Technical White Paper: 2023

Compliance with Gramm-Leach-Bliley Act (GLBA)

VMware Cloud on AWS

Table of contents

Introduction to Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) is a federal law that governs the financial services industry. In simple terms, the GLBA made several legislative changes, including requiring financial institutions to take measures to protect the personal financial information of their customers, and to provide customers with information about how their personal financial information is collected, used and shared.

The GLBA's privacy provisions note above cab be categorized in three main groups: the Financial Privacy Rule, the Safeguards Rule and the Pretexting Provisions. The Financial Privacy Rule requires financial institutions to inform customers about their information-handling practices and to provide customers with the opportunity to opt out of having their information shared with non-affiliated third parties. The Safeguards Rule requires financial institutions to implement appropriate security measures to protect personal financial information from unauthorized access, use or disclosure. The Pretexting Provisions prohibit pretexting and require financial institutions to take steps to protect their customers' personal financial information from pretexting.

Financial Privacy Rule and Pretexting Rule do not apply to VMware Cloud™ on AWS and are outside the scope of this paper.

FTC Safeguards Rules

The FTC Safeguards Rule, which is found in the GLBA, requires financial institutions to have measures in place to ensure the security and confidentiality of customer information. The rule applies to any company that is considered a financial institution under the GLBA, including banks, securities firms and insurance companies.

To comply with the Safeguards Rule, financial institutions must design and implement a comprehensive information security program that includes administrative, technical and physical safeguards to protect customer information. This may include measures such as:

- Dedicated employees to manage the safeguards
- A thorough risk analysis on every department handling the nonpublic information
- Plan, develop, monitor and test a program to secure the information
- Implement and keep updating security measures in accordance with current trends in data collection, storage and utilization

How VMware Cloud on AWS supports FTC Safeguards Rules compliance

VMware Cloud on AWS (VMC) is a managed service that allows customers to run their workloads on VMware's software-defined data center (SDDC) on Amazon Web Services (AWS) infrastructure. It provides customers with the ability to run their applications in a consistent and secure environment, regardless of where their data is stored.

Jointly engineered by VMware and AWS, this on-demand, scalable Infrastructure as a Service (IaaS) enables IT teams to seamlessly extend, migrate, protect and manage their cloud-based resources with familiar VMware tools. With the same architecture and operational experience on-premises and in the cloud, IT teams can now quickly derive instant value through the AWS and VMware hybrid cloud experience while meeting the most stringent security and compliance requirements including GLBA.

VMware Cloud on AWS can support compliance with the Gramm-Leach-Bliley Act (GLBA) by providing customers with the necessary security controls to protect personal financial information. These features include:

- Access controls to limit who can view customer data
- Encryption to protect customer data in transit and at rest
- Regular risk assessments to identify potential vulnerabilities
- Incident response plans to address security breaches
- Compliance reporting and audit trails
- Training modules for employees

In the table below we describe how VMware Cloud on AWS has controls in place to support GLBA requirements.

GLBA Requirement	VMware Control
Employee training and management	VMware employs security and privacy experts throughout the company including our legal and compliance teams, information security organization, VMware Security Engineering, Communications & Response group (vSECR), VMware Security Incident Response Team (vSIRT), and our security operations center (SOC). These teams collectively work together to build programs, policies, and practices to help identify, prevent and remediate security vulnerabilities in our products and services. These programs are continuously reviewed and evolve based on our experiences, changes in the threat landscape, and industry observation and collaboration. The VMware Software Development Lifecycle is described in the VMware Product Security Whitepaper. VMware has also developed service operations practices following industry best-practices including regular risk assessments, privacy reviews, intrusion and threat detection, user access reviews, continuous security monitoring and third-party vulnerability, security and compliance audits. All VMware employees, including those who may handle personal data that customers provide to VMware as a processor or controller, have signed confidentiality agreements, receive regular training on security and are required to follow code of conduct and data handling policies.
Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall: 1. Retain responsibility for compliance with this part; 2. Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and 3. Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.	

GLBA Requirement	VMware Control
Risk management	In alignment with the ISO 27001 standard, VMware maintains a Risk Management program to mitigate and manage risk companywide. Risk assessments are performed at least annually to ensure appropriate controls are in place to reduce the risk related to the confidentiality, integrity and availability of sensitive information. VMware Cloud on AWS management has a strategic business plan which includes risk identification and the implementation of controls to mitigate or manage risks. VMware Cloud on AWS management reevaluates the strategic business plan at least biannually. This process requires management to identify risks within its areas of responsibility and to implement appropriate measures designed to address those risks. Executive and senior leadership, led by the VMware Chief Information Security Officer, play important roles in establishing the Company's tone and values as it relates to information security. The Information Security and Compliance teams, together with management, are responsible for maintaining awareness and complying with security policies. Business Conduct Guidelines and Security Awareness training is required for employees both upon hire and annually. VMware provides security policies and security training to employees to educate them about their role and responsibilities concerning information security. Employees who violate VMware standards or protocols are subject to appropriate disciplinary action. Applicable security provisions are added to supplier agreements to ensure providers are contractually obligated to maintain appropriate security provisions. These policies are reviewed as part of the VMware audit and assessment program. VMware third-party auditors also perform reviews against industry standards, including ISO 27001. VMware has documented security baselines to guide personnel in ensuring that appropriate configurations are in place to protect sensitive information. Baseline configurations for all software and hardware installed in the production environment are documented and updated regularly. Changes are governed by a defined change management policy, with baseline configurations securely recorded.
(b) Base your information security program on a risk assessment that identifies 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 assesses the sufficiency of any safeguards in place to control these risks. 1. The risk assessment shall be written and shall include: – (i) Criteria for the evaluation and categorization of identified security risks or threats you face; – (ii) Criteria for the assessment of the confidentiality, integrity and availability of your information systems and customer information, including the adequacy of the existing controls in the context of the identified risks or threats you face; and – (iii) Requirements describing how identified risks will be mitigated or accepted based on the risk assessment and how the information security program will address the risks 2. You shall periodically perform additional risk assessments that reexamine the 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 reassess the sufficiency of any safeguards in place to control these risks.	

GLBA Requirement	VMware Control
Risk management	VMware has a formal risk management process which includes identification and monitoring of risks. All risks are documented into a risk register which is reviewed regularly by the security and compliance teams and any actions needed are followed up through to closure.
(c) Design and implement safeguards to control the risks you identity through risk assessment, including by: 1. Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to: – (i) Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and – (ii) Limit authorized users' access only to customer information that they need to perform their duties and functions, or, in the case of customers, to access their own information; 2. Identify and manage the data, personnel, devices, systems and facilities that enable you to achieve business purposes in accordance with their relative importance to business objectives and your risk strategy; 3. Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer information using effective alternative compensating controls reviewed and approved by your Qualified Individual; 4. Adopt secure development practices for in-house developed applications utilized by you for transmitting, accessing or storing customer information and procedures for evaluating, assessing or testing the security of externally developed applications you utilize to transmit, access or store customer information; 5. Implement multi-factor authentication for any individual accessing any information system, unless your Qualified Individual has approved in writing the use of reasonably equivalent or more secure access controls; 6. (i) Develop, implement and maintain procedures for the secure disposal of customer information in any format no later than two years after the last date the information is used in connection with the provision of a product or service to the customer to which it relates, unless such information is necessary for business operations or for other legitimate business purposes, is otherwise required to be retained by law or regulation or where targeted disposal is not reasonably feasible due to the manner in which the information is maintained; and – (ii) Periodically review your data retention policy to minimize the unnecessary retention of data; 7. Adopt procedures for change management; and 8. Implement policies, procedures and controls designed to monitor and log the activity of authorized users and detect unauthorized access or use of, or tampering with, customer information by such users.	

GLBA Requirement	VMware Control
Risk assessment	VMware has a formal risk management process which includes identification and monitoring of risks. All risks are documented into a risk register which is reviewed regularly by the security and compliance teams and any actions needed are followed up through to closure.
1. Regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems and procedures, including those to detect actual and attempted attacks on, or intrusions into, information systems. 2. For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, you shall conduct: – (i) Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and – (ii) Vulnerability assessments, including any systemic scans or reviews of information systems reasonably designed to identify publicly known security vulnerabilities in your information systems based on the risk assessment, at least every six months; and whenever there are material changes to your operations or business arrangements; and whenever there are circumstances you know or have reason to know may have a material impact on your information security program	

GLBA Requirement	VMware Control
Risk assessment	**Providing security awareness training:** VMware offers various optional and mandatory training and certification programs, including a mandatory annual training for all personnel, to help personnel stay up-to-date on the latest security risks and best practices and ensure that personnel are able to enact VMware's information security program. VMware also provides a wide range of resources, such as whitepapers, documentation and webinars, to educate customers and partners on security best practices. **Utilizing qualified information security personnel:** VMC on AWS has a team of dedicated security personnel who are responsible for managing and overseeing the information security program. Additionally, VMware works with independent auditors to regularly assess and audit the security of the VMC on AWS platform. **Providing security updates and training:** VMware provides regular security updates and patches to the VMC on AWS platform to address relevant security risks. VMware also provides access to security resources, including the VMware Security Advisories and the VMware Security Blog, to help customers stay informed about potential security threats. **Verifying key personnel knowledge:** VMware ensures that its security personnel are knowledgeable about changing security threats and countermeasures by providing ongoing training and certification programs. Additionally, VMware has implemented a process for customers to report security vulnerabilities and incidents, allowing for continuous monitoring and improvement of the VMC on AWS platform's security posture.
(e) Implement policies and procedures to ensure that personnel are able to enact your information security program by: 1. Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment; 2. Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program; 3. Providing information security personnel with security updates and training sufficient to address relevant security risks; and 4. Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.	

GLBA Requirement	VMware Control
Vendor management	VMware has a formal vendor on-boarding process. VMware conducts a security risk assessment on third parties that may have access to VMware's non-public information prior to working with VMware. Based on risk and business impact, periodic reviews and/or audits are conducted where there is determined to be a change to the third party profile. VMware monitors, reviews and audits third party service delivery to ensure alignment with agreed level of information security and service delivery in line with the third party agreement. Based on risk and business impact, changes to the provision of services by the third party will be appropriately managed. VMware manages third party relationships and address any deficiencies in the third party's capabilities to securely deliver the services. Based on the risk and business impact VMware request suppliers to complete third party security questionnaires if not already on file or not updated within the past 12 months. VMware Cloud provides several controls to help organizations comply with this requirement of GLBA. Firstly, VMware Cloud provides the ability to conduct regular risk assessments to identify potential security threats and vulnerabilities. This helps organizations to evaluate their information security program and adjust it in response to the results of the risk assessments. Secondly, VMware Cloud provides various monitoring and logging capabilities to detect and respond to security incidents. This includes monitoring of system logs, network traffic and other events to identify potential security breaches. VMware Cloud also provides alerts and notifications to inform security personnel of any suspicious activity. Thirdly, VMware Cloud provides the ability to implement security controls such as firewalls, intrusion detection and prevention systems and access controls to protect sensitive information. Organizations can adjust these controls based on the results of testing and monitoring and any material changes to their operations or business arrangements. In summary, VMware Cloud provides various controls that help organizations to evaluate and adjust their information security program in response to the results of testing and monitoring, as well as any material changes to their operations or business arrangements, which is a requirement of GLBA.
(f) 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; 2. Requiring your service providers by contract to implement and maintain such safeguards; and 3. Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards. (g) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (d) of this section; any material changes to your operations or business arrangements; the results of risk assessments performed under paragraph (b)(2) of this section; or any other circumstances that you know or have reason to know may have a material impact on your information security program.	

GLBA Requirement	VMware Control
Incident response	The VMware Security Incident Response Team (vSIRT) is responsible for developing breach handling procedures, forensics and they handle incident management across VMware. The vSIRT team is notified by the Security Operations Center of any potential breach and participates in any investigation. If VMware becomes aware of a security incident on VMware Cloud on AWS, VMware that leads to the unlawful disclosure or access to personal information provided to VMware as a processor, we will notify customers without undue delay and will provide information relating to a data breach as reasonably requested by our customers. VMware will use reasonable endeavors to assist customers in mitigating, where possible, the adverse effects of any personal data breach. VMware Cloud on AWS backs up Account Information including system configuration settings, but does not provide data backup or archive services for Customer Content. In the event of a customer data breach, VMware will not relocate, replicate, archive or copy Customer Content. VMware Cloud on AWS does not provide customer SDDC administration services, but provides customers self-service administrative tools to remediate and/or isolate their virtual machines, physical hosts and/or SDDCs as required to secure their Customer Content. The Incident response program, plans and procedures are documented and implemented. If VMware becomes aware of a security incident on VMware Cloud on AWS, VMware that leads to the unlawful disclosure or access to personal information provided to VMware as a processor, we will notify customers without undue delay and will provide information relating to a data breach as reasonably requested by our customers. VMware will use reasonable endeavors to assist customers in mitigating, where possible, the adverse effects of any data breach.
(h) Establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity or availability of customer information in your control. Such incident response plan shall address the following areas: 1. The goals of the incident response plan; 2. The internal processes for responding to a security event; 3. The definition of clear roles, responsibilities and levels of decision-making authority; 4. External and internal communications and information sharing; 5. Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls; 6. Documentation and reporting regarding security events and related incident response activities; and 7. The evaluation and revision as necessary of the incident response plan following a security event.	

GLBA Requirement	VMware Control
Compliance — annual evaluation	On a quarterly basis, senior management meets with the Board of Directors to review business objectives, company initiatives, resource needs, and risk management activities, including results from internal and external assessments. Additionally, the Chief Security Officer (“CSO”) reports to the Audit Committee annually and Internal Audit reports to the Audit Committee quarterly on information security matters and concerns. Further details are available in the VMware Cloud on AWS SOC2 Audit Report.
i) Require your Qualified Individual to report in writing, regularly and at least annually, to your board of directors or equivalent governing body. If no such board of directors or equivalent governing body exists, such report shall be timely presented to a senior officer responsible for your information security program. The report shall include the following information: 1. The overall status of the information security program and your compliance with this part; and 2. Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security events or violations and management’s responses thereto, and recommendations for changes in the information security program.	

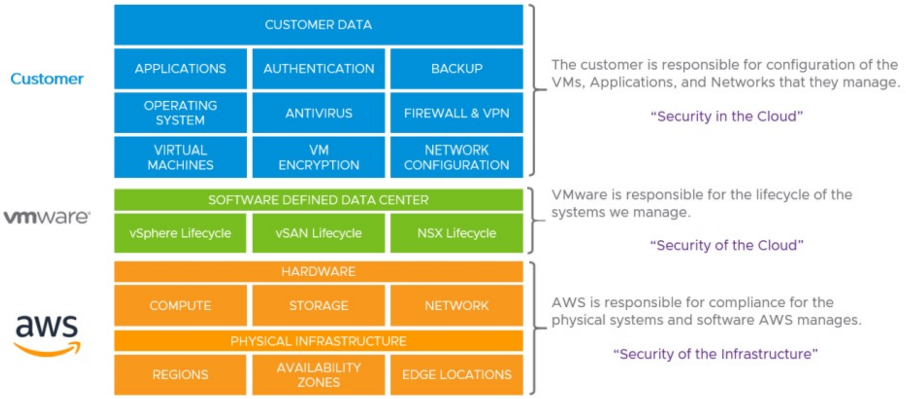
Additionally, VMware Cloud on AWS complies with various certifications and regulations such as ISO 27001, SOC 2, PCI DSS, HIPAA and a number of global government certifications. VMware also has a dedicated compliance program that provides customers with the necessary information, guidance and resources to help them comply with various regulations and industry standards.

It is also important to remember that the GLBA compliance is an ongoing proces, and financial institutions should stay informed about any changes or updates to the act and its implementing regulations, as well as any industry standards that may apply to their business. Financial institutions should also regularly conduct risk assessments and audits to ensure that their security measures are adequate and effective.

Customers who require additional disaster recovery capabilities can also opt for the VMware Site Recovery™ (VSR) or VMware Cloud Disaster Recovery (VCDR) service. These services provide an end-to-end disaster recovery solution that can eliminate secondary sites, accelerate time-to-protection and simplify recovery operations. The VSR service is available as an optional add-on service for VMC on AWS. For details on VSR and VCDR please visit vmc.vmware.com.

VMware Cloud on AWS shared responsibility model

VMware Cloud on AWS implements a shared responsibility model that defines distinct roles and responsibilities of the three parties involved in the offering: Customer, VMware and Amazon Web Services.



The customer is responsible for configuration of the VMs, Applications, and Networks that they manage.

"Security in the Cloud"

VMware is responsible for the lifecycle of the systems we manage.

"Security of the Cloud"

AWS is responsible for compliance for the physical systems and software AWS manages.

"Security of the Infrastructure"

Customer responsibility "Security in the Cloud" — Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with VMware vCenter® Roles and Permissions to apply the appropriate controls for users.

Customer responsibility "Security in the Cloud" — Customers are responsible for the deployment and ongoing configuration of their SDDC, virtual machines and data that reside therein. In addition to determining the network firewall and VPN configuration, customers are responsible for managing virtual machines (including in guest security and encryption) and using VMware Cloud on AWS User Roles and Permissions along with VMware vCenter® Roles and Permissions to apply the appropriate controls for users.

VMware responsibility "Security of the Cloud" — VMware is responsible for protecting the software and systems that make up the VMware Cloud on AWS service. This software infrastructure is composed of the compute, storage and networking software comprising the SDDC, along with the service consoles used to provision VMware Cloud on AWS.

AWS responsibility "Security of the Infrastructure" — AWS is responsible for the physical facilities, physical security, infrastructure and hardware underlying the entire service.

Financial institution customers should be aware of their responsibilities of securing and protecting personal financial information, including implementing appropriate administrative, technical and physical safeguards, and regularly assessing and updating their information security program as needed.

Customers should also conduct their own risk assessments to identify any applicable compliance requirements for the data they upload on to the VMC platform and any contractual commitments to be included in the addendum/terms of service.

Conclusion

VMware Cloud on AWS is architected and operated with stringent security measures keeping in mind the security, availability and confidentiality requirements of Financial Institutions. VMware regularly conducts various internal and external security assessments and audits to protect our platform and maintain customers' trust in securing their data. VMware also has a dedicated compliance program that provides customers with the necessary information, guidance and resources to help them comply with various regulations and industry standards. If customers wish to understand specific areas in more depth, VMware can assist agencies by providing further resources in line with a specific use case.

Further reading

- VMware Cloud on AWS
- VMware Site Recovery
- VMware Cloud Disaster Recovery
- VMWare Cloud on AWS — Privacy Datasheet
- VMware Trust Center

Contributors

- Shekhar Hemnani — Product Line Manager, VMware Cloud Solutions
- Patrick O'Brien — Group Product Line Manager, VMware Cloud Solutions
- Matt Dreyer — Sr. Director, VMware Cloud Solutions

Item No: Compliance with Gramm-Leach-Bliley Act (GLBA) 4/23