

# Best Security Practices for the Gramm-Leach-Bliley Act (Section 314) *matrix*



**ISS Solutions for Security Best Practices for the Gramm-Leach-Bliley Act  
Part 314 of the Gramm-Leach-Bliley Act—Standards for safeguarding customer information.**

**Section 314.3 Standards for safeguarding customer information.**

Gramm-Leach-Bliley Requirement	Description	ISS Program Phase	ISS Solutions to Achieve Gramm-Leach-Bliley Compliance
Section 314.3 (a) Information security program.	<p>You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.</p> <p>Such safeguards shall include the elements set forth in Section 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.</p>	Design	<p><b>Professional Security Services (PSS):</b></p> <ul style="list-style-type: none"> <li>• Collaborative Business Case Assessment</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for Gramm-Leach-Bliley</li> <li>• ISO-17799 Gap Analysis</li> <li>• Security Strategy Workshop</li> <li>• Documentation</li> </ul>
Section 314.3 (b) Define objectives.	<p>(1) Insure the security and confidentiality of customer information;</p> <p>(2) Protect against any anticipated threats or hazards to the security or integrity of such information; and</p> <p>(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.</p>	Assess and Design	<p><b>Professional Security Services (PSS):</b></p> <ul style="list-style-type: none"> <li>• Collaborative Business Case Assessment</li> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Penetration Test</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for Gramm-Leach-Bliley</li> <li>• ISO-17799 Gap Analysis</li> <li>• Security Strategy Workshop</li> <li>• Documentation</li> </ul>

## Section 314.4 Elements

Gramm-Leach-Bliley Requirement	Description	ISS Program Phase	ISS Solutions to Achieve Gramm-Leach-Bliley Compliance
Section 314.4 (a) Designate an employee or employees to coordinate your information security program.	In order to develop, implement, and maintain your information security program.	Design	<b>Professional Security Services (PSS):</b> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for Gramm-Leach-Bliley</li> <li>• Security Strategy Workshop</li> <li>• Documentation</li> </ul>
Section 314.4 (b) Identify reasonably foreseeable internal and external risks	Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including: <ol style="list-style-type: none"> <li>(1) Employee training and management;</li> <li>(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and</li> <li>(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.</li> </ol>	Assess and Design	<b>Professional Security Services (PSS):</b> <ul style="list-style-type: none"> <li>• Collaborative Business Case Assessment</li> <li>• Information, Policy, Application and Vulnerability Security Assessments</li> <li>• Penetration Test</li> <li>• Network Architecture Design</li> <li>• Security Strategy Workshops</li> <li>• Gramm-Leach-Bliley Act Gap Analysis</li> <li>• Gramm-Leach-Bliley Act Quick Start Program</li> <li>• Policy and Procedures Design</li> <li>• Best Practices for Gramm-Leach-Bliley</li> <li>• Documentation</li> </ul> <b>X-Force® Education Services</b>
Section 314.4 (c) Design and implement information safeguards.	Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.	Deploy  Manage and Support	<b>Proventia™ Integrated Security Appliances</b> Single, all-in-one protection for networks, servers and desktops combining: <ul style="list-style-type: none"> <li>• Stateful Inspection Firewall</li> <li>• VPN</li> <li>• Antivirus</li> <li>• Intrusion Detection and Prevention</li> <li>• Content Filtering</li> <li>• Anti-spam</li> <li>• Application Protection</li> </ul>

			<p><b>SiteProtector™</b></p> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul>
Section 314.4 (d) Oversee service providers	Oversee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.	Design  Manage and Support	<p><b>Professional Security Services (PSS):</b></p> <ul style="list-style-type: none"> <li>• Policy and Procedures Design</li> <li>• Best Practices for Gramm-Leach-Bliley</li> <li>• Documentation</li> </ul> <p><b>Managed Services:</b></p> <ul style="list-style-type: none"> <li>• Managed Protection Services</li> <li>• Managed Firewall Service</li> <li>• Managed Intrusion Detection and Prevention Services</li> <li>• Vulnerability Management</li> <li>• Customer Portal</li> </ul>
Section 314.4 (e) Evaluate and adjust information security program	(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.		

#### 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