700Credit

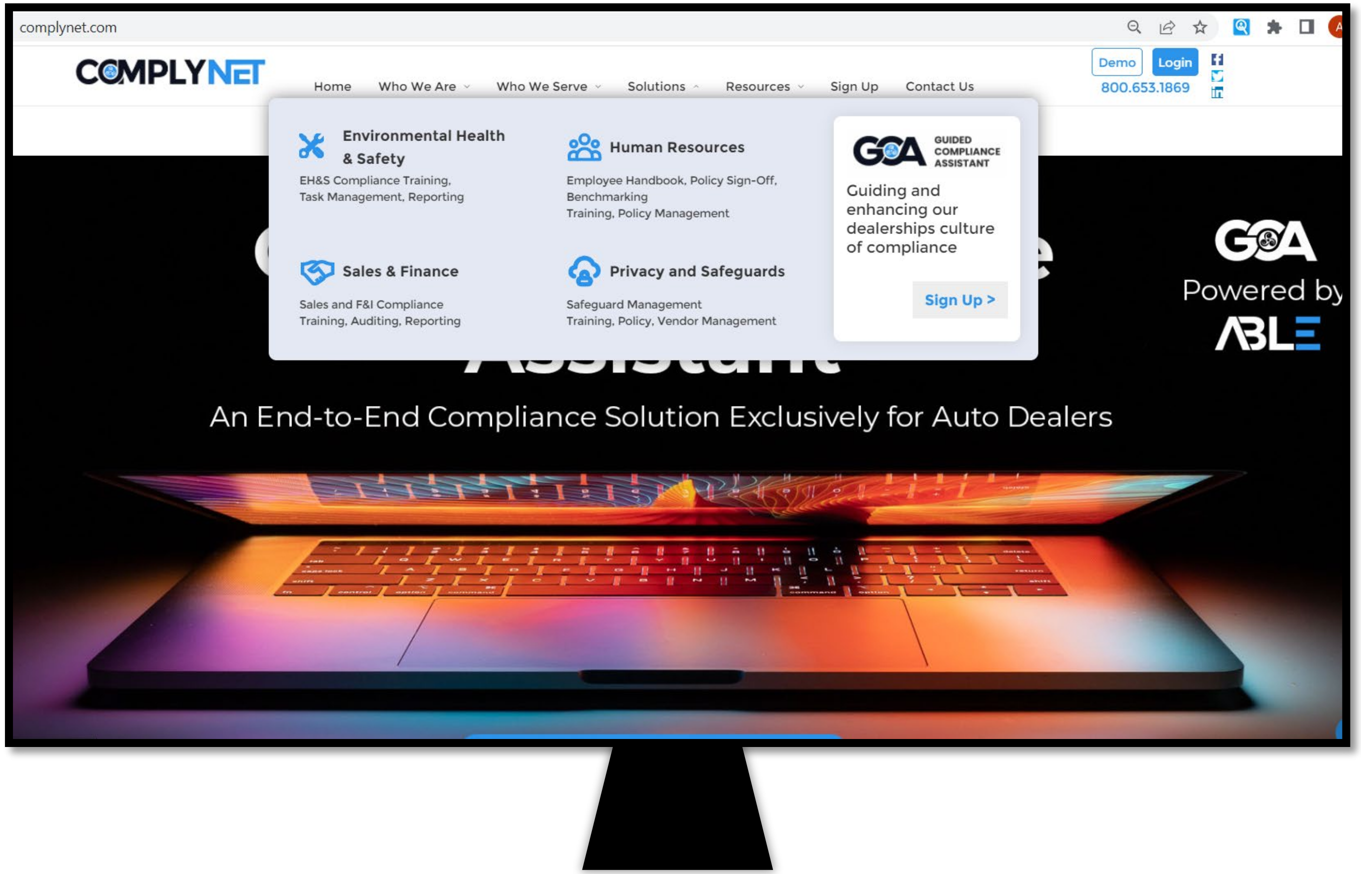
CREDIT | COMPLIANCE | SOFT-PULLS

Complynet Safeguards Sales Deck

July 2022

Complynet's History

- Founded in 1994
- Automotive exclusive
- End-to-end compliance
- Tech-enabled solutions
- Association endorsed
- Over 3,000 rooftop partners



Environmental Health & Safety
EH&S Compliance Training, Task Management, Reporting

Human Resources
Employee Handbook, Policy Sign-Off, Benchmarking
Training, Policy Management

Sales & Finance
Sales and F&I Compliance
Training, Auditing, Reporting

Privacy and Safeguards
Safeguard Management
Training, Policy, Vendor Management

GCA GUIDED COMPLIANCE ASSISTANT

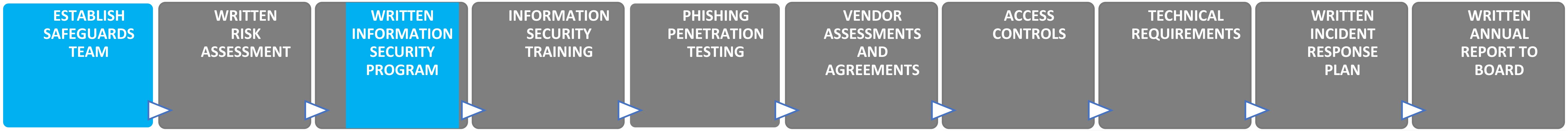
Guiding and enhancing our dealerships culture of compliance

An End-to-End Compliance Solution Exclusively for Auto Dealers

Safeguards History

SAFEGUARDS RULE FACTS	
Original Effective Date	2003
Revised	October 2021
Enforcement Date for New Provisions	December 9, 2022
Penalties	up to $46,517 per violation
ComplyNet InfoSec Solutions	8 years
Steps to Compliance	10

1. Establish a Safeguards Team


ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

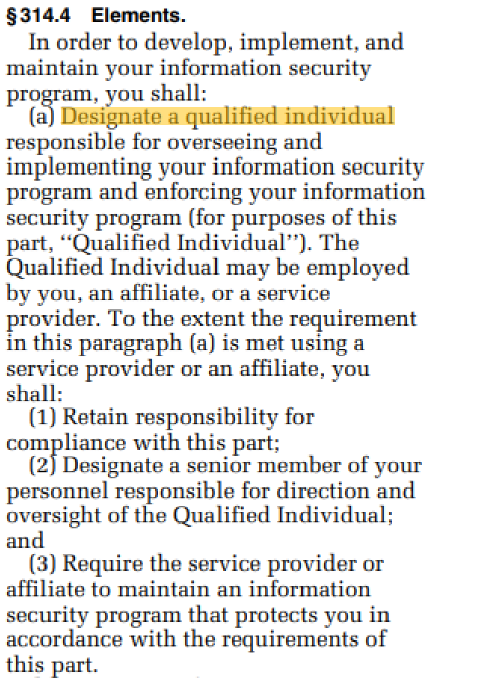
TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

- Team Members:
  - Qualified Individual
    - Implement
    - Oversee
    - Enforce
  - Qualified IT/MSP
    - Perform or oversee
  - Compliance
- Establish KPIs, meet regularly, and track progress

RULE



§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

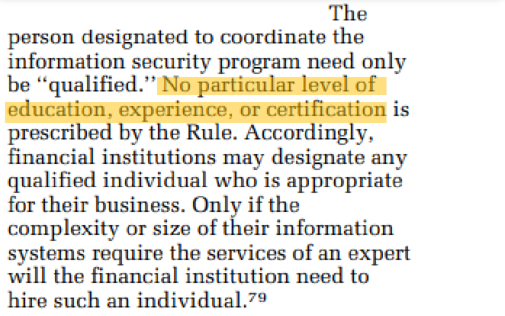
(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(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

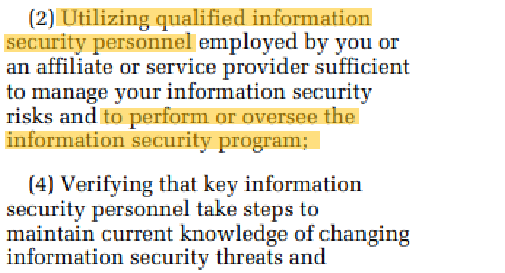
(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

FTC COMMENT



The person designated to coordinate the information security program need only be "qualified." No particular level of education, experience, or certification is prescribed by the Rule. Accordingly, financial institutions may designate any qualified individual who is appropriate for their business. Only if the complexity or size of their information systems require the services of an expert will the financial institution need to hire such an individual.[79]

RULE

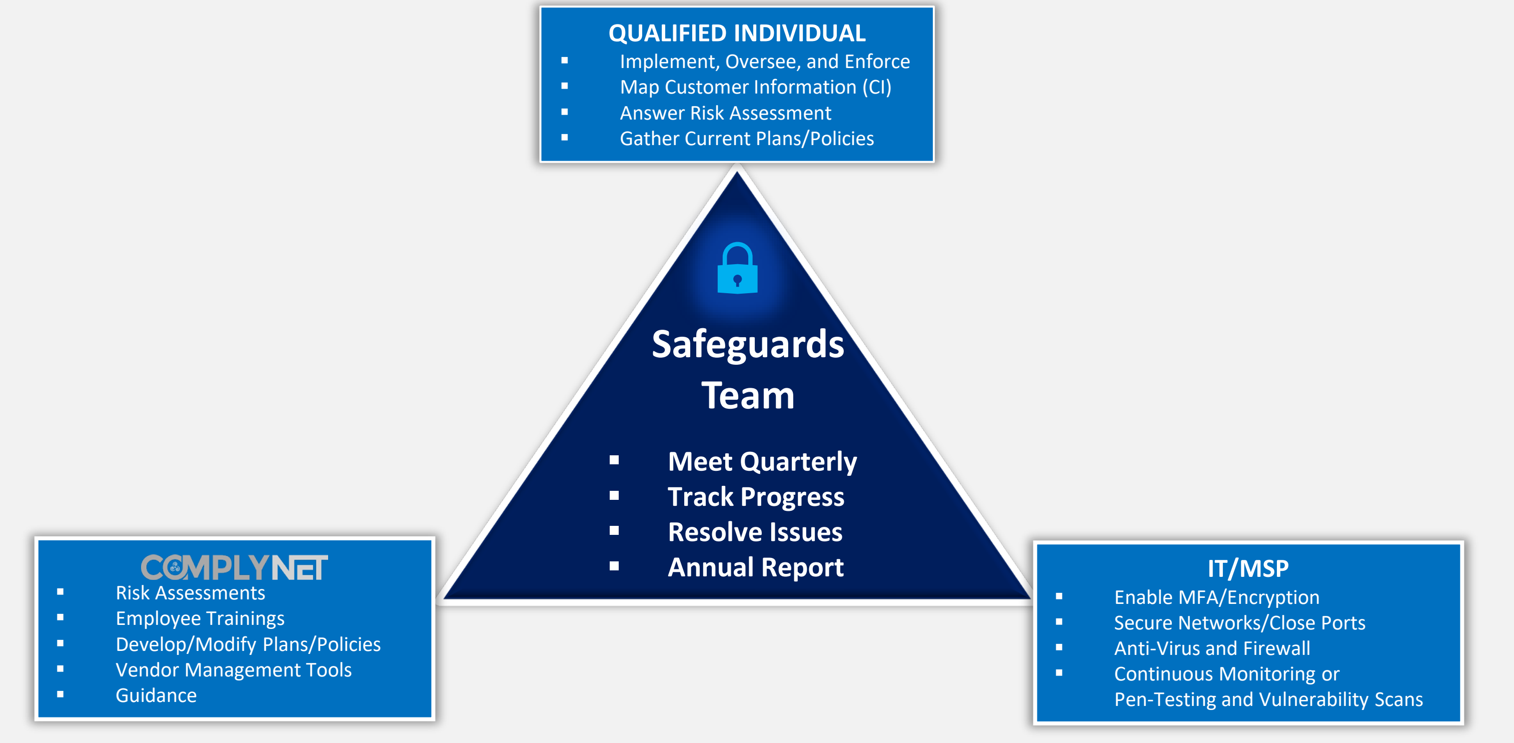


(2) Utilizing qualified information security personnel employed by you or an affiliate or service provider sufficient to manage your information security risks and to perform or oversee the information security program;

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and

1. Establish a Safeguards Team

- ESTABLISH SAFEGUARDS TEAM
- WRITTEN RISK ASSESSMENT
- WRITTEN INFORMATION SECURITY PROGRAM
- INFORMATION SECURITY TRAINING
- PHISHING PENETRATION TESTING
- VENDOR ASSESSMENTS AND AGREEMENTS
- ACCESS CONTROLS
- TECHNICAL REQUIREMENTS
- WRITTEN INCIDENT RESPONSE PLAN
- WRITTEN ANNUAL REPORT TO BOARD



QUALIFIED INDIVIDUAL

- Implement, Oversee, and Enforce
- Map Customer Information (CI)
- Answer Risk Assessment
- Gather Current Plans/Policies

Safeguards Team

- Meet Quarterly
- Track Progress
- Resolve Issues
- Annual Report

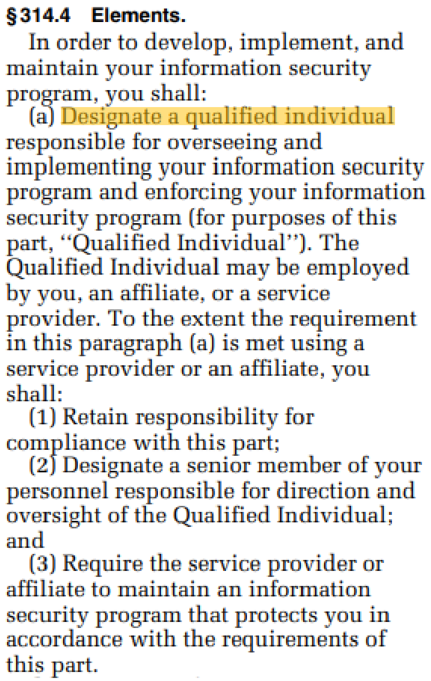
COMPLYNET

- Risk Assessments
- Employee Trainings
- Develop/Modify Plans/Policies
- Vendor Management Tools
- Guidance

IT/MSP

- Enable MFA/Encryption
- Secure Networks/Close Ports
- Anti-Virus and Firewall
- Continuous Monitoring or Pen-Testing and Vulnerability Scans

RULE



§ 314.4 Elements.

In order to develop, implement, and maintain your information security program, you shall:

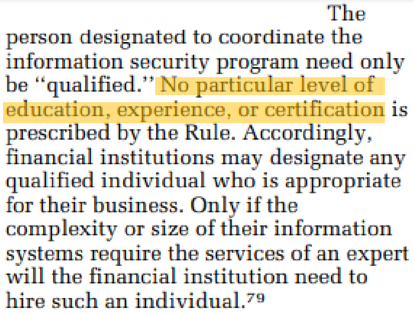
(a) Designate a qualified individual responsible for overseeing and implementing your information security program and enforcing your information security program (for purposes of this part, "Qualified Individual"). The Qualified Individual may be employed by you, an affiliate, or a service provider. To the extent the requirement in this paragraph (a) is met using a service provider or an affiliate, you shall:

(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

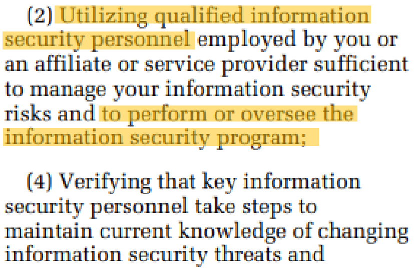
(3) Require the service provider or affiliate to maintain an information security program that protects you in accordance with the requirements of this part.

FTC COMMENT



The person designated to coordinate the information security program need only be "qualified." No particular level of education, experience, or certification is prescribed by the Rule. Accordingly, financial institutions may designate any qualified individual who is appropriate for their business. Only if the complexity or size of their information systems require the services of an expert will the financial institution need to hire such an individual.[79]

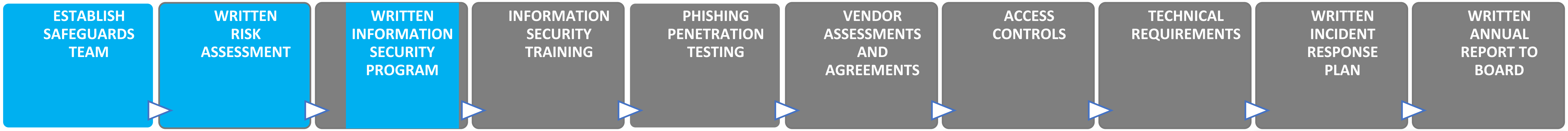
RULE



(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;

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and

2. Written Risk Assessment


ESTABLISH SAFEGUARDS TEAM
WRITTEN RISK ASSESSMENT
WRITTEN INFORMATION SECURITY PROGRAM
INFORMATION SECURITY TRAINING
PHISHING PENETRATION TESTING
VENDOR ASSESSMENTS AND AGREEMENTS
ACCESS CONTROLS
TECHNICAL REQUIREMENTS
WRITTEN INCIDENT RESPONSE PLAN
WRITTEN ANNUAL REPORT TO BOARD

- Map (where CI is stored, who accesses, and how)
- Identify risks
- Evaluate and categorize risks
- Examine controls/safeguards
- Mitigate risks (or accept and address)
- Periodically reexamine controls/safeguards

RULE

(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;

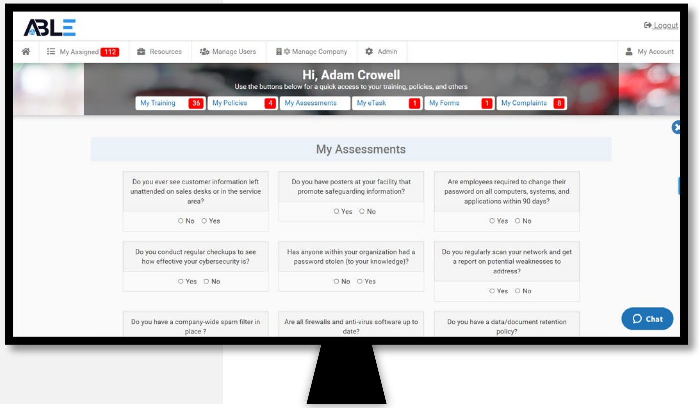
RULE

(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



Hi, Adam Crowell

Use the buttons below for a quick access to your training, policies, and others

My Assessments

Do you ever see customer information left unattended on sales desks or in the service area?
○ No ○ Yes

Do you have posters at your facility that promote safeguarding information?
○ Yes ○ No

Are employees required to change their password on all computers, systems, and applications within 90 days?
○ Yes ○ No

Do you conduct regular checkups to see how effective your cybersecurity is?
○ Yes ○ No

Has anyone within your organization had a password stolen (to your knowledge)?
○ No ○ Yes

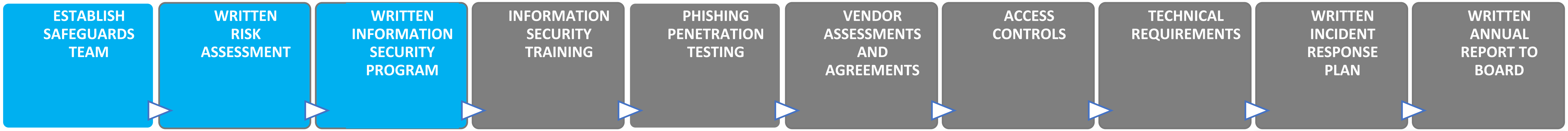
Do you regularly scan your network and get a report on potential weaknesses to address?
○ Yes ○ No

Do you have a company-wide spam filter in place ?

Are all firewalls and anti-virus software up to date?

Do you have a data/document retention policy?

3. Written Information Security Program



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

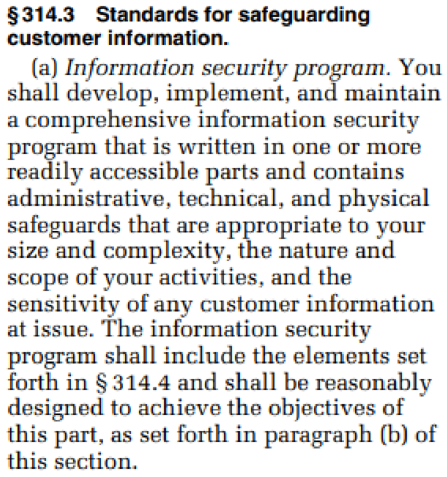
TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

- Created based upon the risk assessment
- Includes:
  - Administrative safeguards
  - Technical safeguards
  - Physical safeguards
- Establishes clear roles and responsibilities
- Automotive specific and custom-tailored
- Clear and concise
- Periodically evaluated and adjusted

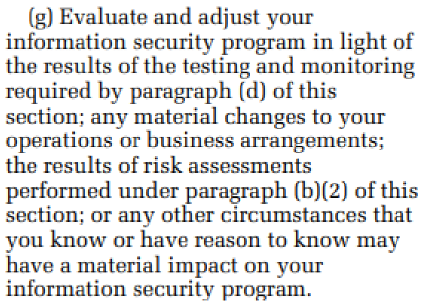
RULE



§ 314.3 Standards for safeguarding customer information.

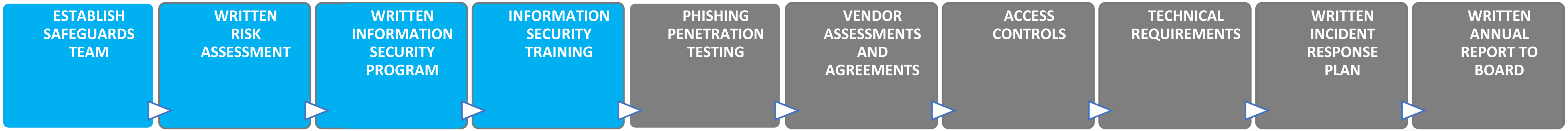
(a) *Information security program.* You shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. The information security program shall include the elements set forth in § 314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

RULE



(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.

4. Information Security Training



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

COMPLYNET

Privacy for Shop

Mandatory Training (Job-Role and Industry-Specific):

- Privacy
- Privacy for the Shop
- Safeguards
- Safeguards for the Shop
- Disposal
- Information Security Awareness
- Phishing
- PCI

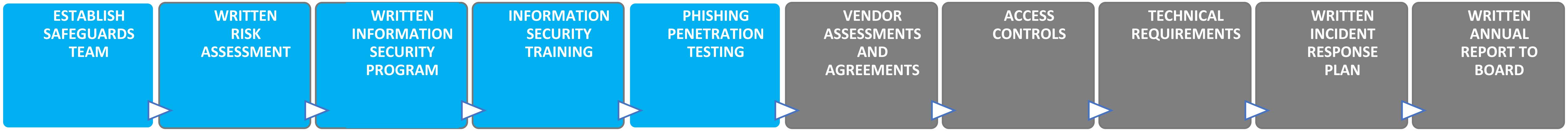
RULE

(1) Providing your personnel with security awareness training that is updated as necessary to reflect risks identified by the risk assessment;

RULE

(4) Verifying that key information security personnel take steps to maintain current knowledge of changing information security threats and countermeasures.

5. Phishing Penetration Testing



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

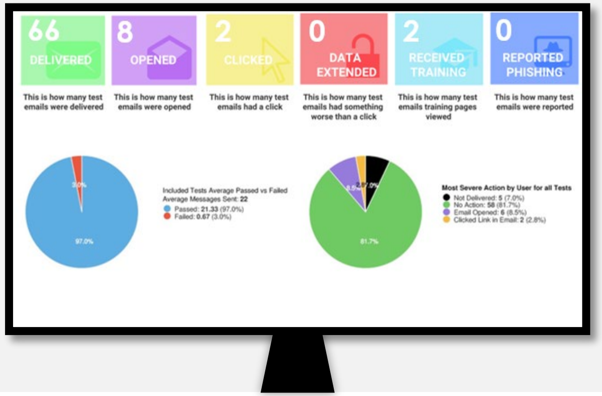
FTC COMMENT

Penetration testing, as defined by the Final Rule, is a process through which testers "attempt to circumvent or defeat the security features of an information system."[56] One way such security features are tested is through social engineering and phishing.[57] The fact that the testing involves employees with access to the information system, rather than just the system itself, does not exclude such tests from the definition of "penetration testing." Attempted social engineering and phishing are important parts of testing the security of information systems and would not be excluded by this definition.

FTC COMMENT FOOTNOTE

[57] Indeed, Workshop participant Scott Wallace noted, in conducting penetration testing, "the first thing [he does]" is generally to "prepare for the phishing campaign." Remarks of Scott Wallace, Safeguards Workshop Tr., *supra* note 17, at 131–32.

- 91% of all hacking starts with phishing
  - Greatest known risk
- ComplyNet conducts phishing pen-testing



This is how many test emails were delivered

This is how many test emails were opened

This is how many test emails had a click

This is how many test emails had something worse than a click

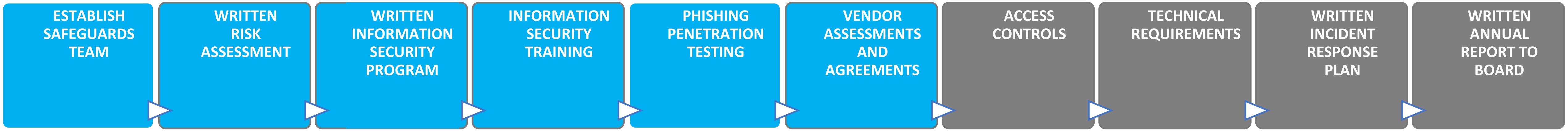
This is how many test emails training pages viewed

This is how many test emails were reported

Included Tests Average Passed vs Failed
Average Messages Sent: 22
● Passed: 21.33 (97.0%)
● Failed: 0.67 (3.0%)

Most Severe Action by User for all Tests
● Not Delivered: 5 (7.0%)
● No Action: 58 (81.7%)
● Email Opened: 6 (8.5%)
● Clicked Link in Email: 2 (2.8%)

6. Vendor Assessments and Agreements


ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

RULE

(f) Oversee service providers, by:

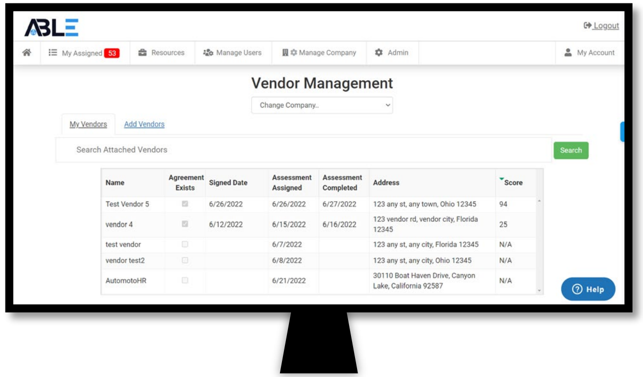
(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue;

(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.

COMMENT FOOTNOTE

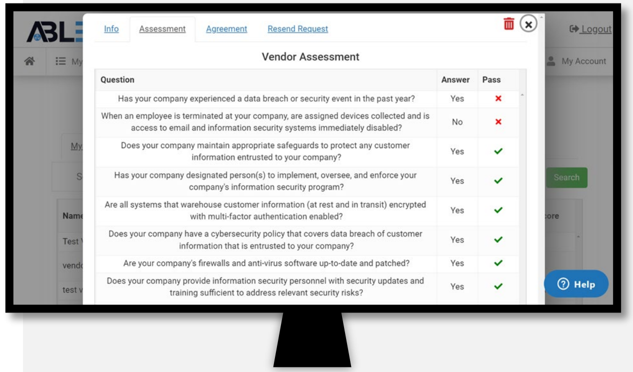
If it is infeasible for the service provider to meet these requirements then the financial institution's Qualified Individual must work with the service provider to develop compensating controls or cease doing business with the service provider.



Vendor Management

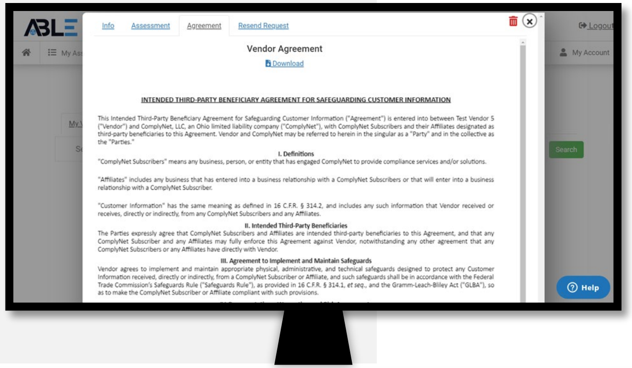
Name	Agreement Exists	Signed Date	Assessment Assigned	Assessment Completed	Address	Score
Test Vendor 5	☑	6/26/2022	6/26/2022	6/27/2022	123 any st, any town, Ohio 12345	94
vendor 4	☑	6/12/2022	6/15/2022	6/16/2022	123 vendor rd, vendor city, Florida 12345	25
test vendor	□		6/7/2022		123 any st, any city, Florida 12345	N/A
vendor test2	□		6/8/2022		123 any st, any city, Ohio 12345	N/A
AutomotoHR	□		6/21/2022		30110 Boat Haven Drive, Canyon Lake, California 92587	N/A

- Vendor Management
  - Vendor Assessments (1:many)
  - Vendor Agreements (1:many)



Vendor Assessment

Question	Answer	Pass
Has your company experienced a data breach or security event in the past year?	Yes	✗
When an employee is terminated at your company, are assigned devices collected and is access to email and information security systems immediately disabled?	No	✗
Does your company maintain appropriate safeguards to protect any customer information entrusted to your company?	Yes	✓
Has your company designated person(s) to implement, oversee, and enforce your company's information security program?	Yes	✓
Are all systems that warehouse customer information (at rest and in transit) encrypted with multi-factor authentication enabled?	Yes	✓
Does your company have a cybersecurity policy that covers data breach of customer information that is entrusted to your company?	Yes	✓
Are your company's firewalls and anti-virus software up-to-date and patched?	Yes	✓
Does your company provide information security personnel with security updates and training sufficient to address relevant security risks?	Yes	✓



Vendor Agreement

INTENDED THIRD-PARTY BENEFICIARY AGREEMENT FOR SAFEGUARDING CUSTOMER INFORMATION

This Intended Third-Party Beneficiary Agreement for Safeguarding Customer Information ("Agreement") is entered into between Test Vendor 5 ("Vendor") and ComplyNet, LLC, an Ohio limited liability company ("ComplyNet"), with ComplyNet Subscribers and their Affiliates designated as third-party beneficiaries to this Agreement. Vendor and ComplyNet may be referred to herein in the singular as a "Party" and in the collective as the "Parties."

I. Definitions

"ComplyNet Subscribers" means any business, person, or entity that has engaged ComplyNet to provide compliance services and/or solutions.

"Affiliates" includes any business that has entered into a business relationship with a ComplyNet Subscribers or that will enter into a business relationship with a ComplyNet Subscriber.

"Customer Information" has the same meaning as defined in 16 C.F.R. § 314.2, and includes any such information that Vendor received or receives, directly or indirectly, from any ComplyNet Subscribers and any Affiliates.

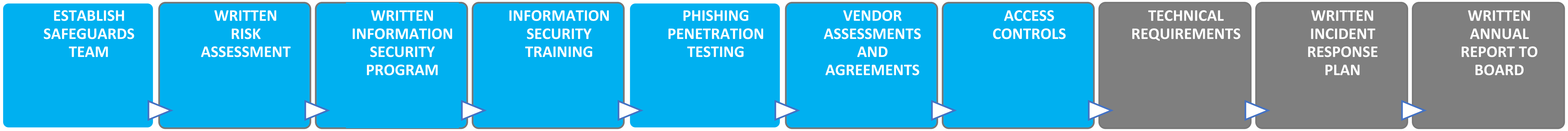
II. Intended Third-Party Beneficiaries

The Parties expressly agree that ComplyNet Subscribers and Affiliates are intended third-party beneficiaries to this Agreement, and that any ComplyNet Subscriber and any Affiliates may fully enforce this Agreement against Vendor, notwithstanding any other agreement that any ComplyNet Subscribers or any Affiliates have directly with Vendor.

III. Agreement to Implement and Maintain Safeguards

Vendor agrees to implement and maintain appropriate physical, administrative, and technical safeguards designed to protect any Customer Information received, directly or indirectly, from a ComplyNet Subscriber or Affiliate, and such safeguards shall be in accordance with the Federal Trade Commission's Safeguards Rule ("Safeguards Rule"), as provided in 16 C.F.R. § 314.1, *et seq.*, and the Gramm-Leach-Bliley Act ("GLBA"), so as to make the ComplyNet Subscriber or Affiliate compliant with such provisions.

7. Access Controls


ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

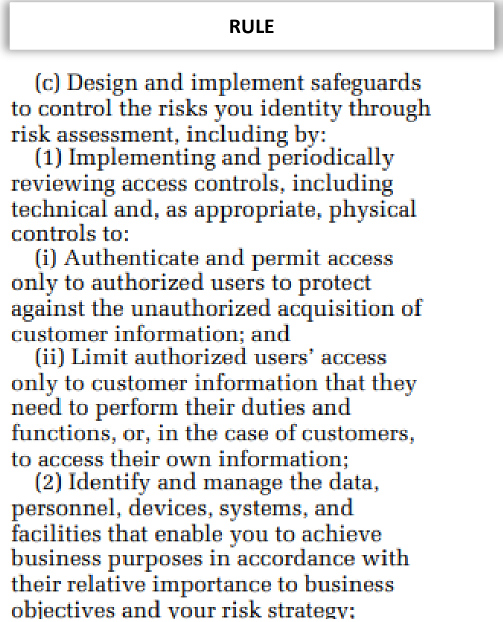
VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD


RULE

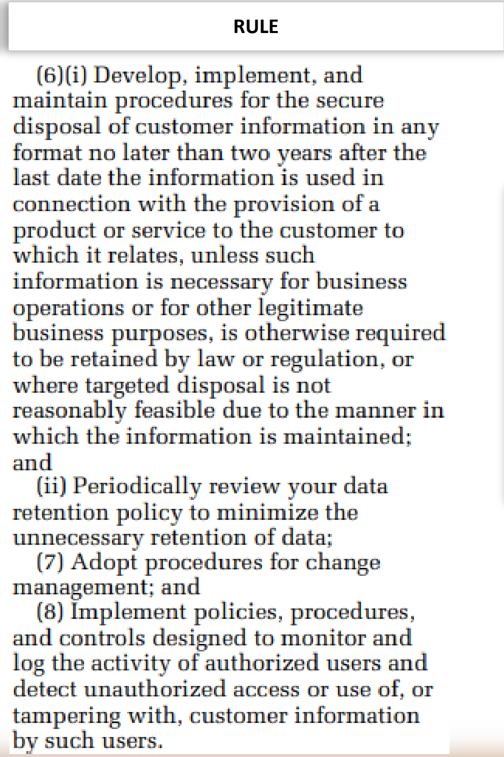
(c) Design and implement safeguards to control the risks you identity through risk assessment, including by:

(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;


RULE

(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

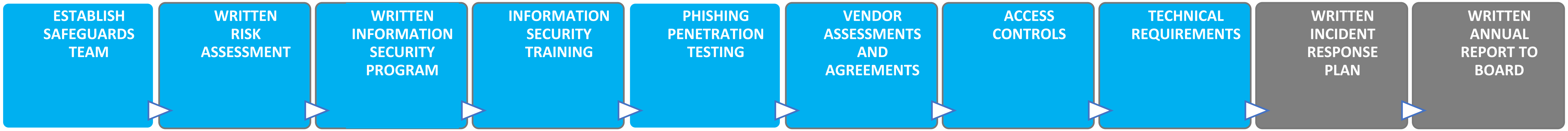
(ii) Periodically review your data retention policy to minimize the unnecessary retention of data;

(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.

- Grant limited access
- Monitor and log activity
- Detect unauthorized use, access or tampering
- Adopt change management procedures
  - Onboarding and offboarding
    - Systems administrators?
- Data and document retention and disposal

8. Technical Requirements



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

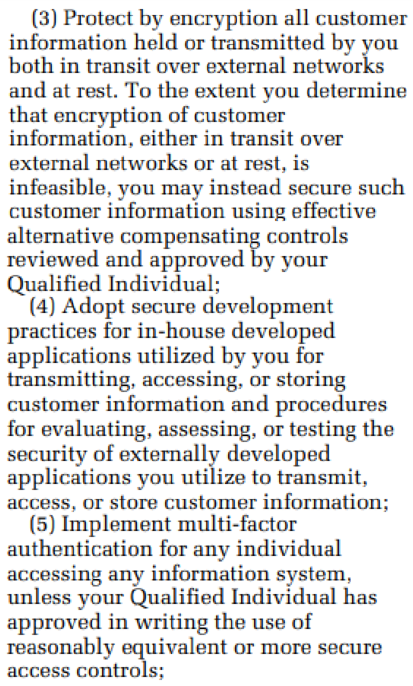
ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

RULE

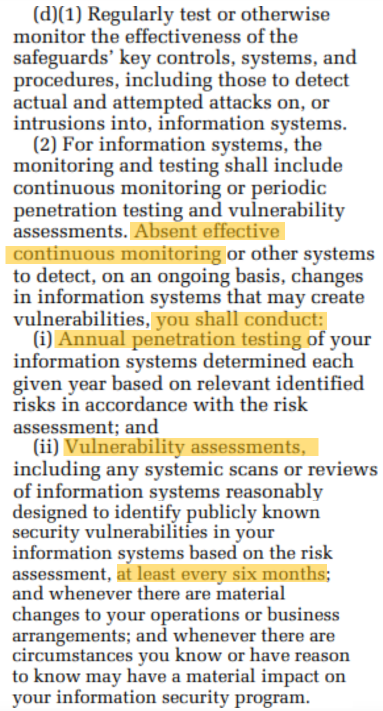


(3) Protect by encryption all customer information held or transmitted by you both in transit over external networks and at rest. To the extent you determine that encryption of customer information, either in transit over external networks or at rest, is infeasible, you may instead secure such customer 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;

RULE



(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.

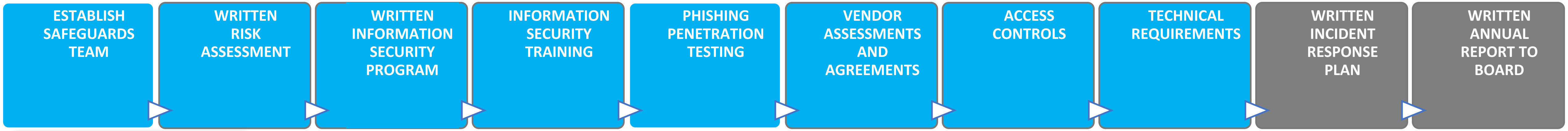
(2) For information systems, the monitoring and testing shall include continuous monitoring or periodic penetration testing and vulnerability assessments. Absent effective continuous monitoring or other systems to detect, on an ongoing basis, changes in information systems that may create vulnerabilities, 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.

- Encryption
- Multi-factor authentication (MFA)
- Continuous monitoring
  - Absent effective continuous monitoring, at least annual penetration testing and vulnerability scans every six months

8. Technical Requirements



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

RULE

(m) Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

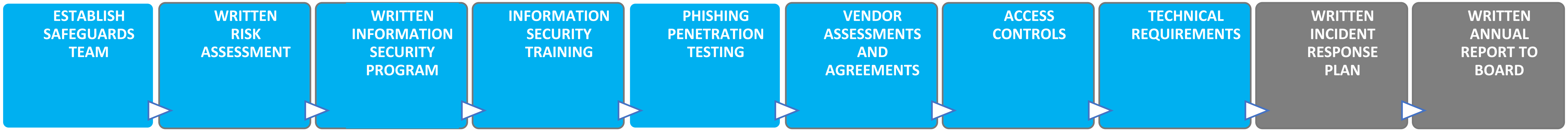
FTC COMMENT

Commission does not agree. Penetration testing, as defined by the Final Rule, is a process through which testers "attempt to circumvent or defeat the security features of an information system."[56] One way such security

- Vulnerability scan – looks for weaknesses (inexpensive – free tools are available)
- Penetration testing – can I get inside? How far can I get? What can I do? (requires "ethical hacker" and is very expensive)
  - Artificial intelligence ("AI") programs do not meet the FTC's qualifications for "assessors" in previous enforcement actions
    - "Assessors" have been defined as independent third-party professionals with experience and cybersecurity certifications
  - TIP: IF you are offered inexpensive "next gen" penetration testing with AI, it is likely just a vulnerability scan
- Continuous monitoring – 24/7/365 security that detects and stops intruders (once reserved for large companies – is now affordable to all)

- Encryption
- Multi-factor authentication (MFA)
- Continuous monitoring
  - Absent effective continuous monitoring, at least annual penetration testing and vulnerability scans every six months

8. Technical Requirements



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

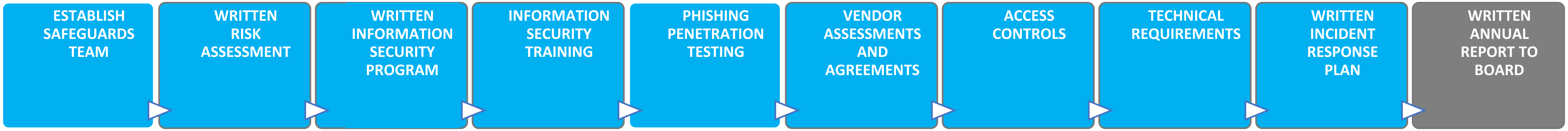
WRITTEN ANNUAL REPORT TO BOARD

- **<u>Recommendations</u>:**
  - Establish continuous threat monitoring

  - IT/MSPs have tools that they prefer to use

- Encryption
- Multi-factor authentication (MFA)
- Continuous monitoring
  - <u>Absent effective continuous monitoring</u>, at least annual penetration testing and vulnerability scans every six months

9. Written Incident Response Plan



ESTABLISH SAFEGUARDS TEAM

WRITTEN RISK ASSESSMENT

WRITTEN INFORMATION SECURITY PROGRAM

INFORMATION SECURITY TRAINING

PHISHING PENETRATION TESTING

VENDOR ASSESSMENTS AND AGREEMENTS

ACCESS CONTROLS

TECHNICAL REQUIREMENTS

WRITTEN INCIDENT RESPONSE PLAN

WRITTEN ANNUAL REPORT TO BOARD

RULE

(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:

RULE

(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.

Incident Response:

- Respond
- Recover
- Remediate
- Revise

10. Written Annual Report to Board

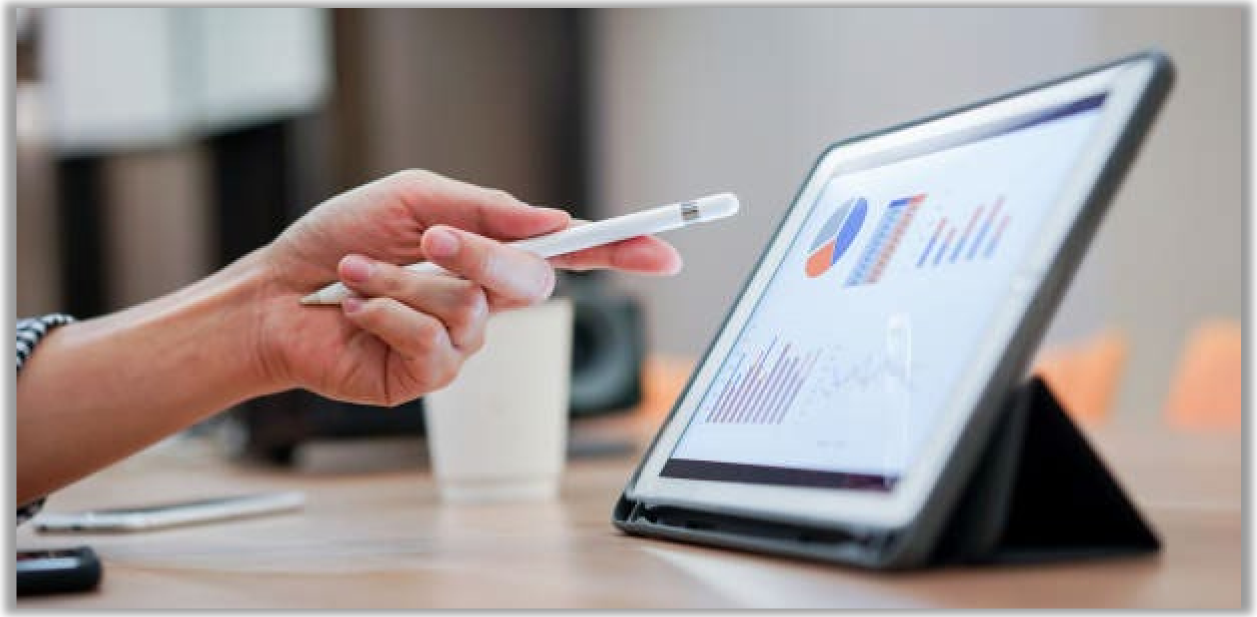
ESTABLISH SAFEGUARDS TEAM ▷ WRITTEN RISK ASSESSMENT ▷ WRITTEN INFORMATION SECURITY PROGRAM ▷ INFORMATION SECURITY TRAINING ▷ PHISHING PENETRATION TESTING ▷ VENDOR ASSESSMENTS AND AGREEMENTS ▷ ACCESS CONTROLS ▷ TECHNICAL REQUIREMENTS ▷ WRITTEN INCIDENT RESPONSE PLAN ▷ WRITTEN ANNUAL REPORT TO BOARD

RULE

(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.



- Overall status – compliance
- Risks assessed
- Risks managed and controlled
- Service provider arrangements
- Testing results
- Security violations, events, and responses
- Proposed changes

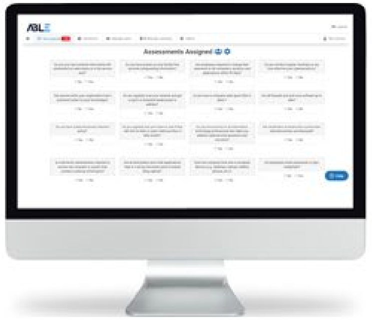
GCA GUIDED COMPLIANCE ASSISTANT

PRIVACY – SAFEGUARDS

COMPLYNET

Privacy

The goal of this training is to provide you with enough information that you will know how to protect our customers' non-public information (NPI).


ABLE

Assessments Assigned

FEATURES SUMMARY

- Assigned Compliance Success Consultant
- Compliance Management System
- Information Security Awareness Training:
  - Privacy
  - Privacy for the Shop
  - Safeguards
  - Safeguards for the Shop
  - Disposal
  - Information Security Awareness
  - Phishing
  - PCI
- Phishing Penetration Testing
- Written Risk Assessments
- Onsite Facility Vulnerability Assessments
- Vendor Assessments and Agreements
- Quarterly Meetings with Qualified Individual/IT/MSP
- Written Data/Document Retention Policy
- Written Information Security Program
- Written Data and Technology Use Policy
- Written Incident Response Plan
- Annual Written Report to the Board

Offerings	ComplyNet	Other Providers
Privacy Course	✓	✓
Safeguards Course	✓	✓
Disposal Course	✓	
Red Flags Course	✓	✓
OFAC Course	✓	
Paper Flow Course	✓	
Information Security Awareness Course	✓	✓
Phishing Course	✓	
PCI Course	✓	
Phishing Penetration Testing	✓ ComplyNet performed	✓ Dealer has to run service
Risk Assessments	✓	✓
Vendor Assessments	✓	✓
Quarterly Meetings w/ Qualified Individual, IT, and/or MSP	✓	
Document/Data Retention Policy	✓ ComplyNet created and custom-tailored to Dealer	✓ Dealer has to create with template
Information Security Program	✓ ComplyNet created and custom-tailored to Dealer	✓ Dealer has to create with template
Incident Response Plan	✓ ComplyNet created and custom-tailored to Dealer	✓ Dealer has to create with template
Annual Board Report Prepared for the Qualified Individual	✓	
Facility Vulnerability Assessment	✓ Add-On: ComplyNet performed	
Continuous Monitoring of Systems	✓ Add-On: MSP provided	

Pricing

As your partner, we make pricing transparent:

Service	Suggested Monthly Rooftop Pricing
GCA Environmental - Health - Safety	$299
GCA Sales - Finance - Advertising	$299
GCA Privacy - Safeguards	$299
GCA Deluxe (2 GCA Programs)	$549
GCA Premier (3 GCA Programs)	$799
Onsite Assessments	+ $100 per annual visit

700Credit

CREDIT | COMPLIANCE | SOFT-PULLS

Contact 700Credit Today for Help

sales@700Credit.com | (866) 273-3848