"/> A service level agreement that specifies security requirements and responsibilities <input type="checkbox"/> Provisions for compliance with applicable regulations (e.g., GLBA, HIPAA, Basel II, etc.) <input type="checkbox"/> A right to audit clause <input type="checkbox"/> Procedures for escalating security related events Additional information:
27. Does your company outsource any portion of your information security? <input type="checkbox"/> Yes <input type="checkbox"/> No	Please provide the name(s) of outsourced security vendor in each area: Access Control: Business Continuity: Computer and Network Management: Compliance: Physical and Environmental Security: Systems Development and Maintenance: Security Organization: Security Policy and Standards: Additional information:

Business Continuity – (Suggested respondent: CIO, CTO, CSO, Information Security Manager)	
<p>28. Does your company have backup and restore procedures in place?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Backup and restore procedures are:</p> <p><input type="checkbox"/> Documented</p> <p><input type="checkbox"/> Tested annually to ensure their effectiveness</p> <p><input type="checkbox"/> Performed by trained personnel</p> <p>Backup tapes/disks are:</p> <p><input type="checkbox"/> Made at least once a week</p> <p><input type="checkbox"/> Kept for a minimum of 90 days</p> <p><input type="checkbox"/> Stored in fire proof safes</p> <p><input type="checkbox"/> Rotated off site for storage</p> <p><input type="checkbox"/> Retired once their lifespan has been reached</p> <p>Additional information:</p>
<p>29. Does your company have a Business Continuity Plan (BCP)?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>The Business Continuity Plan:</p> <p><input type="checkbox"/> Is managed by a dedicated group</p> <p><input type="checkbox"/> Is formally documented</p> <p><input type="checkbox"/> Is tested on an annual basis</p> <p><input type="checkbox"/> Addresses every department</p> <p><input type="checkbox"/> Users are trained on their BCP responsibilities.</p> <p><input type="checkbox"/> A “hot site” is in place.</p> <p><input type="checkbox"/> Redundant systems are in place.</p> <p><input type="checkbox"/> Hardware vendors are contracted to provide replacement systems.</p> <p>Additional information:</p>

Financial Management of Network Security Losses – (Suggested respondent: CFO, CIO)		
<p>30. Security breaches cause unexpected financial losses. Has your company planned for the funding of such expenses?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Funding is available via:</p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p><input type="checkbox"/></p> <p>Additional information:</p>	<p>Cash on hand</p> <p>A loss reserve</p> <p>Available credit</p> <p>Network Security Insurance</p> <p>Other Insurance</p>
<p>31. Does your company require all vendors to maintain liability insurance?</p> <p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>	<p>Liability insurance includes the following:</p> <p><input type="checkbox"/> Limits of at least \$1,000,000.</p> <p><input type="checkbox"/> Loss arising from vendor negligence.</p> <p><input type="checkbox"/> Loss arising from a breach of security (including data corruption, business interruption, etc.)</p> <p>Additional information:</p>	

When you have completed the assessment, please save as a Microsoft Word file and e-mail to:
netAdvantageAssessment@aig.com

Your assessment will be reviewed by an AIG IT-Security analyst, and you will receive the results of your assessment via return e-mail. The results will be password protected and the password will be communicated separately via email.