DATA SHEET

Total Security Management GLBA Compliance Guide

The Gramm-Leach-Bliley Act (also known as the Financial Services Modernization Act of 1999) requires any financial institutions that offer loans, financial advice, and insurance to regulate the protection of private information between clients and customers. Following the FFIEC IT Examination Handbook guidelines, RackFoundry TSM provides you with regular GLBA Compliance Reports to ensure that you pass your next audit and avoid any penalties. You can utilize our File Integrity Monitoring and Log Management tools to monitor access to private consumer information as well as user activity. Additionally, GLBA compliance mode automatically detects if any threat is directly related to this compliance and issues a critical alert. With all of these tools included, you can rest easy knowing that your network security is well protected. Below is a table that explains, in detail, how RackFoundry TSM can help you meet each relevant GLBA objective:

Tier 1	Example of how RackFoundry TSM Helps
Objective 6. Determine the Adequacy of Security Monitory	
1.6.1 Obtain an understanding of the institution's monitoring plans and activities, including both activity monitoring and condition monitoring. *Activity monitoring consists of host and network data gathering, and analysis.	RackFoundry TSM provides real-time monitoring of host and network data and correlates events to detect security threats.
1.6.2 Identify the organizational unit and personnel responsible for performing the functions of a security response center.	RackFoundry TSM automates many of the functions of a security response center, providing actionable alerts and reports to simplify the remediation process.

Tier 1	Example of how RackFoundry TSM Helps
	RackFoundry TSM's SOC provides 24/7/365 monitoring and utilizes proven methods to classify threats, escalate if necessary, and respond accordingly.
1.6.3 Evaluate the adequacy of information used by the security response center. Information should include external information on threats and vulnerabilities (ISAC and other reports) and internal information related to controls and activities.	RackFoundry TSM includes an internal Vulnerability Scanner as well as external Penetration Testing.
1.6.4 Obtain and evaluate the policies governing security response center functions, including monitoring, classification, escalation, and reporting.	RackFoundry TSM automates many of the functions of a security response center, providing actionable alerts and reports to simplify the remediation process. RackFoundry TSM's SOC provides 24/7/365 monitoring and utilizes proven methods to classify threats, escalate if necessary, and respond accordingly.
1.6.7 Ensure that the institution utilizes sufficient expertise to perform its monitoring and testing.	RackFoundry's SOC is staffed only with trained, RackFoundry Certified Security Analysts.
1.6.1 Obtain an understanding of the institution's monitoring plans and activities, including both activity monitoring and condition monitoring. *Activity monitoring consists of host and network data gathering, and analysis.	RackFoundry TSM provides real-time monitoring of host and network data and correlates events to detect security threats.
1.6.2 Identify the organizational unit and personnel responsible for performing the functions of a security response center.	RackFoundry TSM automates many of the functions of a security response center, providing actionable alerts and reports to simplify the remediation process. RackFoundry TSM's SOC provides 24/7/365 monitoring and utilizes proven methods to classify threats, escalate if necessary, and respond accordingly.
1.6.3 Evaluate the adequacy of information used by the security response center. Information should include external information on threats and vulnerabilities (ISAC and other reports) and internal information related to controls and activities.	RackFoundry TSM includes an internal Vulnerability Scanner as well as external Penetration Testing.
Objective 7. Evaluate the effectiveness of enterprise-wide security administration	
1.7.2 Determine whether management and department heads are adequately trained and sufficiently accountable for the security of their personnel, information, and systems.	RackFoundry provides training for the RackFoundry TSM solution. RackFoundry's SOC is staffed only with trained, RackFoundry Certified Security Analysts.
1.7.7 Evaluate the adequacy of automated tools to support secure configuration management, security monitoring, policy monitoring, enforcement, and reporting.	RackFoundry TSM is a proveny enterprise grade security monitoring tool that alerts on configuration and policy changes and provides comprehensive reports.
A. Access Rights Administration	

Tier 1	Example of how RackFoundry TSM Helps
2.A.4 Determine that administrator or root privilege access is appropriately monitored, where appropriate. Management may choose to further categorize types of administrator/root access based upon a risk assessment. Categorizing this type of access can be used to identify and monitor higher-risk administrator and root access requests that should be promptly reported.	RackFoundry TSM monitors account management and usage activity by regulating the creation of privileged accounts and overseeing privileged changes.
A. Authentication	
2.A.2 Determine whether access to system administrator level is adequately controlled and monitored.	RackFoundry TSM monitors account management and account usage activity by regulating the creation of privileged accounts and overseeing privileged changes.
2.A.4 Evaluate the effectiveness of password and shared-secret administration for employees and customers considering the complexity of the processing environment and type of information accessed. Consider • Confidentiality of passwords and shared secrets (whether only known to the employee/customer); • Maintenance of confidentiality through reset procedures; • The frequency of required changes (for applications, the user should make any changes from the initial password issued on enrollment without any other user's intervention); • Password composition in terms of length and type of characters (new or changed passwords should result in a password whose strength and reuse agrees with the security policy); • The strength of shared secret authentication mechanisms; • Restrictions on duplicate shared secrets among users (no restrictions should exist); and • The extent of authorized access (e.g., privileged access, single sign-on systems).	RackFoundry TSM's Vulnerability Scanner is able to detect weak passwords.
B. Network Security	
2.B.1 Evaluate the adequacy and accuracy of the network architecture. • Obtain a schematic overview of the financial institution's network architecture. • Review procedures for maintaining current information, including inventory reporting of how new hardware are added and old hardware is removed. • Review audit and security reports that assess the accuracy of network architecture schematics and identify unreported systems.	RackFoundry offers Architecture Reviews to review procedures for maintaining information and ensure best practices are utilized.
2.B.12 Determine whether logs of security-related events and log analysis activities are sufficient to affix	RackFoundry TSM aggregates and correlates logs from your Firewalls, IPS/IDS systems, and various network

Tier 1	Example of how RackFoundry TSM Helps
accountability for network activities, as well as support intrusion forensics and IDS. Additionally, determine that adequate clock synchronization takes place.	devices utilizing threat intelligence feeds to detect security threats and provide actionable alerts and reports. RackFoundry TSM accurately and automatically synchronizes audit log time stamps to the absolute time standard (GMT) to ensure the true time is maintained.
2.B.13 Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected. Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.	RackFoundry TSM maintains a strong audit trail by storing logs and events in a secure repository that are protected against unauthorized access, change, and deletion. RackFoundry TSM archives logs for adequate time periods.
2.B.17 Determine whether remote access devices and network access points for remote equipment are appropriately controlled. • Remote access is disabled by default, and enabled only by management authorization. • Management authorization is required for each user who accesses sensitive components or data remotely. • Authentication is of appropriate strength (e.g., two factor for sensitive components). • Modems are authorized, configured, and managed to appropriately mitigate risks. • Appropriate logging and monitoring takes place. • Remote access devices are appropriately secured and controlled by the institution.	RackFoundry TSM monitors remote access activity for VPN, SSH, telnet, etc. and monitors network activity to detect unauthorized communications.
C. Host Security	
2.C.3 Determine whether adequate processes exist to apply host security updates, such as patches and anti-virus signatures, and that such updating takes place.	RackFoundry TSM includes a Vulnerability Scanner to detect areas that need patches.
2.C.4 Determine whether new hosts are prepared according to documented procedures for secure configuration or replication, and that vulnerability testing takes place prior to deployment.	RackFoundry's Vulnerability Scanner can be used to scan hosts before deployment.
2.C.7 Determine whether access to utilities on the host are appropriately restricted and monitored.	RackFoundry TSM has File Integrity Monitoring that can detect unauthorized access to utilities on the host. RackFoundry TSM pulls audit logs from the host to review access to utilities.
2.C.8 Determine whether the host-based IDSs identified as necessary in the risk assessment are properly installed and configured, that alerts go to appropriate individuals using an	RackFoundry TSM includes a HIDS agent that is installed on the host and reports back to the TSM solution to provide alerts.

Tier 1	Example of how RackFoundry TSM Helps
out-of-band communications mechanism, and that alerts are followed up.	RackFoundry TSM's alerts can be configured to be sent to the appropriate individuals based on threat category, severity, etc.
2.C.9 Determine whether logs are sufficient to affix accountability for host activities and to support intrusion forensics and IDS and are appropriately secured for a sufficient time period.	RackFoundry TSM maintains a strong audit trail by storing logs and events in a secure repository that is protected against unauthorized access, change, and deletion.
2.C.10 Determine whether vulnerability testing takes place after each configuration change.	RackFoundry TSM automatically detects configuration changes and includes a Vulnerability Scanner.
G. Application Security	
2.G.4 Determine whether access to sensitive information and processes require appropriate authentication and verification of authorized use before access is granted.	RackFoundry TSM monitors access to sensitive information and alerts users of unauthorized access.
2.G.8 Determine whether appropriate logs are maintained and available to support incident detection and response efforts.	RackFoundry TSM stores logs and events in a secure repository that is protected against unauthorized access, change, and deletion.
H. Software Development and Acquisition	
2.H.4 Evaluate whether the software acquired incorporates appropriate security controls, audit trails, and activity logs and that appropriate and timely audit trail and log reviews and alerts can take place.	RackFoundry TSM ingests logs from custom and commercial applications, generates alerts and reports, and keeps an audit trail.
M. Security Monitoring	
2.M.1 Identify the monitoring performed to identify noncompliance with institution security policies and potential intrusions. • Review the schematic of the information technology systems for common security monitoring devices. • Review security procedures for report monitoring to identify unauthorized or unusual activities. • Review management's self-assessment and independent testing activities and plans.	RackFoundry TSM provides real-time, continuous monitoring and alerting for network devices (firewalls, IPS/IDS, servers, switches, routers, workstations, wireless devices, etc.)
2.M.2 Determine whether users are appropriately notified regarding security monitoring.	RackFoundry TSM utilizes policies to determine the appropriate users to notify for different security threats, based on threat category, severity, location, etc.
2.M.3 Determine whether the activity monitoring sensors identified as necessary in the risk assessment process are properly installed and configured at appropriate locations.	RackFoundry Security Engineers assist with the installation and configuration of RackFoundry TSM sensors to ensure they are deployed properly.
2.M.5 Determine whether logs of security-related events are sufficient to support security incident detection and response activities, and that logs of application, host, and network activity can be readily correlated.	RackFoundry TSM ingests logs from applications, hosts, and network traffic and correlates events using multiple threat intelligence feeds to detect security incidents.

Tier 1	Example of how RackFoundry TSM Helps
2.M.6 Determine whether logs of security-related events are appropriately secured against unauthorized access, change, and deletion for an adequate time period, and that reporting to those logs is adequately protected.	RackFoundry TSM stores logs and events in a secure repository that is protected against unauthorized access, change, and deletion.
2.M.7 Determine whether logs are appropriately centralized and normalized, and that controls are in place and functioning to prevent time gaps in logging.	RackFoundry TSM accurately and automatically synchronizes audit log time stamps to the absolute time standard (GMT) to ensure the true time is maintained.
2.M.8 Determine whether an appropriate process exists to authorize employee access to security monitoring and event management systems and that authentication and authorization controls appropriately limit access to and control the access of authorized individuals.	RackFoundry TSM utilizes access controls to restrict users to defined sets of log/event data and ensure they only have access to authorized data.
2.M.9 Determine whether appropriate detection capabilities exist related to: • Network related anomalies, including - Blocked outbound traffic - Unusual communications, including communicating hosts, times of day, protocols, and other header-related anomalies - Unusual or malicious packet payloads • Host-related anomalies, including - System resource usage and anomalies - User related anomalies - Operating and tool configuration anomalies - File and data integrity problems - Anti-virus, anti-spyware, and other malware identification alerts - Unauthorized access - Privileged access	RackFoundry TSM provides real-time, continuous monitoring and alerting for network devices (firewalls, IPS/IDS, servers, switches, routers, workstations, wireless devices, etc.) and alerts users of unusual network behavior such as blocked outbound traffic, unusual packet payloads, and activity at an unusual time of the day. RackFoundry TSM monitors user and host activity to detect anomalies including file changes, configuration changes, and unauthorized access. RackFoundry TSM ingests logs from applications, hosts, network traffic, and other network devices and correlates events using multiple threat intelligence feeds to detect security incidents.

RackFoundry TSM is a comprehensive security monitoring solution that combines real-time threat intelligence with continuous monitoring and intrusion prevention capabilities. Along with assistance from RackFoundry's two Security Operations Centers (SOC), RackFoundry TSM provides the essential tools to achieve and maintain GLBA compliance.

About RackFoundry

RackFoundry, the maker of Total Security Management (TSM), is a leader in complete coverage security appliances, secure cloud services and professional services such as SecurityXpert that provides security expertise to organizations of all sizes and industries. The RackFoundry security team, FortressLabs™, help find new vulnerabilities in the wild, mitigate any found vulnerabilities, and head up the RackFoundry Security Operations Center.

For more information visit us at www.rackfoundry.com.