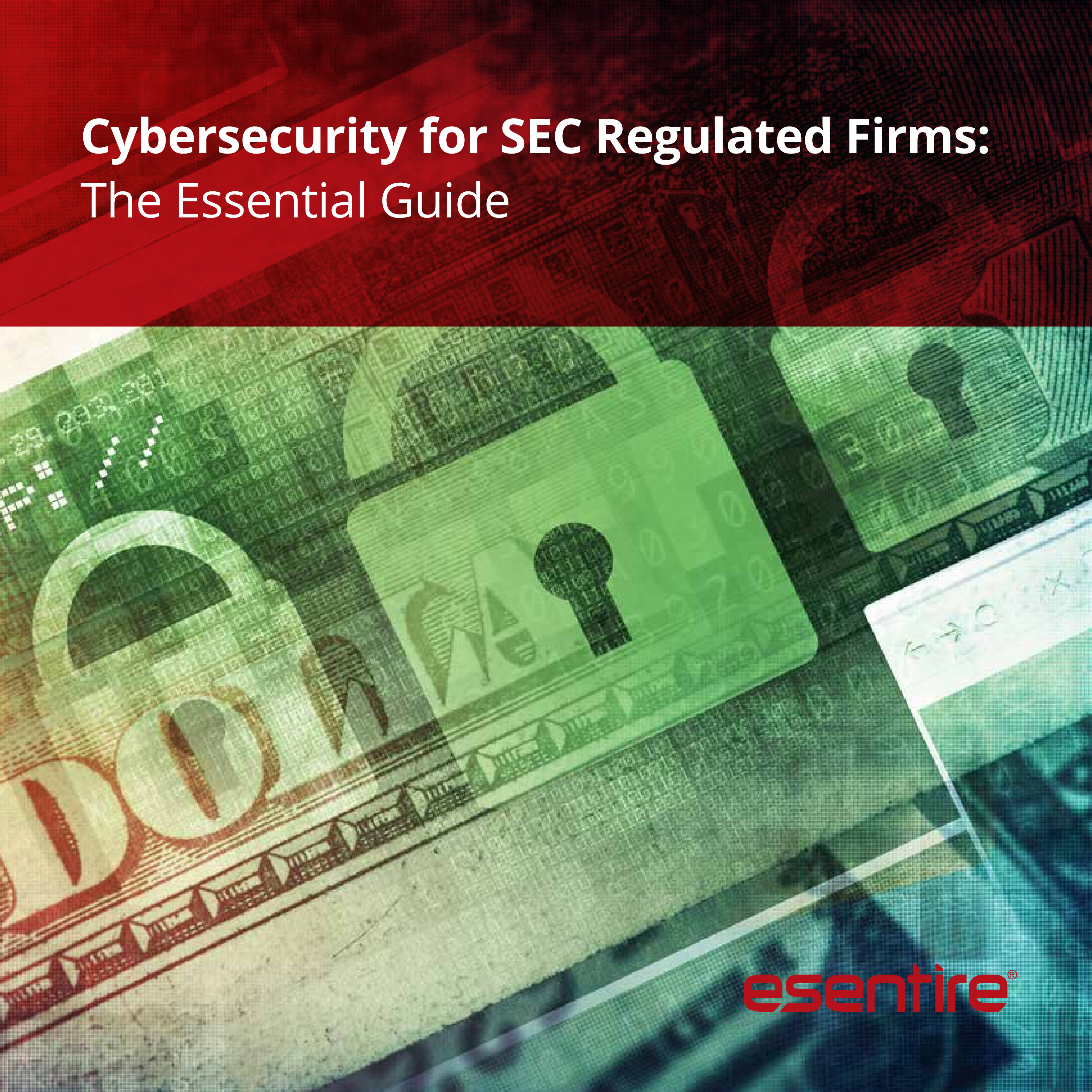
Cybersecurity for SEC Regulated Firms:
The Essential Guide



esentire®

Cybersecurity can no longer be ignored

What's the biggest risk facing the financial services industry? The U.S. Securities and Exchange Commission (SEC) believes the answer is cybersecurity.[1]

In recent years, the number and complexity of cyber-attacks has increased significantly. This has prompted a response from the SEC in the form of exam sweeps, regulatory guidance and fines.

In this eBook, we'll take a look at the current state of the regulatory landscape, the history that led up to it, and what your firm can do to keep up with growing requirements.

[1] https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf

The target is on you.

Cybercriminals will go where the money is.
Cybercrime is a lucrative business and significant financial gain is the primary motivator driving attacks against financial firms. Whether it's access to accounts, trading and investor information, or consumer data, the financial industry holds a wealth of information that can be quickly turned into monetary gain.

Size doesn't matter.
In the past, many small and midsized firms considered themselves too small to be of interest to cybercriminals. Results from the SEC's exam sweep contradict this, revealing that most of the examined firms had been the subject of a cyber-related incident. A majority of the broker-dealers (88%) and the advisors (74%) stated that they have experienced cyber-attacks directly or through one or more of their vendors.[2]

88% of broker-dealers stated that they have experienced cyber-attacks directly or through one or more of their vendors.[2]

[2] http://www.reuters.com/article/us-finance-summit-sec-idUSKCN0Y82K4

A marathon, not a sprint.

Though keeping up with new regulations can feel like an ongoing marathon, it's important for firms to devote time to planning and implementing a comprehensive cybersecurity plan. There is no quick-fix solution to cybersecurity, and those who sprint to the finish line leave room for error in their policies and plans.

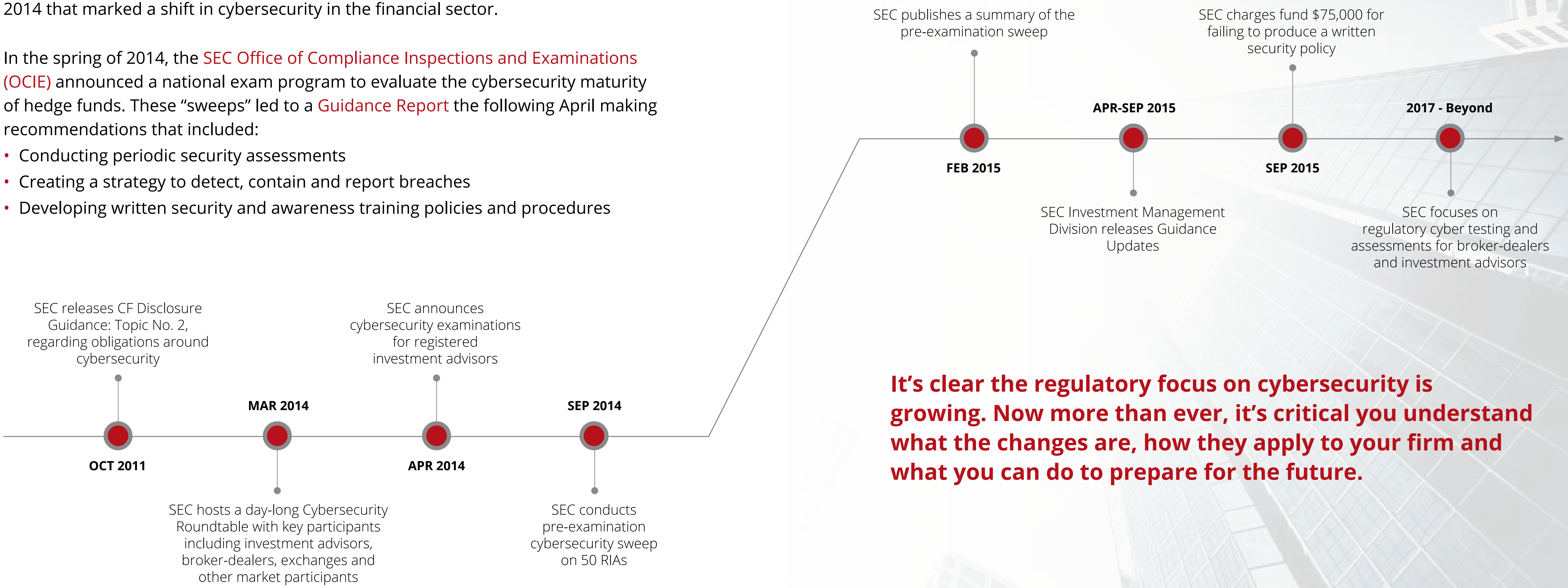
Firms should consider cybersecurity an ongoing program that is flexible and agile to new regulations and never before seen threats.

A look back.

Although the SEC first signaled their concern for industry preparedness in 2011, it was 2014 that marked a shift in cybersecurity in the financial sector.

In the spring of 2014, the SEC Office of Compliance Inspections and Examinations (OCIE) announced a national exam program to evaluate the cybersecurity maturity of hedge funds. These “sweeps” led to a Guidance Report the following April making recommendations that included:

- Conducting periodic security assessments
- Creating a strategy to detect, contain and report breaches
- Developing written security and awareness training policies and procedures



OCT 2011
SEC releases CF Disclosure Guidance: Topic No. 2, regarding obligations around cybersecurity

MAR 2014
SEC hosts a day-long Cybersecurity Roundtable with key participants including investment advisors, broker-dealers, exchanges and other market participants

APR 2014
SEC announces cybersecurity examinations for registered investment advisors

SEP 2014
SEC conducts pre-examination cybersecurity sweep on 50 RIAs

FEB 2015
SEC publishes a summary of the pre-examination sweep

APR-SEP 2015
SEC Investment Management Division releases Guidance Updates

SEP 2015
SEC charges fund $75,000 for failing to produce a written security policy

2017 - Beyond
SEC focuses on regulatory cyber testing and assessments for broker-dealers and investment advisors

It’s clear the regulatory focus on cybersecurity is growing. Now more than ever, it’s critical you understand what the changes are, how they apply to your firm and what you can do to prepare for the future.

Looking ahead.

2015

2015 Cybersecurity Examination Initiative:

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

2016

2016 Cybersecurity Examination Initiative:

- Organizational Purview/Security Governance/Audit Results
- Security Controls, Access Rights and Analysis
- Data-Focused Technology Review–MFA/DLP/Logging/Patch Management
- Vendor Management
- Security Education
- Incident Response Planning

2017

2017 exam priorities released by the SEC stated a continued initiative to examine for cybersecurity compliance procedures and controls, including testing the implementation of those procedures and controls.[3]

In 2017, the SEC is being proactive about cyber examinations and has encouraged firms to be proactive in their approach as well.

Looking beyond surface level defense, the SEC wants an understanding of how deep policies go and how well cybersecurity defenses have been implemented. Firms should be prepared to identify:

- What data they have
- Who has access to it
- How it's stored
- How it's protected

The initiative to increase cybersecurity awareness in the industry is working, but the SEC wants to take that one step further, ensuring that policies and procedures are tailored to particular risks.[3]

[3] https://www.sec.gov/about/offices/ocie/national-examination-program-priorities-2017.pdf

Are you ready?

Cyber threats will continue to evolve, but your priorities should remain consistent when it comes to cybersecurity.

Here's what you should consider when preparing for a cybersecurity-specific exam:

- Do you understand what data you have?
- Do you know what legislation governs the data you have?
- Do you know what cybersecurity threats exist against your firm?
- How are you defending your firm against threats?
- Do you know what access risks exist?
- Can you demonstrate that you're doing what you've claimed?

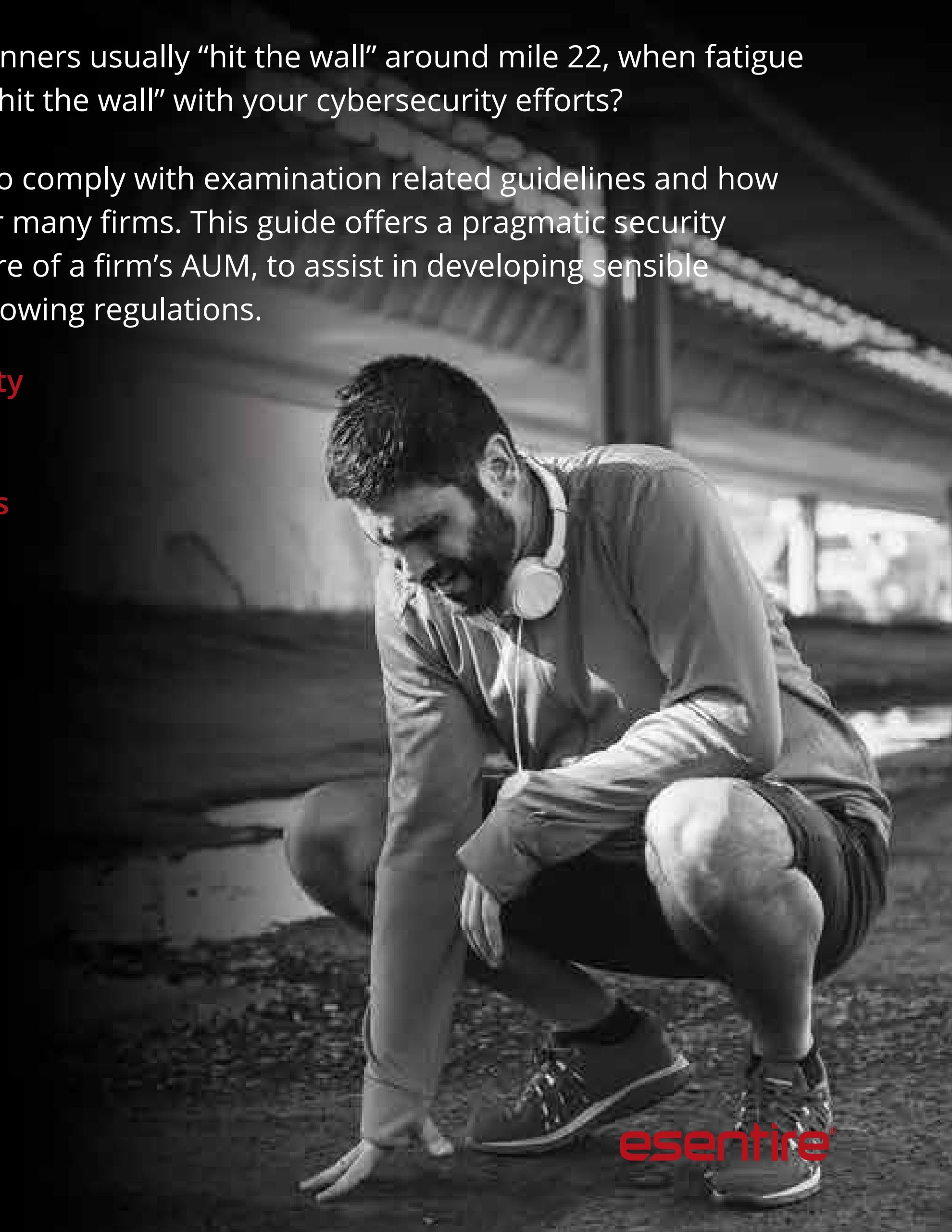
These recommendations may vary depending on a firm's domicile(s), number of employees, technical maturity, regulatory requirements and strategies. It should be recognized that no regulatory body has given approval, either explicit or tacit, to these recommendations. As such, they should be reviewed on their own merits, as deemed appropriate to the firm.

Have you hit the wall? Regulatory Response Guide

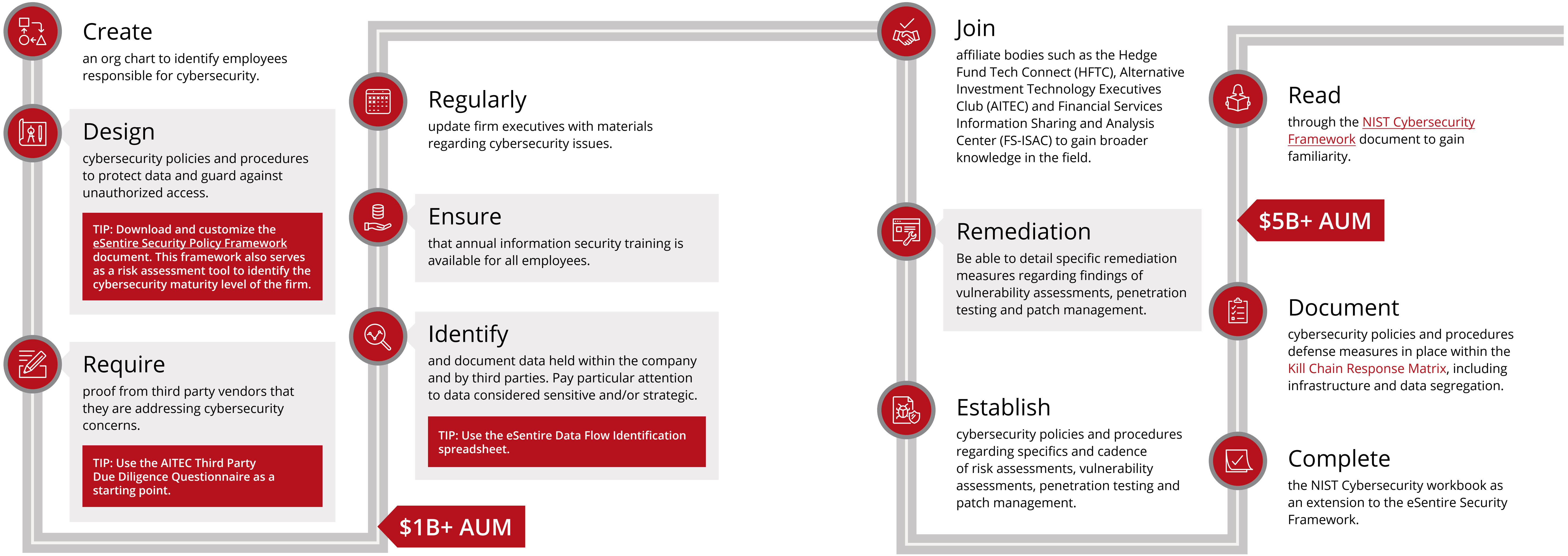
A marathon is 26.2 miles long. Runners usually "hit the wall" around mile 22, when fatigue and exhaustion set in. Have you "hit the wall" with your cybersecurity efforts?

Understanding what is required to comply with examination related guidelines and how you measure up is a challenge for many firms. This guide offers a pragmatic security to-do-list according to the measure of a firm's AUM, to assist in developing sensible approaches to meeting today's growing regulations.

- Organizational Purview Security Governance Policies and Procedures Audit Details ▶
- Security Controls Access Rights and Analysis ▶
- Periodic Cybersecurity Assessments ▶
- Detecting and Responding to Cybersecurity Threats ▶
- Cybersecurity Policies and Procedures (Extended) ▶



Organizational Purview Security Governance Policies and Procedures Audit Details



Create

an org chart to identify employees responsible for cybersecurity.

Design

cybersecurity policies and procedures to protect data and guard against unauthorized access.

TIP: Download and customize the eSentire Security Policy Framework document. This framework also serves as a risk assessment tool to identify the cybersecurity maturity level of the firm.

Require

proof from third party vendors that they are addressing cybersecurity concerns.

TIP: Use the AITEC Third Party Due Diligence Questionnaire as a starting point.

Regularly

update firm executives with materials regarding cybersecurity issues.

Ensure

that annual information security training is available for all employees.

Identify

and document data held within the company and by third parties. Pay particular attention to data considered sensitive and/or strategic.

TIP: Use the eSentire Data Flow Identification spreadsheet.

$1B+ AUM

Join

affiliate bodies such as the Hedge Fund Tech Connect (HFTC), Alternative Investment Technology Executives Club (AITEC) and Financial Services Information Sharing and Analysis Center (FS-ISAC) to gain broader knowledge in the field.

Remediation

Be able to detail specific remediation measures regarding findings of vulnerability assessments, penetration testing and patch management.

Establish

cybersecurity policies and procedures regarding specifics and cadence of risk assessments, vulnerability assessments, penetration testing and patch management.

Read

through the NIST Cybersecurity Framework document to gain familiarity.

$5B+ AUM

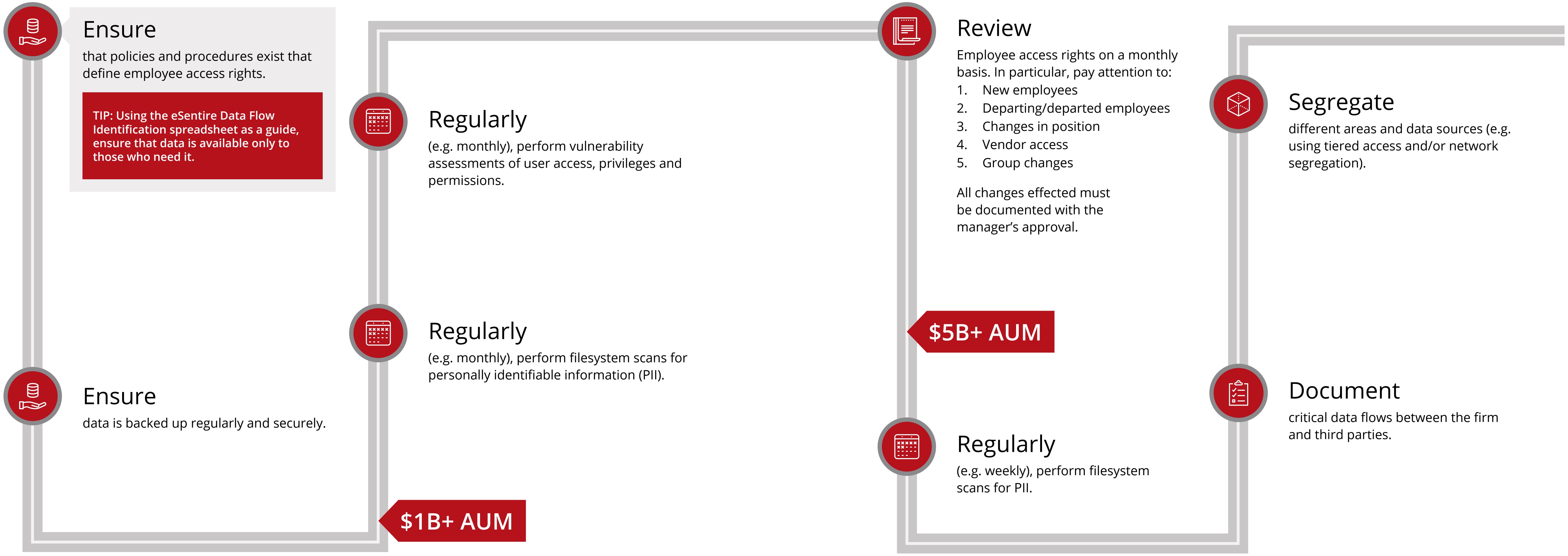
Document

cybersecurity policies and procedures defense measures in place within the Kill Chain Response Matrix, including infrastructure and data segregation.

Complete

the NIST Cybersecurity workbook as an extension to the eSentire Security Framework.

Security Controls
Access Rights and Analysis



Ensure

that policies and procedures exist that define employee access rights.

TIP: Using the eSentire Data Flow Identification spreadsheet as a guide, ensure that data is available only to those who need it.

Ensure

data is backed up regularly and securely.

Regularly

(e.g. monthly), perform vulnerability assessments of user access, privileges and permissions.

Regularly

(e.g. monthly), perform filesystem scans for personally identifiable information (PII).

$1B+ AUM

Review

Employee access rights on a monthly basis. In particular, pay attention to:

1. New employees
2. Departing/departed employees
3. Changes in position
4. Vendor access
5. Group changes

All changes effected must be documented with the manager's approval.

$5B+ AUM

Regularly

(e.g. weekly), perform filesystem scans for PII.

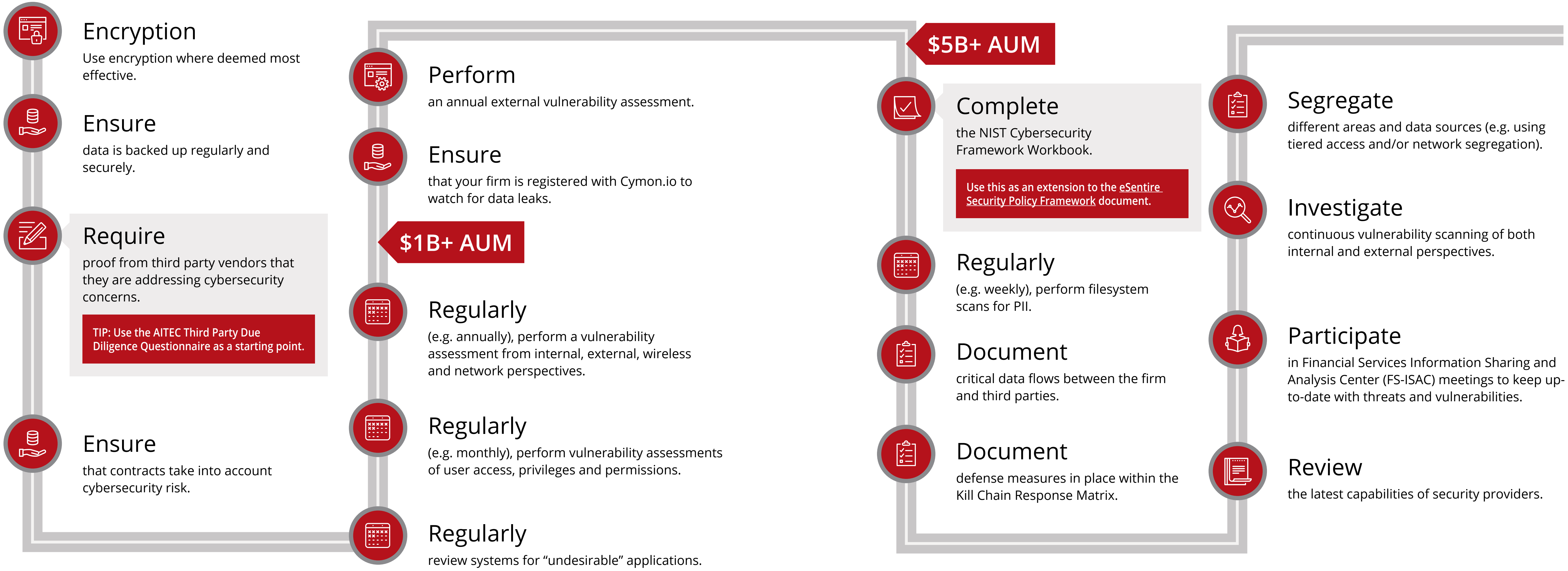
Segregate

different areas and data sources (e.g. using tiered access and/or network segregation).

Document

critical data flows between the firm and third parties.

Periodic Cybersecurity Assessments



Encryption

Use encryption where deemed most effective.

Ensure

data is backed up regularly and securely.

Require

proof from third party vendors that they are addressing cybersecurity concerns.

TIP: Use the AITEC Third Party Due Diligence Questionnaire as a starting point.

Ensure

that contracts take into account cybersecurity risk.

Perform

an annual external vulnerability assessment.

Ensure

that your firm is registered with Cymon.io to watch for data leaks.

$1B+ AUM

Regularly

(e.g. annually), perform a vulnerability assessment from internal, external, wireless and network perspectives.

Regularly

(e.g. monthly), perform vulnerability assessments of user access, privileges and permissions.

Regularly

review systems for “undesirable” applications.

$5B+ AUM

Complete

the NIST Cybersecurity Framework Workbook.

Use this as an extension to the eSentire Security Policy Framework document.

Regularly

(e.g. weekly), perform filesystem scans for PII.

Document

critical data flows between the firm and third parties.

Document

defense measures in place within the Kill Chain Response Matrix.

Segregate

different areas and data sources (e.g. using tiered access and/or network segregation).

Investigate

continuous vulnerability scanning of both internal and external perspectives.

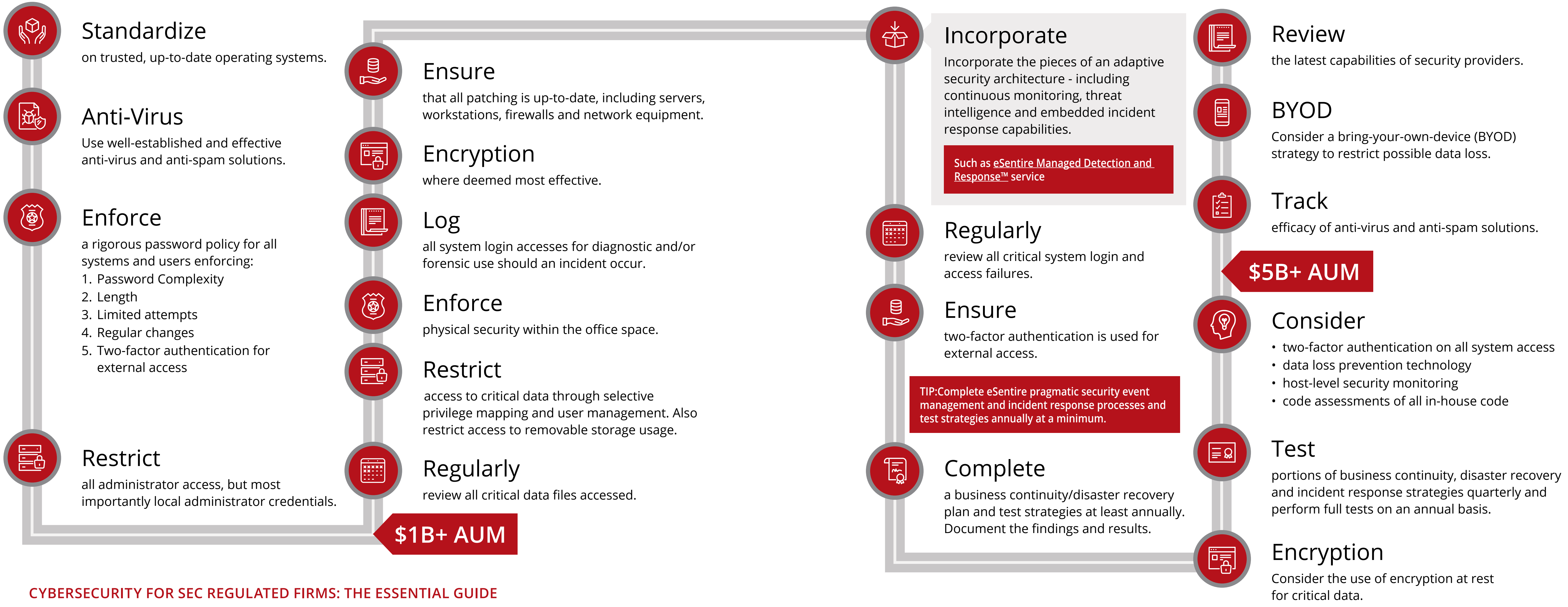
Participate

in Financial Services Information Sharing and Analysis Center (FS-ISAC) meetings to keep up-to-date with threats and vulnerabilities.

Review

the latest capabilities of security providers.

Detecting and Responding to Cybersecurity Threats



Standardize

on trusted, up-to-date operating systems.

Anti-Virus

Use well-established and effective anti-virus and anti-spam solutions.

Enforce

a rigorous password policy for all systems and users enforcing:

1. Password Complexity
2. Length
3. Limited attempts
4. Regular changes
5. Two-factor authentication for external access

Restrict

all administrator access, but most importantly local administrator credentials.

Ensure

that all patching is up-to-date, including servers, workstations, firewalls and network equipment.

Encryption

where deemed most effective.

Log

all system login accesses for diagnostic and/or forensic use should an incident occur.

Enforce

physical security within the office space.

Restrict

access to critical data through selective privilege mapping and user management. Also restrict access to removable storage usage.

Regularly

review all critical data files accessed.

$1B+ AUM

Incorporate

Incorporate the pieces of an adaptive security architecture - including continuous monitoring, threat intelligence and embedded incident response capabilities.

Such as eSentire Managed Detection and Response™ service

Regularly

review all critical system login and access failures.

Ensure

two-factor authentication is used for external access.

TIP:Complete eSentire pragmatic security event management and incident response processes and test strategies annually at a minimum.

Complete

a business continuity/disaster recovery plan and test strategies at least annually. Document the findings and results.

Review

the latest capabilities of security providers.

BYOD

Consider a bring-your-own-device (BYOD) strategy to restrict possible data loss.

Track

efficacy of anti-virus and anti-spam solutions.

$5B+ AUM

Consider

- two-factor authentication on all system access
- data loss prevention technology
- host-level security monitoring
- code assessments of all in-house code

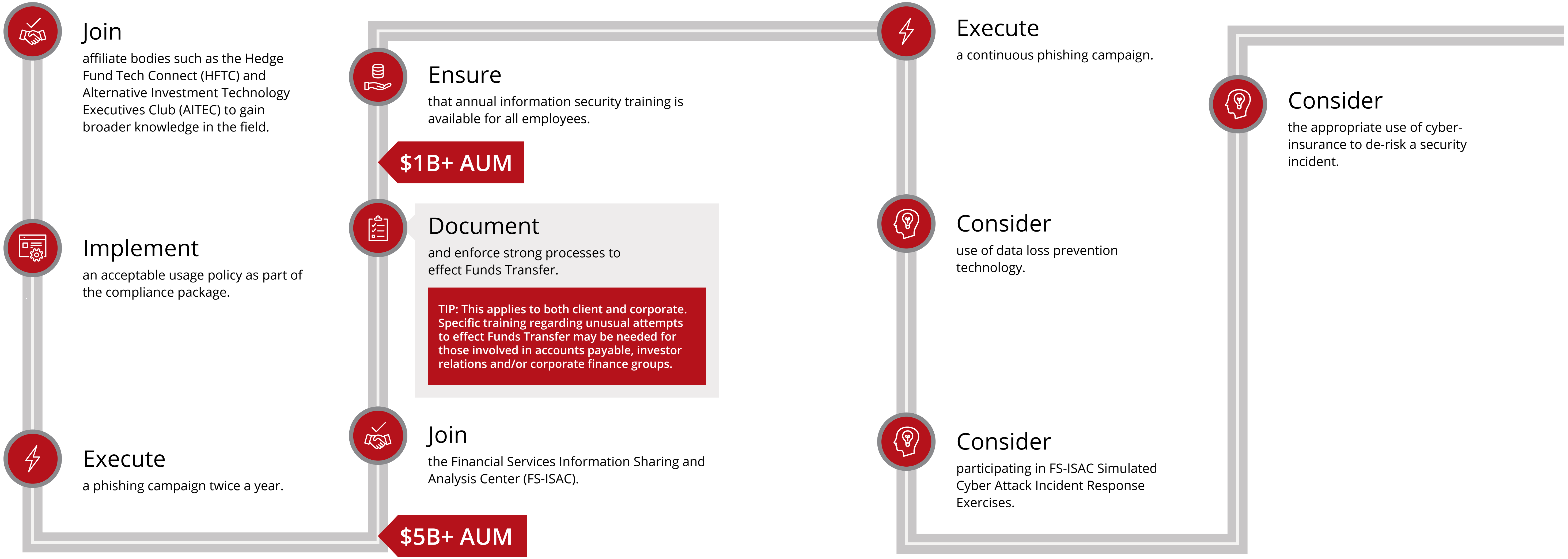
Test

portions of business continuity, disaster recovery and incident response strategies quarterly and perform full tests on an annual basis.

Encryption

Consider the use of encryption at rest for critical data.

Cybersecurity Policies and Procedures (Extended)



Join

affiliate bodies such as the Hedge Fund Tech Connect (HFTC) and Alternative Investment Technology Executives Club (AITEC) to gain broader knowledge in the field.

Implement

an acceptable usage policy as part of the compliance package.

Execute

a phishing campaign twice a year.

Ensure

that annual information security training is available for all employees.

$1B+ AUM

Document

and enforce strong processes to effect Funds Transfer.

TIP: This applies to both client and corporate. Specific training regarding unusual attempts to effect Funds Transfer may be needed for those involved in accounts payable, investor relations and/or corporate finance groups.

Join

the Financial Services Information Sharing and Analysis Center (FS-ISAC).

$5B+ AUM

Execute

a continuous phishing campaign.

Consider

use of data loss prevention technology.

Consider

participating in FS-ISAC Simulated Cyber Attack Incident Response Exercises.

Consider

the appropriate use of cyber-insurance to de-risk a security incident.

Crossing the finish line

The SEC's sustained focus on cybersecurity reinforces the importance of a comprehensive cybersecurity and incident-response program.

Regulatory compliance is not just about checking a box. At the heart of SEC regulations is the recognized need for preparedness in the financial industry. Identifying risks, writing policies and procedures, and having the appropriate defenses in place is essential for your business.

Learn More

Visit www.eSentire.com/resources for workbooks, webinars and other free resources to help you improve your cybersecurity approach.

esentire®

About eSentire:

eSentire® is the largest pure-play Managed Detection and Response (MDR) service provider, keeping organizations safe from constantly evolving cyber-attacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates, and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $6 trillion in corporate assets, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements.

For more information, visit www.esentire.com and follow @eSentire.