CHECKLIST

Safeguards Rule Compliance Checklist for Financial Institutions

How eSentire helps your organization build a security program that complies with the new FTC Safeguards Rule

Recent updates to the Federal Trade Commission's 2003 Gramm-Leach-Bliley Act Safeguards Rule create new standards and procedures that will apply to non-banking financial institutions and go into effect in June 2023. These updates require non-banking financial institutions to develop, implement, and maintain a comprehensive security program to keep customer information safe. These financial institutions include, but are not limited to, automotive dealers, mortgage lenders, "payday" lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, travel agencies operated in connection with financial services, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, investment advisors not required to register with the Securities and Exchange Commission, and entities acting as finders.

Financial Institutions Have Access to Highly Valuable Customer Information

The updates to the Safeguards Rule will apply to all financial services companies in the US, regardless of size. All financial institutions have a significant amount of sensitive customer information that they store, handle, process, and/or transmit that must be secured. According to the Safeguards Rule, 'customer information' is any non-public record that contains personal information about the customer that is handled or maintained by, or on behalf of, you or your affiliates. Some examples include:

- Information provided on applications for a loan or mortgage
- Account balances, payment history, or overdraft history
- Any information you collect through an Internet 'cookie' from your website visitors (e.g., web browsing history, IP address, location, etc.)
- Information from a consumer report

It's critical for financial institutions to understand how these amendments may apply to their organizations before renewing or signing a new contract with a data security vendor.

Using This Checklist: Where Every Financial Institution Should Start

Financial institutions throughout the United States are expected to have deployed and implemented an information security program with administrative, technical, and physical safeguards designed to:

- Ensure the security and confidentiality of consumer information
- Protect against anticipated threats or hazards to the security or integrity of that information
- Protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer

While the purpose of the Safeguards Rule is to establish standards for data security and breach notification for customers, it also serves as a good framework to start from as your organization looks to develop an end-to-end cybersecurity and incident response plan that will ensure data security and prevent business disruption. eSentire has broken down the Safeguards Rule to provide tangible recommendations that can be leveraged as a Cyber Risk checklist in terms of services and adoption by financial institutions.

Safeguards Rule Requirements	Sections	Testing Procedures	eSentire Services
Designate a Qualified Individual to implement and supervise your company's information security program	16 CFR 314.4(a)	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:	**eSentire vCISO** eSentire's named Virtual CISO (vCISO) works directly with you to assess your cybersecurity program maturity against your industry peers and measures your ability to address the latest cyber threats. We help you align your cybersecurity strategy and business objectives to build a cyber roadmap that reduces your cyber risk.
	16 CFR 314.4(a)(1)	Retain responsibility for compliance with this part;	
	16 CFR 314.4(a)(2)	Designate a senior member of your personnel responsible for direction and oversight of the Qualified Individual; and	
	16 CFR 314.4(a)(3)	Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.	
Conduct a risk assessment	16 CFR 314.4(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.	**eSentire vCISO** eSentire Virtual CISO (vCISO) service, Security Program Maturity Assessment (SPMA), provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time.
	16 CFR 314.4(b)(1)	The risk assessment shall be written and shall include:	
	16 CFR 314.4(b)(1)(i)	Criteria for the evaluation and categorization of identified security risks or threats you face;	
	16 CFR 314.4(b)(1)(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	
	16 CFR 314.4(b)(1)(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.	
	16 CFR 314.4(b)(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.	

Safeguards Rule Requirements	Sections	Testing Procedures	eSentire Services
Design and implement safeguards to control the risks identified through your risk assessment.	16 CFR 314.4(c)	Design and implement safeguards to control the risks you identity through risk assessment, including by:	**eSentire vCISO** eSentire's Virtual CISO (vCISO) service reviews, assesses, and assists you in developing and tailoring information security policies to address the cybersecurity threats and regulatory compliance requirements specific to your organization. **eSentire vCISO services:** - Security Program Maturity Assessment (SPMA) - Security Policy Review and Guidance (SPG) - Security Architecture Review (SAR) - Vendor Risk Management Program (VRM) **eSentire MDR for Network** eSentire MDR for Network monitors your network traffic around-the-clock using proprietary deep packet inspection and advanced behavioral analytics. We automatically disrupt malicious traffic on your behalf and our 24/7 SOC Cyber Analysts work as an extension of your team to determine root cause and provide remediation support so threat actors cannot complete attacks to your network. **eSentire MDR for Endpoint** eSentire MDR for Endpoint protects your assets 24/7 no matter where your users or data reside. We combine elite threat hunting with endpoint threat prevention and endpoint detection and response capabilities. Our 24/7 SOC Cyber Analysts rapidly investigate and isolate compromised endpoints on your behalf, preventing lateral spread. We work alongside you to determine root cause, remediate with corrective actions and ensure you are protected against business disruption. Our best-of-breed MDR approach means we partner with leaders in endpoint protection (EPP) and endpoint detection and response (EDR) to deliver eSentire MDR for Endpoint.
	16 CFR 314.4(c)(1)	Implementing and periodically reviewing access controls, including technical and, as appropriate, physical controls to:	
	16 CFR 314.4(c)(1)(i)	Authenticate and permit access only to authorized users to protect against the unauthorized acquisition of customer information; and	
	16 CFR 314.4(c)(1)(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;	
	16 CFR 314.4(c)(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;	
	16 CFR 314.4(c)(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;	
	16 CFR 314.4(c)(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;	
Design and implement safeguards to control the risks identified through your risk assessment.	16 CFR 314.4(c)(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;	**eSentire MDR for Log** eSentire MDR for Log provides you with multi-signal visibility across your network assets, endpoints, applications and cloud services enabling data correlation and deep investigation regardless if your data is in the cloud, on premises or in between. We support you with a team of researchers who power MDR for Log with hundreds of proprietary runbooks, and cutting edge detections of threat actor tactics, techniques and procedures (TTPs). Our best-of-breed MDR approach means we partner with the leading technology platforms in data analytics, log management, and cloud SIEM.
	16 CFR 314.4(c)(6)		
	16 CFR 314.4(c)(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	
	16 CFR 314.4(c)(6)(ii)	Periodically review your data retention policy to minimize the unnecessary retention of data;	
	16 CFR 314.4(c)(7)	Adopt procedures for change management; and	
	16 CFR 314.4(c)(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.	

Safeguards Rule Requirements	Sections	Testing Procedures	eSentire Services
Regularly monitor and test the effectiveness of your safeguards	16 CFR 314.4(d)		**eSentire Managed Vulnerability Service & eSentire Managed Risk Programs** eSentire's Managed Vulnerability Service accurately identifies vulnerabilities across traditional and dynamic IT assets such as mobile devices, OT, IoT, virtual machines and cloud. With eSentire Managed Risk Programs, our risk management team conducts regular penetration testing and vulnerability assessments, and risk assessments, to help you identify blind spots, build a strategy for mitigating cyber risk, and operationalize capabilities to predict and prevent known & unknown threats.
	16 CFR 314.4(d)(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.	
	16 CFR 314.4(d)(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:	
	16 CFR 314.4(d)(2)(i)	Annual penetration testing of your information systems determined each given year based on relevant identified risks in accordance with the risk assessment; and	
	16 CFR 314.4(d)(2)(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.	
Train your staff	16 CFR 314.4(e)	Implement policies and procedures to ensure that personnel are able to enact your information security program by:	**eSentire Managed Phishing and Security Awareness Training (PSAT)** eSentire's Managed Phishing and Security Awareness Training helps you identify risk, alleviate resource constraints, and test user resiliency, while you enable behavioral change with your employees and generate measurable results across your business.
	16 CFR 314.4(e)(1)	Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;	
	16 CFR 314.4(e)(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;	
	16 CFR 314.4(e)(3)	Providing information security personnel with security updates and training sufficient to address relevant security risks; and	
	16 CFR 314.4(e)(4)	Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.	
Monitor your service providers	16 CFR 314.4(f)	Oversee service providers, by:	**eSentire Vendor Risk Assessment** Based on the eSentire Security Framework that is built on the foundations of NIST, the eSentire Vendor Risk Assessment is designed to help resource constrained organizations: - Determine risk identification and measurement criteria - Categorize assessment data access against risk appetite - Develop questionnaires for assessment - Conduct comprehensive assessments - Analyze data with comparisons against risk categorizations - Define corrective actions for risky third parties and vendors - Determine defensive adjustments to mitigate risk
	16 CFR 314.4(f)(1)	Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;	
	16 CFR 314.4(f)(2)	Requiring your service providers by contract to implement and maintain such safeguards; and	
	16 CFR 314.4(f)(3)	Periodically assessing your service providers based on the risk they present and the continued adequacy of their safeguards.	

Safeguards Rule Requirements	Sections	Testing Procedures	eSentire Services
Keep your information security program current	16 CFR 314.4(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.	**eSentire vCISO** eSentire Virtual CISO (vCISO) service, Security Program Maturity Assessment (SPMA), provides an in-depth analysis of your organization's current security posture and creates a roadmap plan with a framework playbook to follow. Annual re-assessments help you mature and measure how security programs improve over time.
Create a written incident response plan	16 CFR 314.4(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:	**eSentire On-Demand 24/7 Incident Response Retainer** eSentire's IR experts can work with your team on Security Incident Response Planning (SIRP) and development, as well as table top exercises. eSentire's industry-leading On-Demand 24/7 Incident Response Retainer provides 4-hour threat suppression, remotely, anywhere in the world.
	16 CFR 314.4(h)(1)	The goals of the incident response plan;	
	16 CFR 314.4(h)(2)	The internal processes for responding to a security event;	
	16 CFR 314.4(h)(3)	The definition of clear roles, responsibilities, and levels of decision-making authority;	
	16 CFR 314.4(h)(4)	External and internal communications and information sharing;	
	16 CFR 314.4(h)(5)	Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;	
	16 CFR 314.4(h)(6)	Documentation and reporting regarding security events and related incident response activities; and	
	16 CFR 314.4(h)(7)	The evaluation and revision as necessary of the incident response plan following a security event.	
Require your Qualified Individual to report to your Board of Directors	16 CFR 314.4(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:	**eSentire vCISO** eSentire's Virtual CISO (vCISO) service reviews, assesses, and assists you in developing and measuring your information security program, as well as compliance with the Safeguards Rule.
	16 CFR 314.4(i)(1)	The overall status of the information security program and your compliance with this part; and	
	16 CFR 314.4(i)(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.	

eSentire Cybersecurity Services Portfolio for Financial Institutions

At eSentire, we go beyond the market's capability in threat response. eSentire's multi-signal MDR approach ingests endpoint, network, log, cloud, asset and vulnerability data that enables complete attack surface visibility. Enriched detections from the eSentire Threat Response Unit (TRU) are applied to captured data identifying known & unknown threats including suspicious activity and zero-day attacks. With two 24/7 Security Operations Centers staffed with cyber experts and Elite Threat Hunters, an industry-leading XDR Cloud Platform, and refined security operations processes, eSentire can detect and respond with a Mean Time to Contain of 15 minutes.

Gain Confidence, Control & Expertise

Managed Risk Services

TAKE CONTROL OF CYBER RISK

Strategic services including Vulnerability Management, vCISO and Managed Phishing & Security Awareness Training to identify gaps, build defensive strategies, operationalize risk mitigation and continuously advance your security program.

Managed Detection & Response

PREVENT THREATS BECOMING BUSINESS DISRUPTING EVENTS

We deliver Response + Remediation you can trust. By combining our cutting-edge XDR platform, 24/7 threat hunting and security operations leadership, we hunt and disrupt known and unknown threats before they impact your business.

Incident Response & Digital Forensics

BE READY WITH THE WORLD'S FASTEST THREAT SUPPRESSION

Battle-tested Incident Commander level expertise, crime scene reconstruction and digital forensics investigations that can bear scrutiny in a court of law. The world's fastest threat suppression with a 4-hourSLA available with our IR Retainer.

eSentire MDR features include:

- ✓ 24x7 Always-on Monitoring
- ✓ 24x7 Live SOC Cyber Analyst Support
- ✓ 24x7 Threat Hunting
- ✓ 24x7 Threat Disruption and Containment Support
- ✓ Mean Time to Contain: 15 minutes
- ✓ Machine Learning XDR Cloud Platform
- ✓ Multi-signal Coverage and Visibility
- ✓ Automated Detections with Signatures, IOCs and IPs
- ✓ Security Network Effects
- ✓ Detections mapped to MITRE ATT&CK Framework
- ✓ 5 Machine Learning patents for threat detection and data transfer
- ✓ Detection of unknown attacks using behavioral analytics
- ✓ Rapid human-led investigations
- ✓ Threat containment and remediation
- ✓ Detailed escalations with analysis and security recommendations
- ✓ eSentire Insight Portal access and real-time visualizations
- ✓ Threat Advisories, Threat Research and Thought Leadership
- ✓ Operational Reporting and Peer Coverage Comparisons
- ✓ Named Cyber Risk Advisor
- ✓ Business Reviews and Strategic Continuous Improvement planning

Reach out to connect with an eSentire security specialist **Get Started**

If you're experiencing a security incident or breach contact us **1-866-579-2200**

eSENTIRE

eSentire, Inc. is the Authority in Managed Detection and Response, protecting the critical data and applications of 1500+ organizations in 80+ countries, representing 35 industries from known and unknown cyber threats. Founded in 2001, the company's mission is to hunt, investigate and stop cyber threats before they become business disrupting events. Combining cutting-edge machine learning XDR technology, 24/7 Threat Hunting, and proven security operations leadership, eSentire mitigates business risk, and enables security at scale. The Team eSentire difference means enterprises are protected by the best in the business with a named Cyber Risk Advisor, 24/7 access to SOC Cyber Analysts, Elite Threat Hunters, and industry-leading threat intelligence research from eSentire's Threat Response Unit (TRU). eSentire provides Managed Risk, Managed Detection and Response and Incident Response services. For more information, visit **www.esentire.com** and follow **@eSentire**.