RAPID7

WHITE PAPER

Simplifying the complex: Common practices across cybersecurity regulations

An analysis of similarities among cybersecurity practices in regulations across sectors and how organizations can implement those practices.

December 2021

Cybersecurity regulations are complex, target a patchwork of industry sectors, and are enforced by disparate federal, state, and international government agencies. However, many of these regulations share high level cybersecurity requirements. Rapid7 presents this educational resource aimed at breaking down complicated regulatory text into a set of consistent cybersecurity practices. We do this by identifying commonalities across 10 major cybersecurity regulations and categorizing them as core components of organizational security programs.

This white paper also maps how Rapid7's portfolio of solutions can help meet and exceed the cybersecurity practices commonly required by regulations, and provides insight into how organizations can operationalize these practices. Please note: this resource should not be used as a compliance guide, is not legal advice, and is not exhaustive.

Contents

I. Common Cybersecurity Practices Incorporated Into Regulations

Cybersecurity regulations for the private sector often require similar baseline security practices, even though the regulations may structure the compliance requirements differently. Identifying these common elements can help regulated entities, cybersecurity practitioners, and regulators communicate how compliance obligations across sectors translate to operational practices. For example, an organization's security leader could use this approach to drive executive support and investment prioritization by demonstrating how a robust security program addresses an array of compliance obligations facing the organization.

This white paper organizes common regulatory requirements into six categories of cybersecurity practices:

SP

1. **Security Program:** Maintain a comprehensive security program. This may include written administrative, technical, and physical safeguards and procedures to protect the confidentiality, integrity, and availability of sensitive information and systems.

RA

2. **Risk Assessment:** Assess internal and external cybersecurity risks and threats to the confidentiality, integrity, and availability of sensitive information and systems. This may include:
   - Periodically documenting changing risks and threats.
   - Identifying gaps in security program maturity.
   - Inventory and classification of assets.

SS

3. **Security Safeguards:** Implement safeguards to control the risks identified in the risk assessment. This may include:
   - Protecting sensitive information at rest and in transit.
   - Network, software, and application security.
   - User access controls and monitoring.
   - Requiring third party vendors and service providers to maintain safeguards.

TE

4. **Testing and Evaluation:** Assess the effectiveness of policies, procedures, and safeguards to control risks. This may include:
   - Regular testing of information security controls, such as through penetration tests and independent audits.
   - Adjusting security safeguards based on testing results and changes to business operations.

WP

5. **Workforce and Personnel:** Establish security roles and responsibilities for personnel. This may include:
   - Designating personnel to manage the security program.
   - Employee training.
   - Management approval and regular oversight of the information security program.

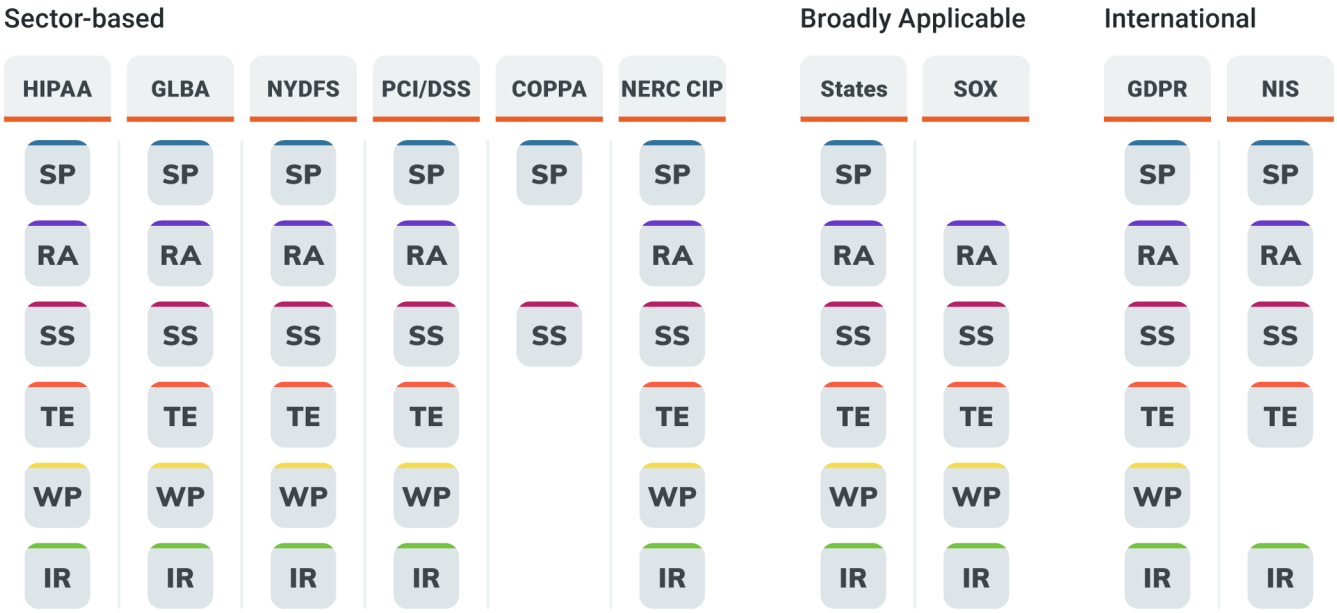
IR

6. **Incident Response:** Detect, investigate, document, and respond to cybersecurity incidents and events. This may include:
   - Monitoring systems to detect actual and attempted attacks or intrusions.
   - Procedures to investigate incidents of unauthorized access to sensitive information or systems.

II. Select Regulations & Requirements

This section demonstrates how the six cybersecurity practices identified in Section I are incorporated into several major regulations. This section also provides additional background information on each regulation, as well as extensive citations to each requirement to enable readers to locate the official text directly. It is important to note that even if a regulation does not specify that a practice is required, the regulating agency may still expect that practice to be implemented.[1]

Overview of practice requirements



A. Sector-Based Requirements

1. Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act (HIPAA) requires that patient medical records and other protected health information (PHI) be safeguarded against security breaches. To help achieve this, the HIPAA Security Rule details administrative, technical, and physical safeguards for electronically stored PHI (e-PHI).[2] The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is empowered to administer and enforce Security Rule requirements, including periodic audits and investigations for compliance. [3]

1 For example, Sarbanes-Oxley does not explicitly require public companies to have an overarching security program. However, the Securities and Exchange Commission has issued guidance to "encourage companies to adopt comprehensive policies related to cybersecurity and to assess their compliance regularly." See Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 18, https://www.sec.gov/rules/interp/2018/33-10459.pdf.
2 45 CFR 164.306.
3 42 USC 17940.

Who is affected

The Security Rule applies to covered entities (including health care providers, retail pharmacies, health plans and insurers, and health care clearinghouses) and business associates of covered entities that store, process, or transmit e-PHI.[4] Business associates are also directly responsible for HIPAA security requirements and subject to HIPAA penalties.[5]

Summary of HIPAA cybersecurity practices

The HIPAA Security Rule requires covered entities and business associates to ensure the confidentiality, integrity, and availability of e-PHI.[6] This includes protecting against any reasonably anticipated threats and unauthorized uses and disclosures of e-PHI.[7] To implement these requirements, the Security Rule prescribes administrative, physical, and technical safeguards — some of which are required, while others need only be addressed as appropriate.[8] Many of these safeguards can be broken down into six fundamental cybersecurity practices: security program, risk assessment, security safeguards, testing and evaluation, workforce and personnel, and incident response.

SP

1. Security Program

- Implement policies and procedures to prevent, detect, and correct security violations.[9]
- Maintain documentation on security policies and procedures.[10]

RA

2. Risk Assessment

- Conduct an assessment of risks to confidentiality, integrity, and availability of e-PHI.[11]
- Evaluate the risks and potential impact to e-PHI in selecting security safeguards.[12]

SS

3. Security Safeguards

- Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable level.[13]
- Guard against malicious software.[14]
- Monitor workforce behavior and implement access controls.[15]
- Secure transmitted e-PHI (such as through encryption).[16]
- Covered entities must require business associates to comply with security safeguards, and business associates must oversee subcontractors.[17]

TE

4. Testing and Evaluation

- Implement procedures to regularly review information system activity, including audit logs, access reports, and security incident tracking.[18]
- Perform periodic evaluations, including in response to environmental or operational changes affecting security, to maintain ongoing compliance of the covered entity and business associates.[19]

4 45 CFR 164.302.
5 Per the Health Information Technology for Economic and Clinical Health Act of 2009. 42 USC 17931(a)-(b).
6 45 CFR 164.306(a)(1).
7 45 CFR 164.306(a)(1)-(2).
8 Where a security measure is not applicable, or is inappropriate or unreasonable, the covered entity must document the decision not to implement the measure. 45 CFR 164.306(d).
9 45 CFR 164.308(a)(1)(i).
10 45 CFR 164.316(b)(1)-(2).
11 45 CFR 164.308(a)(1)(ii)(A).
12 45 CFR 164.306(b)(2).
13 45 CFR 164.308(a)(1)(ii)(B).
14 45 CFR 164.308(a)(5)(ii)(B).
15 45 CFR 164.308(a)(3)-(4), (a)(5)(C)-(D), 312(a), 312(d).
16 45 CFR 164.312(e).
17 45 CFR 164.314(a). See also 45 CFR 308(b).
18 45 CFR 164.308(a)(1)(ii)(D).
19 45 CFR 164.308(a)(8)

WP

5. Workforce and Personnel

- Assign a security official responsible for development and implementation of security policies and procedures.[20]
- Implement security awareness training, as well as supervision procedures, for all workforce.[21]

IR

6. Incident Response

- Implement policies and procedures to identify, respond to, and mitigate security incidents.[22]
- Establish data backup, disaster recovery, and emergency mode operation plans.[23]
- Exercise reasonable diligence in scanning for breaches.[24]
- For a suspected breach, investigate the probability that PHI was compromised based on a risk assessment.[25]
- Maintain logs and documentation of breaches.[26]

Penalties for noncompliance

OCR may resolve noncompliance with voluntary action or resolution agreements, but OCR also has authority to levy penalties for noncompliance with HIPAA security requirements. These penalties include complaint investigations, compliance reviews, and fines.[27] Depending on the conduct, OCR may impose civil penalties ranging from $100 to $50,000 for each violation (per record), and up to $1.5 million for repeated willful violations.[28]

A law enacted in 2021 creates a path for mitigating HIPAA penalties and streamlining audits for organizations with strong security.[29] Under this law, HHS must consider whether covered entities or business associates with "recognized security practices" in place for at least 12 months should have mitigated fines and early termination of audits.[30] The "recognized security practices" are the standards and best practices from several sources: National Institute of Standards and Technology (NIST),[31] the Cybersecurity Act of 2015,[32] and other authorities. Covered entities and business associates that use these recognized security practices must still do so in a way that is consistent with the HIPAA Security Rule.

Further reading

- HHS Security Rule Guidance and Risk Assessment Tool[33]
- Rapid7 HIPAA Compliance Solutions[34]
- Rapid7 Healthcare Industry Solutions[35]
- Rapid7 Healthcare Industry brief[36]
- NIST SP 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule[37]
- Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients[38]

20 45 CFR 164.308(a)(2)
21 45 CFR 164.308(a)(5), 308(a)(3)(ii).
22 45 CFR 164.308(a)(6).
23 45 CFR 164.308(a)(7)(ii).
24 45 CFR 164.404(a)(2).
25 45 CFR 164.402(2).
26 45 CFR 164.408(c).
27 US Department of Health and Human Services, How OCR enforces the HIPAA Privacy and Security Rules, Jun. 7, 2017, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples/how-ocr-enforces-the-hipaa-privacy-and-security-rules/index.html
28 45 CFR 160.404.
29 Pub. Law No. 116-321.
30 The law does not authorize HHS to increase penalties on organizations that choose not to use these "recognized security practices."
31 See NIST Special Publications, https://csrc.nist.gov/publications/sp
32 See Cybersecurity Act Section 405(d) Task Group, https://www.phe.gov/Preparedness/planning/405d/Pages/default.aspx
33 https://www.hhs.gov/hipaa/for-professionals/security/guidance/index.html
34 https://www.rapid7.com/solutions/compliance/hipaa/
35 https://www.rapid7.com/solutions/industry/healthcare
36 https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-healthcare-industry-brief.pdf
37 https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf
38 https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf

2. Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions to protect customer information.[39] Enforcement of GLBA is divided among several federal regulators, depending on the type of financial institution: FTC, FFIEC, SEC, and CFTC. Several of these regulators have issued rules that expand upon the GLBA security requirements.[40]

Who is affected

GLBA's security requirements apply to a wide range of "financial institutions," covering most businesses that offer any financial products and services.

- **Non-bank financial institutions** are covered under the Federal Trade Commission (FTC) Safeguards Rule.[41]
- **Banking financial institutions** are covered under the Federal Financial Institutions Examination Council (FFIEC) Interagency Guidelines Establishing Information Security Standards.[42]
- **SEC-registered financial institutions** are covered under the Security and Exchange Commission's (SEC) Safeguards Rule.[43]
- **CFTC-covered financial institutions** are covered under the Commodity Futures Trading Commission (CFTC) Security Safeguards.[44]

Summary of GLBA cybersecurity practices

GLBA requires all financial institutions to have a comprehensive security program to protect customer information.[45] On that foundation, the different GLBA regulatory agencies have issued guidance (with varying levels of detail) on what this security requirement entails.[46] The FTC regulations and FFIEC guidelines are generally more specific than the SEC regulations and CFTC guidance. However, even if an agency does not specify that a particular cybersecurity practice is required, the practice may still fall under the general obligation of having a comprehensive security program.

SP

1. Security Program

- Implement a comprehensive information security program with administrative, technical, and physical safeguards to ensure the security, integrity and confidentiality of customer information.[47]

RA

2. Risk Assessment

- Identify internal and external risks and threats to customer information that could result in unauthorized disclosure, misuse, or alteration of the information.[48]

39 15 USC 6801(b). Note: "customers" does not include all consumers.
40 15 USC 6805(a).
41 16 CFR 314.3-314.4. This includes some retailers, automobile dealers, mortgage brokers, nonbank lenders, property appraisers, tax preparers, and others non-bank businesses that offer financial products or services. This also includes entities that are "significantly engaged in activities that are incidental to financial activity." 16 CFR 314.2(h)(1)-(4). The FTC updated the Safeguard Rule in 2021, though several parts of that updated rule have not yet gone into effect at the time of this writing: https://www.ftc.gov/news-events/press-releases/2021/10/ftc-strengthens-security-safeguards-consumer-financial
42 66 Fed. Reg. 8615, 8616-8641. FFIEC includes principals from the Federal Reserve Board of Governors, Federal Deposit Insurance Corporation, National Credit Union Administration, Comptroller of the Currency, Consumer Financial Protection Bureau, and State Liaison Committee. This includes commercial and savings banks, state member banks, bank holding companies, credit unions, and their non-bank subsidiaries. See 12 CFR 30, App. B (national banks); 12 CFR 208, App. D-2 and 255, App. F (state member banks and holding companies); 12 CFR 364, App. B (state non-member banks); 12 CFR 570, App. B (savings associations); 12 CFR 748, App. A (credit unions).
43 17 CFR 248.30. See also SEC Regulation S-P. This includes brokers, dealers, investment companies, and investment advisors. 17 CFR 248.1.
44 7 USC 7b-2. This includes commodity trading advisors, futures commission merchants, commodity pool operators, introducing brokers, retail foreign exchange dealers, swap dealers and participants. 17 CFR 160. See also CFTC Staff Advisory No. 14-21 (2014), https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf
45 "Customer information" is any record with nonpublic personal information about a customer of a financial institution. 16 CFR 314.2(d).
46 See the footnote references for what each agency requires. See also "Further reading" on regulators' best practices guidance.
47 16 CFR 314.3 (FTC). Security Guidelines II.A-B (FFIEC). 17 CFR 248.30(a) (SEC). 17 CFR 160.30 (CFTC).
48 16 CFR 314.4(b) (FTC). Security Guidelines III.B (FFIEC). 17 CFR 248.30(a)(2) (SEC). CFTC Staff Advisory No. 14-21, Best Practice 2.

SS

3. Security Safeguards

- Implement administrative, technical, and physical safeguards to control risks identified in the risk assessment.[49]
- Implement access controls on customer information systems.[50]
- Encrypt customer information in storage and in transit.[51]
- Require service providers to maintain safeguards.[52]

TE

4. Testing and Evaluation

- Regularly assess the effectiveness of safeguards.[53] For the FTC Safeguards Rule, this includes either continuous monitoring or periodic penetration tests and vulnerability assessments.[54]
- Adjust the security program in light of testing results.[55]

WP

5. Workforce and Personnel

- Designate an employee to implement the security program.[56]
- Train employees in the security program.[57]
- The Board of Directors (or equivalent) must oversee the security program, and management must report to the Board annually on all material matters related to the program.[58]
- Select and oversee service providers capable of maintaining safeguards.[59]

IR

6. Incident Response

- Implement procedures to detect and respond to attacks, intrusions, and system failures.[60]
- Monitor systems to detect attempted attacks, assess and investigate incidents, and take steps to contain and mitigate incidents.[61]

Penalties for noncompliance

The penalty for noncompliance with GLBA security requirements depends on the conduct, the type of institution, and harm to individuals. The penalties may include civil fines, injunctions, redress to consumers for loss, disgorgement of profits, as well as revocation of licenses.[62] Civil fines can range up to $100,000 for each violation, and officers and directors can be fined up to $10,000 for each violation and even face imprisonment.

49 16 CFR 314.4(c) (FTC). Security Guidelines III.C.1 (FFIEC). 17 CFR 248.30(a)(3) (SEC). CFTC Staff Advisory No. 14-21, Best Practice 3. The safeguards should be "appropriate" for identified risks, commensurate with the sensitivity of the information and complexity and scope of the company's activities.
50 16 CFR 314.4(c)(1) [updated 2021 rule] (FTC). Security Guidelines III.C.1.a (FFIEC), as appropriate.
51 16 CFR 314.4(b)(2) (FTC). 16 CFR 314.4(c)(3) [updated 2021 rule] (FTC). Security Guidelines III.C.1.c (FFIEC), as appropriate.
52 16 CFR 314.4(d)(2) (FTC). 16 CFR 314.4(f)(2) [updated 2021 rule] (FTC). Security Guidelines III.D (FFIEC).
53 16 CFR 314.4(c), (e) (FTC). 16 CFR 314.4(d) [updated 2021 rule] (FTC), includes regular penetration tests and vulnerability assessments. Security Guidelines III.C.3 (FFIEC), tests should be conducted by independent third parties or independent staff. CFTC Staff Advisory No. 14-21, Best Practices 5-6.
54 16 USC 314.4(d) [updated 2021 rule] (FTC).
55 16 CFR 314.4(e) (FTC). 16 CFR 314.4(g) [updated 2021 rule] (FTC). Security Guidelines III.E (FFIEC). CFTC Staff Advisory No. 14-21, Best Practice 8.
56 16 CFR 314.4(a) (FTC). CFTC Staff Advisory No. 14-21, Best Practice 1.
57 16 CFR 314.4(b)(1) (FTC). 16 CFR 314.4(e) [updated 2021 rule] (FTC). Security Guidelines III.C.2 (FFIEC), as appropriate. CFTC Staff Advisory No. 14-21, Best Practice 4.
58 16 CFR 314.4(i) [updated 2021 rule] (FTC). Security Guidelines III.A, F (FFIEC). CFTC Staff Advisory No. 14-21, Best Practice 10.
59 16 CFR 314.4(d)(1) (FTC). 16 CFR 314.4(f)(1) [updated 2021 rule] (FTC). CFTC Staff Advisory No. 14-21, Best Practice 7.
60 16 CFR 314.4(b)(3) (FTC). 16 CFR 314.4(h) [updated 2021 rule] (FTC). The FTC has opined that incident response is generally required. See https://www.federalregister.gov/d/2019-04981/p-50 Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice. 70 Fed. Reg. 15736, See also Supp. A to App. B to 12 CFR 30 (FFIEC). The SEC has opined that an inadequate incident response plan is deficient for purposes of complying with GLBA, Investment Advisor and Broker-Dealer Compliance Issues Related to Regulation S-P - Privacy Notices and Safeguard Policies, https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf. CFTC Staff Advisory No. 14-21, Best Practice 9.
61 Response Programs Guidance II.A-III.A (FFIEC).
62 15 USC 6805. See, for example, SEC, Regulated Entities – Cybersecurity Controls and Safeguarding Customer Information, https://www.sec.gov/spotlight/cybersecurity-enforcement-actions See also, FTC Enforcement Overview, https://www.ftc.gov/about-ftc/what-we-do/enforcement-authority Note: FTC does not have civil penalty authority for GLBA violations.

Further reading

- FTC Safeguards Rule compliance guidance[63]
- FTC 2021 updates to the Safeguards Rule[64]
- FFIEC Cybersecurity Assessment Tool[65]
- SEC Office of Compliance Inspections and Examinations Guidance[66]
- CFTC Staff Advisory on GLBA Security Safeguards[67]
- Rapid7 Financial Services Security Solutions[68]

3. New York Department of Financial Services (NYDFS)

The NYDFS issued its Cybersecurity Regulation to require comprehensive cybersecurity practices for information systems of financial institutions doing business in New York.[69]

Who is affected

Organizations regulated, chartered, or licensed by NYDFS are covered. This includes financial institutions doing business in New York such as state-chartered banks, trust companies, private bankers, mortgage companies, insurance companies, licensed lenders, and non-US banks. Small companies have limited exemptions.[70]

Summary of NYDFS cybersecurity practices

SP

1. Security Program

- Maintain a cybersecurity program designed to protect the confidentiality, integrity, and availability of information systems.[71]

RA

2. Risk Assessment

- Conduct periodic risk assessments, responsive to technological developments, evolving threats, and business operations.[72]
- Perform asset inventory and device management.[73]

SS

3. Security Safeguards

- Implement safeguards to control risks identified in the risk assessment.[74] Depending on the risks, this may include protecting sensitive information in storage and transit,[75] systems and network monitoring,[76] access privileges and authentication controls,[77] monitoring users to prevent unauthorized access,[78] application security,[79] and maintaining audit trails and logs.[80]
- Require service providers to implement security measures and oversee the providers.[81]

63 https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying
64 https://www.ftc.gov/system/files/documents/federal_register_notices/2021/10/safeguards_rule_final.pdf
65 https://www.ffiec.gov/cyberassessmenttool.htm
66 https://www.sec.gov/files/OCIE%20Risk%20Alert%20-%20Regulation%20S-P.pdf
67 https://www.cftc.gov/sites/default/files/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf
68 https://www.rapid7.com/solutions/industry/financial-services/
69 23 NYCRR 500.
70 23 NYCRR 500.19(a)(1)-(3). Companies with less than 10 employees, or less than $5M annual revenue, or less than $10M in assets must still implement a cybersecurity program that meets some (but not all) of the regulatory requirements.
71 23 NYCRR 500.02(a), 500.03.
72 23 NYCRR 500.09.
73 23 NYCRR 500.03(c).
74 23 NYCRR 500.03.
75 23 NYCRR 500.15.
76 23 NYCRR 500.03(h).
77 23 NYCRR 500.07, 500.12.
78 23 NYCRR 500.14(a).
79 23 NYCRR 500.08.
80 23 NYCRR 500.06.
81 23 NYCRR 500.11.

TE

4. Testing and Evaluation

- The cybersecurity program must include continuous monitoring or annual penetration testing and bi-annual vulnerability scanning.[82]

WP

5. Workforce and Personnel

- Designate a Chief Information Security Officer (may be affiliate or service provider) responsible for overseeing the cybersecurity program.[83]
- Report annually to the Board of Directors (or equivalent) on the cybersecurity program, events, and risks.[84]
- Senior officer or the Board must approve cybersecurity policies.[85]
- Select and continuously train qualified cybersecurity personnel and staff (may be affiliate or service provider).[86]

IR

6. Incident Response

- Implement processes to detect, respond to, mitigate, and recover from cybersecurity events.[87]
- Report material cybersecurity events to the NYDFS Superintendent.[88]

Penalties for noncompliance

The Cybersecurity Regulation does not specify a penalty, but may be enforced under NYDFS authorities. Depending on the conduct and institution, NYDFS may levy civil penalties ranging from $2,500 per day to $75,000 per day, consent orders, or revocation of licensure.[89]

Further reading

- NYDFS Cybersecurity Resource Center[90]
- NYDFS Insurance Circular Letter No. 2[91]
- Rapid7 NYDFS Solution Guide[92]

82 23 NYCRR 500.05(a)-(b).
83 23 NYCRR 500.04(a).
84 23 NYCRR 500.04(b)
85 23 NYCRR 500.03.
86 23 NYCRR 500.10; 500.14(b).
87 23 NYCRR 500.16.
88 23 NYCRR 500.17.
89 Depending on the entity. For example, New York Banking Law Sections 39, 44, and 44-a; Financial Services Law Sections 301-302, 408.
90 https://www.dfs.ny.gov/industry_guidance/cybersecurity
91 https://www.dfs.ny.gov/industry_guidance/circular_letters/cl2021_02
92 https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-nydfs-consulting-services-brief.pdf

4. Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is a non-regulatory standard to strengthen the security of payment card processing globally, reduce fraud, and prevent breaches. PCI DSS details security management requirements and testing procedures, with greater levels of validation for organizations with higher card transaction volumes.[93] There are a large number of requirements, though many fall under the six broad categories of common cybersecurity practices embedded across other regulations.

Who is affected

This standard applies to all entities involved in processing payment, debit, and credit cards from major providers. This includes merchants, processors, issuers, and service providers that process or transmit cardholder data. [94]

Summary of PCI DSS cybersecurity practices

SP

1. Security Program

- Maintain a written policy that addresses security for all personnel.[95]
- Review and update the security policy at least annually.[96]

RA

2. Risk Assessment

- Perform and document a risk assessment at least annually.[97] Identify assets, threats, and vulnerabilities.

SS

3. Security Safeguards

- Maintain a firewall configuration to protect cardholder data.[98]
- Do not use vendor-supplied passwords, accounts, or other default parameters.[99]
- Protect cardholder data in storage and in transit.[100]
- Detect and remove malicious software, and regularly update anti-virus software.[101]
- Maintain secure systems and applications, including processes to identify security vulnerabilities.[102]
- Establish user access controls and monitor all access to data.[103]
- Track and monitor all access to network resources and cardholder data. [104]
- Require service providers to maintain security[105] and oversee compliance. [106]

TE

4. Testing and Evaluation

- Regularly test security systems and processes. [107]
- Perform internal and external vulnerability scans at least quarterly.[108]
- Perform internal and external penetration tests at least annually.[109]

93 PCI DSS v.3.2.1, https://www.pcisecuritystandards.org/documents/PCI_DSS_v3-2-1.pdf
94 PCI DSS, pg. 5. These standards are primarily enforced through contract relationships.
95 PCI DSS, 12.1, 12.3.
96 PCI DSS, 12.1.1.
97 PCI DSS, 12.2.
98 PCI DSS, 1.
99 PCI DSS 2.
100 PCI DSS, 3-4.
101 PCI DSS, 5.
102 PCI DSS, 6.
103 PCI DSS, 7-9.
104 PCI DSS, 10.
105 PCI DSS, 12.8. Applies to service providers with whom cardholder data is shared, or that could affect the security of cardholder data.
106 PCI DSS, 12.8.3-12.8.5.
107 PCI DSS, 11.
108 PCI DSS, 11.2.
109 PCI DSS, 11.3.

WP

5. Workforce and Personnel

- Ensure security policy and procedures define information security responsibilities for all personnel.[110]
- Assign information security responsibilities to Chief Security Officer or qualified manager.[111]
- Train personnel and service providers on information security policies and procedures.[112]

IR

6. Incident Response

- Create an incident response plan, including detection and alerts for intrusions, business recovery, and analysis of legal requirements.[113] Implement the plan in the event of breach.

Penalties for noncompliance

- Payment card brands may fine the banks serving the violator $5,000-$100,000 per month, which may prompt the bank to increase transaction fees on the non-compliant business or drop the business altogether.[114]
- Revocation of ability to accept or process payment cards.

Further reading

- PCI DSS Document Library[115]
- Rapid7 PCI DSS Compliance Solutions[116]

5. Children's Online Privacy Protection Act (COPPA)

COPPA requires online services to provide protections for the collection of children's personal information.[117] COPPA includes both security and privacy requirements (for example, obtaining parental consent), though this overview focuses on the security requirements. COPAA is enforced by the Federal Trade Commission.[118]

Who is affected

This law applies to any individual or company under US jurisdiction who operates a website or an online service for commercial purposes and knowingly collects individually identifiable information from children under 13 online.[119]

Summary of COPPA cybersecurity practices

SP

1. Security Program

- Establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children online.[120]

110 PCI DSS, 12.4.
111 PCI DSS, 12.5.
112 PCI DSS, 12.6-12.8, 12.10.4.
113 PCI DSS, 12.10.
114 https://www.pcicomplianceguide.org/faq/#15
115 https://www.pcisecuritystandards.org/document_library
116 https://www.rapid7.com/solutions/compliance/pci-dss/
117 16 CFR 312.3.
118 16 CFR 312.9.
119 16 CFR 312.2.
120 16 CFR 312.3(e), 312.8.

SS

2. Security Safeguards

- Take reasonable steps to disclose children's personal information only to service providers who will maintain the confidentiality, security, and integrity of the information.[121]
- Delete children's personal information using reasonable measures to protect against unauthorized access and use.[122]

Penalties for noncompliance

Civil penalties of up to more than $40,000 per violation, injunctions, and settlement orders under Sec. 5 of the FTC Act.[123] Civil penalties can range to millions of dollars.[124]

Further reading

- FTC enforcement and resource page for COPPA[125]

6. North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)

NERC is a nonprofit organization that operates as a regulatory authority for the North American bulk power system.[126] NERC develops and enforces standards to ensure the reliability and safety of the bulk power system, including the CIP standards to strengthen cybersecurity. NERC also regularly assesses system reliability, and trains and certifies industry personnel. NERC is subject to oversight by the Federal Energy Regulatory Commission, as well as other international government agencies.[127]

Who is affected

All bulk power system owners and operators must comply with approved NERC reliability standards.[128] This includes control centers and backup centers, transmission stations and substations, electricity generation resources, system restoration facilities, and power generation facilities — which together create, protect, and transport electric power to hundreds of millions of users throughout North America.[129]

Summary of NERC CIP cybersecurity practices

NERC CIP is presently composed of twelve enforceable standards, nearly all of which are directly related to cybersecurity.[130] These detailed standards use a risk management approach to require a baseline level of organizational, operational, and procedural controls to mitigate risks to bulk electric system assets. Low impact systems have less stringent safeguard requirements, while high impact systems have more stringent requirements.[131] Below, we organize CIP standard requirements around the six fundamental cybersecurity practices commonly found across other regulations.

121 16 CFR 312.8. The FTC has opined that this includes periodically monitoring service providers and third parties to whom children's personal information is disclosed, to ensure they maintain the confidentiality and security of that information. See "Disclosure of information to third parties," https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions-0#COPPA%20Enforcement

122 16 CFR 312.10.

123 16 CFR 312.9. See also "COPPA enforcement," https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#COPPA%20Enforcement

124 See, for example, the $170 million penalty YouTube and Google paid to settle COPPA claims in 2019, https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc

125 https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

126 NERC was designated an Electric Reliability Organization under the Federal Power Act. 16 USC 824o.

127 https://www.nerc.com/AboutNERC/Pages/default.aspx

128 16 USC 824o(e).

129 https://www.nerc.com/pa/Stand/2018_Bulk_Electric_System_Definition_Reference/BES_Reference_Doc_08_08_2018_Clean_for_Posting.pdf

130 https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx

131 The classification is based in part on the severity of consequences if the system is destroyed, degraded, misused, or otherwise unavailable. See CIP-002-5.1a, Attachment 1, Impact Rating Criteria.

SP

1. Security Program

- Implement and document cybersecurity policies that address required security practices.[132] This may be a single comprehensive policy, or a high-level umbrella policy with more detailed policies for each of the required practices.[133]

RA

2. Risk Assessment

- Identify and categorize all bulk electric system cyber assets for high, medium, and low impact systems.[134] This is to support appropriate security safeguards against loss, compromise, or misuse. Review every 15 months.[135]

SS

3. Security Safeguards

Implement processes for high and medium impact bulk electrical systems that address, among other things:

- Electronic security perimeters, including secure firewall configurations and security safeguards for remote access.[136]
- Electronic access controls, password and account management, employee access authorizations based on role.[137]
- System security management, including vulnerability mitigation and patch management, logical port restrictions, methods to detect and mitigate malicious code.[138]
- Perform an active vulnerability assessment of new assets for high impact bulk electric systems.[139]
- Establish a baseline configuration for software, ports, and security patches. Verify the identity, integrity, and impact on security controls for software that deviates from the baseline.[140]
- Information protection, including procedures for protecting system information during storage, transit, use, and disposal.[141]
- Supply chain risk management, including assessing risks from vendor products, disclosure by the vendor of known vulnerabilities, and notification by the vendor of cybersecurity incidents.[142]

TE

4. Testing and Evaluation

For high and medium impact bulk electrical systems:

- At least every 15 months, conduct a paper or active vulnerability assessment. Document results and evaluate mitigations.[143]
- Test the cybersecurity incident response and recovery plans at least once every 15 months. Update the plans as needed based on lessons learned.[144]
- At least every 15 months, review personnel access privileges to protected information to confirm that privileges are appropriate.[145]

WP

5. Workforce and Personnel

- Designate a CIP Senior Manager to be responsible for strategic planning, executive-level awareness, and overall program governance for CIP.[146]

132 CIP-003-8 R1-R2. Failure to implement and document the cybersecurity policy is noted as a potential violation. See CIO-003-8, Security Management Controls, pg. 8.
133 CIP-003-8, Guidelines and Technical Basis, pg. 29.
134 CIP-002-5.1a R1. An inventory list of low impact systems is not required.
135 CIP-002-5.1a R2.
136 CIP-005-6 R1-R2.
137 CIP-007-6 R5. CIP-004-6 R4-R5.
138 CIP-007-6 R1-R3.
139 CIP-010-3 R3.3.
140 CIP-010-3 R1.
141 CIP-011-2 R1.2.
142 CIP-013-1 R1-R2.
143 CIP-010-3 R3.1-3.2.
144 CIP-008-6 R2-3.1. CIP-009-6 R2-3.1.
145 CIP-004-6 R4.3.
146 CIP-003-8 R3-R4. See NERC, CIP-003-8 Supplemental Material, pg. 55, https://www.nerc.com/_layouts/15/PrintStandard.aspx?standardnumber=CIP-003-8&title=Cyber%20Security%20%E2%80%94%20Security%20Management%20Controls&Jurisdiction=United%20States

- Obtain CIP Senior Manager approval for cybersecurity policies, asset classification, and the supply chain risk management plan at least every 15 months.[147]
- For medium and high-impact systems: Reinforce security awareness at least each quarter. Implement cybersecurity training programs for personnel based on roles and responsibilities at least every 15 months.[148] Conduct background checks on employees.[149]

IR

6. Incident Response

For high and medium impact bulk electrical systems:

- Maintain processes for event logging and alerts, including failed access attempts and presence of malicious code.[150]
- Maintain a cybersecurity incident response plan, including processes to identify, classify, and respond to incidents.[151] Provide detailed notification of reportable incidents to authorities.[152]
- Maintain a system recovery plan, including backup and storage of information needed to restore functionality, preserving data to determine the cause of a cybersecurity incident.[153]

Penalties for noncompliance

Penalties for noncompliance with CIP standards can include orders to mitigate violations and track improvements, as well as civil fines ranging to more than a million dollars per violation, per day.[154] The penalty depends heavily on factors such as the violation severity, duration, and whether it is a repeat offense.[155] For example, in 2019 NERC issued a $10 million fine to an organization due to numerous violations of CIP standards.[156]

Many regulated entities self-report compliance issues. NERC also works with regional reliability organizations to enforce CIP standards with periodic audits, spot checks, and compliance assessments.[157]

Further reading

- NERC CIP Standards[158]
- Federal Energy Regulatory Commission Cyber and Grid Security Resources[159]
- Rapid7 Cloud Security and Compliance Guide for the Energy and Utilities Industry[160]
- Rapid7 NERC Compliance Programs and Solutions[161]

147 CIP-003-8 R1. CIP-002-5.1a R2. CIP-013-1 R3.
148 CIP-004-6 R1-R2. Training must include cybersecurity policies, access controls, cyber incident detection and response, and cybersecurity risks.
149 CIP-004-6 R3.
150 CIP-007-6 R4.
151 CIP-008-6 R1.
152 CIP-008-6 R4.
153 CIP-009-6 R1-R2.
154 NERC Sanction Guidelines, Jan. 19, 2021, pg. 4, https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%204B%20effective%2020210119.pdf
155 https://www.nerc.com/FilingsOrders/us/RuleOfProcedureDL/Appendix%204B%20effective%2020210119.pdf
156 Note: NERC does not release the names of penalized organizations. After 2020, NERC releases limited information regarding violations. https://www.nerc.com/pa/comp/CE/Enforcement%20Actions%20DL/Public_FinalFiled_NOP_NOC-2605_Part%201.pdf
157 https://www.nerc.com/pa/comp/Pages/AboutComplianceOperations.aspx
158 https://www.nerc.com/pa/Stand/Pages/CIPStandards.aspx
159 https://www.ferc.gov/industries-data/electric/industry-activities/cyber-and-grid-security
160 https://www.rapid7.com/info/cloud-security-energy-and-utilities-guide/
161 https://www.rapid7.com/solutions/compliance/nerc-cip/

B. Broadly Applicable Requirements

7. State Data Security Laws (CA, FL, MA, NY, TX)

At least half of US states have laws requiring security for personal information held by businesses and private sector entities, and all US states have breach notification laws. States with data security laws include AL, AK, CA, CO, CT, DE, FL, IL, IN, KS, LA, MD, MA, MN, NE, NV, NM, NY, OH, OR, RI, SC, TX, UT, VA, VT, plus DC.[162] More states are taking on these requirements as time goes by.

Who is affected

Most state data security laws apply to persons conducting business in the state. Some states, such as CA and NY,[163] apply security requirements to businesses regardless of location that process personal information of state residents. Several states, such as CA, IL, and NY, exempt businesses that are in compliance with industry sectoral regulations, such as GLBA and HIPAA.[164]

Summary of state data security law cybersecurity practices

These state laws generally require safeguards to protect "personal information," though the laws provide varying levels of detail for the required safeguards. For example, Massachusetts and New York include some of the most detailed guidance on security compliance.[165] However, even if a state law does not specify that a particular security practice is required, the practice may still fall under the state's overarching requirement of safeguards to protect personal information. For this overview, we focus especially on data security laws in California, Florida, Massachusetts, New York, and Texas.[166]

SP

1. Security Program

- Businesses must maintain a comprehensive security program with administrative, technical, and physical safeguards for personal information.[167]

RA

2. Risk Assessment

- Identify internal and external risks to the security of personal information.[168]
- This can include risks to networks and software as well as information processing, transmission, and storage.[169]

SS

3. Security Safeguards

- Implement reasonable safeguards to protect private information from security risks.[170] This may include protecting against unauthorized access, use, or disclosure of private information. [171]
- Require third party service providers to maintain safeguards.[172]

162 See https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws
163 CA: Cal. Civ. Code 1798.81.5(a)-(b), 1798.150. NY: NY Gen. Bus. Law 899-bb(1)(a).
164 CA: Cal. Civ. Code 1798.145(c)(1). IL: 815 ILCS 530/50. NY: NY Gen. Bus. Law 899-bb(1)(a)(i)-(ii).
165 MA: 201 CMR 17.03(1). NY: 21 NY Gen. Bus. Law 899-BB(2)(b). The NY SHIELD Act does not mandate specific security measures, but businesses that comply with the law's listed safeguards "are deemed to be in compliance."
166 See footnotes for references to specific states.
167 MA: 201 CMR 17.03(1). NY: NY Gen. Bus. Law 899-bb(2)(a)-(c).
168 MA: 201 CMR 17.03(2)(b). NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(2), (B)(1), (C)(4).
169 NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3), (B)(1)-(2), (C)(1).
170 CA: Cal. Civ. Code. 1798.81.5(b). FL: Fla. Stat. 501.171(2). MA: 201 CMR 17.03(1). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3). TX: Tex. Bus. & Com. Code 521.052(a)-(b).
171 CA: Cal. Civ. Code. 1798.81.5(b). MA: 201 CMR 17.04. NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(C)(3).
172 CA: Cal. Civ. Code. 1798.81.5(c). FL: Fla. Stat. 501.171(2). MA: 201 CMR 17.03(2)(f). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(5).

TE

4. Testing and Evaluation

- Regularly test and monitor the effectiveness of cybersecurity controls and procedures.[173]

WP

5. Workforce and Personnel

- Designate employees to manage the security program.[174]
- Train and manage employees on security program practices and procedures.[175]

IR

6. Incident Response

- Detect and respond to cyberattacks, intrusions, or system failures.[176]
- Report large breaches of personal information.[177]

Penalties for noncompliance

- State Attorneys General may impose civil penalties and injunctions. Some states have varying caps on civil penalties.[178]
- Some states, such as CA, allow private lawsuits.[179] Other states, such as NY and FL, do not permit private lawsuits under these laws.[180]

Further reading

- National Conference of State Legislatures resource page on state data security[181]
- Rapid7 Advisory and Incident Response Services[182]

8. Sarbanes-Oxley (SOX)

The Securities and Securities Exchange Acts, together with the Sarbanes-Oxley Act (SOX), require public companies to disclose material risks and incidents to the Securities and Exchange Commission (SEC).[183] While those laws do not directly reference cybersecurity, SEC issued multiple statements clarifying their views that the laws include material cybersecurity risks and cybersecurity incidents in disclosure obligations.[184]

Who is affected

Publicly traded companies under SEC jurisdiction are affected.

173 CA: Cal. Civ. Code. 1798.185(a)(15)(A). MA: 201 CMR 17.03(2)(h0-(i). NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3), (B)(4).
174 MA: 201 CMR 17.03(2)(a). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(1).
175 MA: 201 CMR 17.03(2)(b)-(e). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(4).
176 MA: 201 CMR 17.03(2)(b)(3), (2)(j). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(B)(3), (C)(2).
177 All US states. https://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx
178 See, for example, Tex. Bus. & Com. Code 521.151(a)-(b). Civil penalties range from $2,000-$50,000 per record.
179 Cal. Civ. Code 1798.84, 1798.150.
180 N.Y. Gen. Bus. Law Sec. 899-bb(2)(e). Fla. Stat. 501.171(10).
181 https://www.ncsl.org/research/telecommunications-and-information-technology/data-security-laws.aspx#DataSecLaws
182 https://www.rapid7.com/solutions/consulting-services/
183 17 CFR 229, 210, 249.310, 249.308a. 15 USC 78m, 78q. Sarbanes-Oxley Act, Section 404. Materiality of cybersecurity risks and incidents depends on likelihood, potential harm, impact on company operations, and possibility of investigations, regulatory action, and litigation. See Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 10-11, https://www.sec.gov/rules/interp/2018/33-10459.pdf
184 SEC CF Disclosure Guidance, Topic No. 2, Cybersecurity, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm See also Commission Statement and Guidance on Public Company Cybersecurity Disclosures, https://www.sec.gov/rules/interp/2018/33-10459.pdf

Summary of cybersecurity practices for SOX and SEC disclosures

In addition to disclosing material cybersecurity risks and incidents to the SEC and investors, SOX requires that publicly traded companies ensure their internal business processes are securely managed. SEC guidance also "encourage[s] companies to adopt comprehensive policies related to cybersecurity and to assess their compliance regularly."[185]

RA

1. Risk Assessment

- Assess and disclose material cybersecurity risks to the company, including acquisitions.[186] Some companies use governance frameworks such as COBIT, COSO, or SOC2 for this purpose.[187]

SS

2. Security Safeguards

- Ensure systems that enable financial reporting and disclosure are safeguarded with internal controls.[188]

TE

3. Testing and Evaluation

- Management must evaluate effectiveness of disclosure controls and procedures.[189] This is typically done through an independent third party auditor.
- Provide updates to material cybersecurity risks and incidents in periodic reports (i.e., annual 10-K, quarterly 10-Q), and current reports (8-K, 6-K).[190]
- Reassess the effectiveness of security controls after cyber incidents.[191]

WP

4. Workforce and Personnel

- Disclose the Board of Directors' involvement in overseeing management of material cybersecurity risks.[192]

IR

5. Incident Response

- Maintain effective controls and procedures that enable timely disclosures of material cybersecurity events and breaches.[193]

Penalties for noncompliance

Civil penalties can range to several millions of dollars, and can also include cease-and-desist orders or trading suspensions. Criminal penalties may apply for willfully certifying incorrect reports.[194]

Further reading

- SEC Guidance on Public Company Cybersecurity Disclosures[195]
- Rapid7 SOX Compliance Solutions[196]

185 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 18, https://www.sec.gov/rules/interp/2018/33-10459.pdf
186 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pgs. 8-16, https://www.sec.gov/rules/interp/2018/33-10459.pdf
187 AICPA, https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/aicpasoc2report.html See also ISACA, https://www.isaca.org/resources/cobit
188 17 CFR 240.13a-15, 240.15d-15. See also Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 19, https://www.sec.gov/rules/interp/2018/33-10459.pdf
189 17 CFR 240.13a-15, 240.15d-15. See also Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pgs. 14, 19, https://www.sec.gov/rules/interp/2018/33-10459.pdf
190 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg.s 8-10, https://www.sec.gov/rules/interp/2018/33-10459.pdf
191 CF Disclosure Guidance, Topic No. 2, Cybersecurity, https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm
192 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pgs. 17-18, https://www.sec.gov/rules/interp/2018/33-10459.pdf
193 Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 6-7, https://www.sec.gov/rules/interp/2018/33-10459.pdf
194 15 USC 78u, 78u-3, 18 USC 1350. See Public Company Disclosure and Controls, https://www.sec.gov/spotlight/cybersecurity-enforcement-actions See, for example, Altaba, Formerly Known as Yahoo!, Charged With Failing to Disclose Massive Cybersecurity Breach; Agrees To Pay $35 Million https://www.sec.gov/news/press-release/2018-71
195 https://www.sec.gov/rules/interp/2018/33-10459.pdf
196 https://www.rapid7.com/solutions/compliance/sox/

C. International Requirements

9. General Data Protection Regulation (GDPR)

The European Union's GDPR requires the protection of personal data of EU citizens. This includes technical and organizational measures to ensure security is appropriate to the risks.[197] GDPR defines personal data broadly to be any information relating to a person who can be directly or indirectly identified.[198]

Who is affected

All organizations, regardless of size or geographical location, that collect or process personal data of EU citizens and residents. Non-EU organizations are subject to GDPR if they offer goods or services to people in the EU or monitor the behavior of people in the EU (i.e., through web cookies or collecting IP addresses).[199]

Summary of GDPR cybersecurity practices

SP

1. Security Program

- Controllers and processors of personal information must implement technical and organizational measures to ensure security "appropriate to the risk."[200]

RA

2. Risk Assessment

- Take risks of processing into account to assess appropriate security.[201]
- Conduct data protection impact assessments when processing will create data protection risks, including assessment of security measures and processes to ensure data protection.[202]

SS

3. Security Safeguards

- Ensure ongoing confidentiality, integrity, availability, and resilience of processing systems and services.[203]
- Implement measures to protect personal data, such as encryption, as appropriate to the risks.[204]
- Incorporate data protection by design, including default security features.[205]
- Oversee and pass on data protection obligations to service providers.[206]

TE

4. Testing and Evaluation

- Establish a process to regularly test, assess, and evaluate the effectiveness of technical and organizational security measures.[207]

197 GDPR Art. 32, Recital 83.
198 GDPR Art. 5.
199 GDPR Art. 3.
200 GDPR Art. 32.1. In considering the "appropriate" level of security, controllers and processors must take into account the state of the art, the costs of implementation, and the nature and scope of processing, as well as the risk and severity of impact to the privacy rights of data subjects.
201 GDPR Art. 32.2.
202 GDPR Art. 35.7(d).
203 GDPR Art. 32.1(b).
204 GDPR Art. 32.1(a).
205 GDPR Art. 25, Recital 78.
206 GDPR Art. 32.4.
207 GDPR Art. 32.1(d).

WP

5. Workforce and Personnel

- Appoint a qualified data protection officer to be involved in all issues related to the protection of personal data.[208]

IR

6. Incident Response

- Maintain ability to restore availability and access to personal data in the event of an incident.[209]
- Investigate, document, take remedial action, and provide notification for breaches.[210]

Penalties for noncompliance

Each EU state supervisory authority has a range of powers, including orders to comply, limits or bans on data processing, suspending data flows to other countries or organizations, revoking certifications, further investigations, and civil penalties.[211] For example, British Airways was fined £20 million (reduced from £183 million) in 2020 because of a breach of customer information, which the Information Commissioner's Office said was due to inadequate security measures.[212]

- For less severe infringements: a maximum fine of up to €10 million, or 2% of the firm's global annual revenue, whichever is higher.
- For more severe infringements: a maximum fine of up to €20 million, or 4% of the firm's global annual revenue, whichever amount is higher.[213]

Further reading

- EU resource page on data protection rules[214]
- Rapid7 GDPR compliance solutions[215]

208 GDPR Art. 37-39.
209 GDPR Art. 32.1(c).
210 GDPR Art. 33-34, Recitals 85-88.
211 GDPR Art. 58.
212 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers
213 GDPR Art. 83.
214 https://ec.europa.eu/info/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules/eu-data-protection-rules_en
215 https://www.rapid7.com/solutions/compliance/gdpr/

10. EU Network and Information Systems (NIS) Directive

The EU's 2016 NIS Directive requires all EU Member States (as well as the United Kingdom) to establish security safeguard and incident reporting requirements on a variety of digital and critical infrastructure-like services across the EU.[216] Numerous EU Member States and the UK have issued local regulations implementing the Directive for essential services and digital service providers.[217] The EU Commission also issued a 2018 implementing regulation on security safeguards expected for digital service providers.[218]

For purposes of this white paper, we are focusing on the current, EU-wide NIS Directive. However, even if a safeguard is not specifically included in the Directive, it may still appear in implementing regulations from EU Member States or the UK. It is also worth noting that in 2020 the EU Commission proposed a significant expansion of the NIS Directive, called NIS 2, which is presently under negotiation among EU lawmakers.[219]

Who is affected

The NIS Regulations apply to essential services and digital services operating in the Member State and UK territories that meet thresholds for size and criticality.[220] The EU Directive specified that these services include healthcare, banking, financial market infrastructure, water supply, transport, energy providers, digital infrastructure, and digital services (online marketplaces, cloud services, online search services).[221] EU Member States designate specific organizations as being regulated based on how strategically important the entities are to the State (i.e., market size, national security, economic impact, etc.)[222]

Summary of NIS Directive cybersecurity requirements

The NIS Directive requires EU Member States to establish security and reporting requirements for essential services and digital service providers.[223] While the specific security requirements of each Member State may vary, the requirements must follow the broad outlines in the EU Commission's NIS Directive and implementing regulation. Because the EU Commission issued an implementing regulation on digital service providers, there is greater detail regarding security expectations for those providers than for essential services.[224]

SP

1. Security Program

- Essential and digital services must take appropriate technical and organizational safeguards to manage risks to the security of networks and information systems.[225]
- Essential and digital services must take appropriate measures to prevent and minimize the impact of security incidents.[226]

RA

2. Risk Assessment

- Measures taken for the security of networks and information systems must be appropriate to the risks and reflect the state of the art.[227]

216 EU Directive 2016/1148, Art. 1.2., 14, 16. The UK was an EU Member State when the Directive was enacted.
217 See https://ec.europa.eu/digital-single-market/en/state-play-transposition-nis-directive See also, Bird & Bird Developments on NIS Directive in EU Member States (2020), https://www.twobirds.com/~/media/pdfs/developments-on-nis-directive-in-eu-member-states.pdf
218 EU Commission Implementing Regulation 2018/151. Note: EU Directives tell a Member State the broad outcome, but leaves details open to the State to "transpose" into national laws. EU Regulations issue more detailed requirements that bind Member States.
219 The proposed NIS 2 Directive would, among other things, establish more stringent security requirements to more organizations. For an analysis of the draft NIS 2 in comparison to NIS 1, see https://www.rapid7.com/blog/post/2021/04/20/overview-of-the-eus-draft-nis-2-directive/
220 EU Directive 2016/1148, Art. 6.
221 EU Directive 2016/11486, Annex II-III.
222 U Directive 2016/1148, Art. 6.
223 EU Directive 2016/1148, Art. 1.2., 14, 16.
224 EU Commission Implementing Regulation 2018/151.
225 EU Directive 2016/1148, Art. 14.1, 16.1.
226 EU Directive 2016/1148, Art. 14.2, 16.2.
227 EU Directive 2016/1148, Art. 14.1, 16.1.

SS

3. Security Safeguards

- Digital services must implement processes to identify vulnerabilities in information systems.[228]
- Digital services' measures for security of systems and facilities must include asset management, secure system lifecycle management, data protection (encryption where applicable), security business continuity planning, and access controls.[229]

TE

4. Testing and Evaluation

- Digital services' security measures must account for monitoring, auditing, and testing, including vulnerabilities in networks and information systems.[230]

IR

5. Incident Response

- Essential services must take appropriate measures to prevent and minimize the impact of incidents affecting the security of networks and information systems.[231]
- Digital services must implement incident handling measures, including processes to detect anomalies.[232]
- Essential and digital services must notify authorities of security incidents that have a significant impact on services.[233]

Enforcement and penalties

Under the NIS Directive, EU Member State authorities have the power to assess compliance and compel evidence from regulated entities.[234] Member State authorities can issue binding instructions to remedy deficiencies in regulated entities' security programs.[235]

The specific powers and penalties are left up to the EU Member States. For example, the UK (a Member State at the time) announced fines of up to £17 million or 4% of a company's global revenues, depending on the severity.[236]

Further reading

- EU Commission "NIS Toolkit"[237]
- ENISA Guidelines on assessing Digital Service Provider security and Operator of Essential Services compliance with the NIS Directive security requirements[238]
- UK National Cyber Security Centre Cyber Assessment Framework[239]
- ENISA "NIS Investments" report on cybersecurity investment and NIS implementation[240]
- Rapid7, Overview of the EU's draft NIS 2 Directive and Comparison with NIS 1[241]

228 EU Implementing Regulation 2018/151 Art. 2.2(b).
229 EU Directive 2016/1148, Art. 16.1(a). EU Implementing Regulation 2018/151 Art. 2.1. See also ENISA compliance guidelines, pg. 15-22.
230 EU Directive 2016/1148, Art. 16.1(d). EU Implementing Regulation 2018/151 Art. 2.4.
231 EU Directive 2016/1148, Art. 14.2.
232 EU Directive 2016/1148, Art. 16.1(b)-(c). EU Implementing Regulation 2018/151 Art. 2.2.
233 EU Directive 2016/1148, Art. 14.3-14.4, 16.3-16.4. EU Implementing Regulation 2018/151 Art. 3-4.
234 EU Directive 2016/1148, Art. 15, Art. 17. Member State authorities may supervise essential services at any time, and supervise digital services when they are aware of evidence of noncompliance.
235 EU Directive 2016/1148, Art. 15.3, Art. 17.2(b).
236 https://www.gov.uk/government/news/new-fines-for-essential-service-operators-with-poor-cyber-security
237 http://data.consilium.europa.eu/doc/document/ST-12205-2017-ADD-1/en/pdf
238 https://www.enisa.europa.eu/publications/guidelines-on-assessing-dsp-security-and-oes-compliance-with-the-nisd-security-requirements
239 https://www.ncsc.gov.uk/collection/caf
240 https://www.enisa.europa.eu/publications/nis-investments/
241 https://www.rapid7.com/globalassets/_pdfs/policy/rapid7-nis-summary-analysis-2021.pdf

III. Mapping Rapid7 solutions to security practices in regulations

The previous sections categorize security regulatory requirements into six cybersecurity practices. This section provides a description of Rapid7 products and services that can help customers fulfill the cybersecurity practices.

The products and services are grouped into two categories: 1) the key, go-to products and services to help fulfill each practice, and 2) other products and services that can also help fulfill each practice.

This product and service mapping is intended to provide a general guide to help match current and prospective customers with the Rapid7 products and services they need to help achieve their compliance goals.

SP

1. Security Program

Maintain a comprehensive security program. This may include written administrative, technical, and physical safeguards and procedures to protect the confidentiality, integrity, and availability of sensitive information and systems.

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)(1)(i), 316(b)(1)-(2).
GLBA	16 CFR 314.3 (FTC). Security Guidelines II.A-B (FFIEC). 17 CFR 248.30(a) (SEC). 17 CFR 160.30 (CFTC).
NYDFS	23 NYCRR 500.02(a), 500.03.
PCI DSS	PCI DSS, 12.1, 12.1.1, 12.3.
COPPA	16 CFR 312.3(e), 312.8.
NERC CIP	CIP-003-8 R1-R2.
	GENERALLY APPLICABLE
States	MA: 201 CMR 17.03(1). NY: NY Gen. Bus. Law 899-bb(2)(a)-(c).
	INTERNATIONAL
GDPR	GDPR Art. 32.1.
NIS	EU Directive 2016/1148, Art. 14.1-2, 16.1-2.

Key Rapid7 solutions to help meet this practice:

Rapid7 offers services designed to help develop, assess, and strengthen organizational security programs.

- Rapid7 service: ***Cybersecurity Maturity Assessment*** - Measures the effectiveness of your cybersecurity program by evaluating the implemented controls and giving recommendations to improve control maturity. Control sets and frameworks we specialize in currently include PCI DSS, HIPAA, NYDFS, NIST Cybersecurity Framework, NIST 800-53, NIST 800-171, CIS Controls, and more.[242]

- Rapid7 service: ***Cybersecurity Policy Development*** - Develops the governing documentation that allows the organization to know what is expected of them and their role in managing cybersecurity.[243]

How other Rapid7 solutions can help meet this practice:

Each of Rapid7's other solutions help support the implementation of a comprehensive cybersecurity program.

- Rapid7 product: ***InsightVM*** - Enable scanning and management of vulnerabilities and configurations, including risk classification and impact analysis. Automate inventory of systems, services, and installed applications.[244]

- Rapid7 service: ***Managed VM*** - Our experts partner with your team to offer strategic guidance and operational support to help you advance your VM program maturity. Tailored recommendations provide the business context needed to effectively drive remediation and risk mitigation efforts across your environment, and help you improve your overall security posture.[245]

- Rapid7 product: ***InsightIDR*** - Detect and respond to attacks and incidents quickly. Centralize and analyze your data across systems, automatically apply user and attacker behavior analytics, and integrate insights from our threat intel network.[246]

- Rapid7 service: ***Managed Detection & Response*** - Our security operations team provides around-the-clock threat monitoring in your environment to detect, investigate, and respond to incidents and threats.[247]

- Rapid7 product: ***InsightAppSec*** - Measure and manage application security risk with dynamic application security testing for web, mobile, and cloud applications for vulnerabilities. Create actionable compliance and remediation reports.[248]

- Rapid7 service: ***Managed AppSec*** - Our appsec experts partner with your team to provide strategic guidance and operational support to help you build and mature your appsec program. Identify application security vulnerabilities and manage risk with the business context and validation you need to effectively prioritize and accelerate your remediation efforts and reduce your application security risk.[249]

- Rapid7 product: ***InsightCloudSec*** - Get complete visibility into your cloud's network configuration to ensure you can manage the design, changes, and compliance in your environment. Protect cloud and container environments from threats, misconfigurations, policy violations, and IAM challenges. Plus, get integrations for real-time remediation for continuous security and compliance.[250]

- Rapid7 service: ***Penetration Testing*** - Test your defenses against simulated attacks to strengthen gaps and ensure readiness.[251]

242 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-assessment/
243 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-policy-development/
244 https://www.rapid7.com/products/insightvm/
245 https://www.rapid7.com/services/managed-services/vulnerability-management/
246 https://www.rapid7.com/products/insightidr/
247 https://www.rapid7.com/services/managed-services/managed-detection-and-response-services/
248 https://www.rapid7.com/products/insightappsec/
249 https://www.rapid7.com/services/managed-services/managed-appsec/
250 https://www.rapid7.com/products/insightcloudsec/
251 https://www.rapid7.com/services/security-consulting/penetration-testing-services/

RA

2. Risk Assessment

Assess internal and external cybersecurity risks and threats to the confidentiality, integrity, and availability of sensitive information and systems. This may include:

- *Periodically documenting changing risks and threats.*
- *Identifying gaps in security program maturity.*
- *Inventory and classification of assets.*

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)(1)(ii)(A), 306(b)(2).
GLBA	16 CFR 314.4(b) (FTC). Security Guidelines III.B (FFIEC). 17 CFR 248.30(a)(2) (SEC). CFTC Staff Advisory No. 14-21, Best Practice 2.
NYDFS	23 NYCRR 500.09, 500.03(c).
PCI DSS	PCI DSS, 12.2.
NERC CIP	CIP-002-5.1a R1-R2.
	GENERALLY APPLICABLE
States	MA: 201 CMR 17.03(2)(b). NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(2)-(3), (B)(1)-(2), (C)(1), (C)(4).
SOX	Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pgs. 8-16.
	INTERNATIONAL
GDPR	GDPR Art. 32.2, 35.7(d).
NIS	EU Directive 2016/1148, Art. 14.1, 16.1.

Key Rapid7 solutions to help meet this practice:

Rapid7 offers solutions aimed at helping organizations identify, assess, and document cybersecurity risks.

- Rapid7 service: ***Cybersecurity Maturity Assessment*** - Evaluate the effectiveness of your cybersecurity controls, plus get a risk-based security roadmap as well as detailed recommendations.
- Rapid7 service: ***Security Risk Assessment*** - This service performs a qualitative risk assessment using a common baseline of security controls and evaluates to business impact. It also provides a repeatable process for organizations to follow when completed.[252]
- Rapid7 solutions: ***InsightVM and Managed VM*** - Get top-down visibility of risk to cyber assets (such as servers, endpoints, networking devices, and more) and business operations; this enables teams to prioritize assets and quickly focus on the items that pose the greatest risk. Identify where vulnerabilities and insecure configurations exist in their technology environment, which is the foundational basis for understanding and treating risk.

252 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-development/

How other Rapid7 solutions can help meet this practice:

Several Rapid7 solutions work together to provide visibility into organizational risks, identify vulnerabilities and threats, and inventory assets.

- Rapid7 service: ***Penetration Testing Services*** - This service simulates real-world attacks on your networks, applications, devices, and/or people to demonstrate how risk is being managed in practice and how effective risk management is in preventing and detecting real world threats.
- Rapid7 solutions: ***InsightAppSec and Managed AppSec*** - Gain visibility into application level vulnerabilities and dynamically simulate attacks on web applications to identify security risk. It integrates with CI/CD pipeline tools to automate risk assessment of applications in pre-production environments.
- Rapid7 service: ***Breach Readiness Assessment*** - This service analyzes an organization's ability to monitor and respond to cybersecurity intrusions and breaches to understand capability and risk.[253]
- Rapid7 service: ***Vulnerability Management Maturity Assessment*** - Evaluate the vulnerability management program to identify, score, and recommend capability improvements to determine effectiveness and measure residual risk.[254]
- Rapid7 product: ***InsightCloudSec*** - Provide your cloud environment with automated discovery and inventory assessment across cloud service providers and containers. It also allows for the alignment of governance, policy, and practices to be monitored and managed in cloud environments to understand a complete risk picture.

SS

3. Security Safeguards

Implement safeguards to control the risks identified in the risk assessment. This may include:

- *Protecting sensitive information at rest and in transit.*
- *Network, software, and application security.*
- *User access controls and monitoring.*
- *Requiring third party vendors and service providers to maintain safeguards.*

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)-(b), 314(a).
GLBA	16 CFR 314.4(c) (FTC). Security Guidelines III.C.1 (FFIEC). 17 CFR 248.30(a)(3) (SEC). CFTC Staff Advisory No. 14-21, Best Practice 3.
NYDFS	23 NYCRR 500.03, 500.11.
PCI DSS	PCI DSS, 1-12.
COPPA	16 CFR 312.8.
NERC CIP	CIP-004-6 R4-R5. CIP-005-6 R1-R2. CIP-007-6 R1-R3, R5. CIP 010-3 R1-R3.3. CIP-011-2 R1.2. CIP-013-1 R1-R2.
	GENERALLY APPLICABLE
States	CA: Cal. Civ. Code. 1798.81.5(b)-(c). FL: Fla. Stat. 501.171(2). MA: 201 CMR 17.03(1)-(2)(f), 17.04. NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3), (A)(5). TX: Tex. Bus. & Com. Code 521.052(a)-(b).
SOX	17 CFR 240.13a-15, 240.15d-15.
	INTERNATIONAL
GDPR	GDPR Art. 32.1(a)-(b), 32.4, 25.
NIS	EU Directive 2016/1148, Art. 16.1(a). EU Implementing Regulation 2018/151 Art. 2.1, 2.2(b).

253 https://www.rapid7.com/services/security-consulting/incident-response-services/
254 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-development/

Key Rapid7 solutions to help meet this practice:

Rapid7's solutions deploy a full complement of safeguards to secure systems and information in cloud and non-cloud environments, as well as to assess third party service provider security and compliance.

- Rapid7 solutions: ***InsightVM and Managed VM*** - Perform comprehensive scanning to identify vulnerabilities. Detect misconfigurations, as well as identify missing patches and malicious software. Support the entire vulnerability management lifecycle, including collection of asset information, prioritization of vulnerabilities according to real-world risk, and remediation workflows to help reduce overall organizational risk.

- Rapid7 solutions: ***InsightIDR and Managed Detection & Response*** - Monitor for threats and leverage contextual, environment-specific analysis and behavioral analytics. Automatically correlate activity on your network to the users and entities behind them, making it easy to spot risky behavior, as well as detect lateral movement and the use of stolen credentials.

- Rapid7 product: ***InsightCloudSec*** - Continuously scan and monitor cloud resources throughout your cloud environment to ensure services are encrypting both data at rest and in transit. Help govern Identity and Access Management (IAM) and adopt a unified zero trust security model across your cloud and container environments.

- Rapid7 product: ***InsightAppSec and Managed AppSec*** - Identify and report on application and API security risks for prioritization and remediation/mitigation. This solution integrates into DevOps workflows to prevent new risk from entering production environments.

- Rapid7 product: ***tCell*** - This Next Gen Cloud WAF and runtime application self-protection solution monitors and protects web applications, APIs, and microservices against OWASP Top 10 and Zero-Day Attacks. Assess your application attack surface from APIs to 3rd-party packages, monitor & block suspicious actors, immediately identify and remediate breaches, and integrate application security into your DevOps toolchain and SOC.

- Rapid7 service: ***Security Program Development, Vendor Management Program Development*** - This service provides security due diligence in vendor selection, as well as monitoring of third party service providers. Establish best practices and vendor contract language with security requirements to ensure compliance with technology and services agreements. This is a critical security safeguard to manage supply chain risks.[255]

How other Rapid7 solutions can help meet this practice:

Other Rapid7 solutions enhance the impact of security safeguards.

- Rapid7 service: ***Penetration Testing Services*** - Simulate real-world attacks on service provider networks, applications, devices, and/or people to demonstrate the security level and measure performance against contractual terms.

255 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-development/

TE

4. Testing and Evaluation

Assess the effectiveness of policies, procedures, and safeguards to control risks. This may include:

- *Regular testing of information security controls through, for example, penetration tests and independent audits.*
- *Adjusting security safeguards based on testing results and changes to business operations.*

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)(1)(ii)(D), 308(a)(8).
GLBA	16 CFR 314.4(c), (e) (FTC). Security Guidelines III.C.3 (FFIEC). CFTC Staff Advisory No. 14-21, Best Practices 5-6.
NYDFS	23 NYCRR 500.05(a)-(b).
PCI DSS	PCI DSS, 11, 11.2-3.
NERC CIP	CIP-004-6 R4.3. CIP-008-6 R2-3.1. CIP-009-6 R2-3.1. CIP-010-3 R3.1-3.2.
	GENERALLY APPLICABLE
States	CA: Cal. Civ. Code. 1798.185(a)(15)(A). MA: 201 CMR 17.03(2)(h0-(i). NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3), (B)(4).
SOX	17 CFR 240.13a-15, 240.15d-15. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 19. CF Disclosure Guidance, Topic No. 2, Cybersecurity.
	INTERNATIONAL
GDPR	GDPR Art. 32.1(d).
NIS	EU Directive 2016/1148, Art. 16.1(d). EU Implementing Regulation 2018/151 Art. 2.4.

Key Rapid7 solutions to help meet this practice:

Rapid7's services enable organizations to test the effectiveness of their security programs and safeguards.

- Rapid7 service: ***Penetration Testing Services*** - Simulate real-world attacks on your networks, applications, devices, and/or people to demonstrate the security level of your key systems and infrastructure and show you what it will take to strengthen them.
- Rapid7 service: ***Cybersecurity Maturity Assessment*** - Measure the effectiveness of your cybersecurity program by evaluating the implemented controls, and get recommendations to improve control maturity.
- Rapid7 service: ***Vulnerability Management Maturity Assessment*** - Measure the effectiveness of your vulnerability management program by evaluating the implemented processes, workflows and controls, and get recommendations to improve vulnerability identification through to remediation.
- Rapid7 solution: ***InsightVM and Managed VM*** - Scan your environment for vulnerabilities, identify unaddressed flaws, and prioritize remediation according to assessed risk level. Compare the results of vulnerability scans over time.
- Rapid7 solution: ***InsightAppSec and Managed AppSec*** - Scan your modern web applications for vulnerabilities as well as manage risk across your application portfolio and at various stages of the software development lifecycle. Simulate real world web application attacks to understand if safeguards are working as intended.

WP

5. Workforce and Personnel

Establish security roles and responsibilities for personnel. This may include:

- *Designating personnel to manage the security program.*
- *Employee training.*
- *Management approval and regular oversight of the information security program.*

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)(1)(ii)(D), 308(a)(8).
GLBA	16 CFR 314.4(c), (e) (FTC). Security Guidelines III.C.3 (FFIEC). CFTC Staff Advisory No. 14-21, Best Practices 5-6.
NYDFS	23 NYCRR 500.05(a)-(b).
PCI DSS	PCI DSS, 11, 11.2-3.
NERC CIP	CIP-004-6 R4.3. CIP-008-6 R2-3.1. CIP-009-6 R2-3.1. CIP-010-3 R3.1-3.2.
	GENERALLY APPLICABLE
States	CA: Cal. Civ. Code. 1798.185(a)(15)(A). MA: 201 CMR 17.03(2)(h0-(i). NY Gen. Bus. Law 899-bb(2)(b)(ii)(A)(3), (B)(4).
SOX	17 CFR 240.13a-15, 240.15d-15. Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 19. CF Disclosure Guidance, Topic No. 2, Cybersecurity.
	INTERNATIONAL
GDPR	GDPR Art. 32.1(d).
NIS	EU Directive 2016/1148, Art. 16.1(d). EU Implementing Regulation 2018/151 Art. 2.4.

Key Rapid7 solutions to help meet this practice:

Rapid7 solutions help organizations create, enforce, and improve workforce security policies and training.

- Rapid7 service: ***Security Policy Development*** - Get help developing personnel policies and procedures that enable an organization's workforce to know what is expected of them and their roles in managing cybersecurity. This includes policies for security awareness training, telework and remote access, email security, account creation and password protection, and more.

- Rapid7 service: ***Product and Skills Training*** - Receive guided training and hands-on curricula to help your workforce maximize their skills in vulnerability management, detection and response, application security, and SOC Automation utilizing Rapid7 solutions.[256]

How other Rapid7 solutions can help meet this practice:

Rapid7 offers services to evaluate and improve how cybersecurity programs handle workforce policies.

- Rapid7 service: ***Cybersecurity Maturity Assessment*** - Measure the effectiveness of your cybersecurity program by evaluating the implemented controls, including workforce policies and roles, and get recommendations to strengthen the program.[257]

256 https://www.rapid7.com/services/training-certification/training/
257 https://www.rapid7.com/services/security-consulting/security-advisory-services/security-program-assessment/

IR

6. Incident Response

Detect, investigate, mitigate, and document cybersecurity incidents and events. This may include:

- *Monitoring systems to detect actual and attempted attacks or intrusions.*
- *Procedures to investigate incidents of unauthorized access to sensitive information or systems.*

	SECTOR-SPECIFIC
HIPAA	45 CFR 164.308(a)(6), 308(a)(7)(ii), 404(a)(2), 402(2), 408(c).
GLBA	16 CFR 314.4(b)(3) (FTC). 70 Fed. Reg. 15736, Supp. A to App. B to 12 CFR 30 (FFIEC). Regulation S-P (SEC), CFTC Staff Advisory No. 14-21, Best Practice 9.
NYDFS	23 NYCRR 500.16-17.
PCI DSS	PCI DSS, 12.10.
NERC CIP	CIP-007-6 R4. CIP-008-6 R1, R4. CIP-009-6 R1-R2.
	GENERALLY APPLICABLE
States	MA: 201 CMR 17.03(2)(b)(3), (2)(j). NY: NY Gen. Bus. Law 899-bb(2)(b)(ii)(B)(3), (C)(2).
SOX	Commission Statement and Guidance on Public Company Cybersecurity Disclosures, pg. 6-7.
	INTERNATIONAL
GDPR	GDPR Art. 32.1(c), 33-34.
NIS	EU Directive 2016/1148, Art. 14.2-14.4, 16.1(b); 16.3-16.4. EU Implementing Regulation 2018/151 Art. 2.2, 3-4.

Key Rapid7 solutions to help meet this practice:

Rapid7's solutions enable organizations to detect, respond, mitigate, and recover from cybersecurity attacks and incidents.

- Rapid7 product: ***InsightIDR*** - Detect incidents and attack activity, leverage behavior analytics, and get indicators of compromise so alerts are issued early in the attack. Accelerate investigations and containment with timelines that centralize audit logs, endpoint telemetry, user activity, network events, and other data so you know what happened and when.[258]

- Rapid7 service: ***Managed Detection & Response*** - Get continuous detection and response for incidents occurring in your environment using InsightIDR. The service can manage organizational incident response functions as a whole or can augment existing in-house functions. Validated threats can be contained by the MDR SOC team. Full incident reports are sent to you alongside recommendations for any findings (e.g. containment, additional response, and remediation) and recommendations to improve cyber resilience (e.g. mitigation for future attacks) to strengthen your security posture. Rapid7 MDR also includes Remote Incident Response engagements if the SOC detects live, hands-on-keyboard attackers in your environment, delivered by the same personnel on the Breach Response team.[259]

- Rapid7 service: ***Incident Response Plan Development*** - This service develops an incident response plan that includes detection, monitoring, response, and recovery. This would include specific requirements for breach notification and reporting, where necessary.

- Rapid7 service: ***Breach Response and Retainer*** - In the event of a compromise, retainer customers alert the Rapid7 team, who will respond within one hour to plan an approach. Our experts launch incident response activities within 24 hours.[260]

258 https://www.rapid7.com/products/insightidr/
259 https://www.rapid7.com/services/security-consulting/incident-response-services/ir-program-development-services/
260 https://www.rapid7.com/services/security-consulting/incident-response-services/

- Rapid7 service: ***Compromise Assessment*** - This service assesses an organization's systems for leading indicators of compromise and provides visibility into abnormalities. Verify compromise and validate remediation efforts. This service can also be used during the merger and acquisition due diligence phase to assess a target asset.[261]

- Rapid7 service: ***Incident Response Readiness Assessment*** - Get a full evaluation of your threat detection and incident response capabilities compared with best practices, and identify steps to take your program to the next level.

- Rapid7 product: ***tCell*** - Leverage runtime application self-protection to monitor and protect web applications, APIs, and microservices against OWASP Top 10 and Zero-Day Attacks. Monitor and block suspicious actors, immediately identify and remediate breaches, and integrate application security into your DevOps toolchain and SOC.

How other Rapid7 solutions can help meet this practice:

Rapid7 offers additional solutions to boost readiness and prevent incidents from expanding.

- Rapid7 service: ***Table Top Exercise*** - Experience on-site threat simulation to evaluate your detection and response capabilities in a controlled environment. This is a critical step in understanding where gaps exist in the ability to respond to attacks.[262]

- Rapid7 product: ***InsightCloudSec*** - Leverage Cloud Service Provider (CSP) services (e.g., Amazon GuardDuty) for best-in-class intelligent threat detection that continuously monitors for malicious activity and unauthorized behavior. These CSP services use machine learning, anomaly detection, and integrated threat intelligence built by the CSPs themselves to identify and prioritize potential threats.

Table of cybersecurity practices and solutions

Green cells are key solutions for each practice.

	INSIGHTVM & MANAGED VM	INSIGHTIDR & MDR	INSIGHTAPPSEC, TCELL, & MANAGED APPSEC	INSIGHTCLOUDSEC	CONSULTING SERVICES
1) Security Program	✓	✓	✓	✓	✓
2) Risk Assessment	✓	–	✓	✓	✓
3) Security Safeguards	✓	✓	✓	✓	✓
4) Testing & Evaluation	✓	–	✓	–	✓
5) Workforce & Personnel	–	–	–	–	✓
6) Incident Response	–	✓	✓	✓	✓

261 https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-service-brief-compromise-assessment.pdf
262 https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7_threat_simulation_ttx_service_brief.pdf

IV. Operationalizing security practices

The previous sections categorize common regulatory requirements into six cybersecurity practices and describe how Rapid7's solutions can help meet and exceed those practices. This section provides a general description of how organizations operationalize the cybersecurity practices incorporated in regulations. Every organization is different and should operationalize security practices based on their individual risk profile, technology deployment, and structure. Many organizations choose to follow an established cybersecurity framework, such as the Center for Internet Security (CIS) Critical Security Controls, as a template for building their cybersecurity programs.[263]

The below is additional insight based on Rapid7's experiences of how we typically see organizations approach implementation. For each of the six broad cybersecurity practices identified in Section I above, we provide the following context:

A. Operational overview: How the cybersecurity practice generally operates within an organization's security program.

B. Organizational structure: Which teams or functions within an organization implement the cybersecurity practice.

C. Successful approaches: Approaches to successfully implementing the cybersecurity practice.

D. Common challenges: Common issues that hinder consistently successful implementation.

SP

1. Security Program

Maintain a comprehensive security program. This may include written administrative, technical, and physical safeguards and procedures to protect the confidentiality, integrity, and availability of sensitive information and systems.

A. Operational overview: A comprehensive cybersecurity program consists of a combination of people, process, and technology. The most important part of a cybersecurity program is governance, which is used to define the policies, standards, and guidelines. This allows the business, technology, and security teams to define tolerable risk and align on the methods to control and measure key performance and risk indicators. Most security governance approaches are based on a recognized cybersecurity framework that can easily be mapped to compliance responsibilities, such as CIS Controls or the NIST Cybersecurity Framework.[264] This methodology enables executive leadership and board alignment while effectively informing financial, operational, reputational, and compliance risk management functions.

B. Organizational structure: We see a range of organizational structures for where cybersecurity sits. Some organizations have incorporated cybersecurity as a driver for business risk management and will align cybersecurity as a peer to IT, or under a Chief Risk Officer, or under the General Counsel. Other organizations will create a Chief Information Security Officer role and align both physical and cybersecurity under a common organization given the shared mission space both functions have. Others still choose to initially implement cybersecurity programs as a function of IT, because that is a logical place for technology-focused work to live, although we do not recommend this. We strongly encourage organizations to drive cybersecurity out of a function that manages risk across the organization to ensure it intersects with every business function. Effective cybersecurity requires a combination of visibility of the organization, educating all users, implementing processes and policies, and deploying technologies. Sidelining security as a purely technical function will heavily limit its ability to protect and enable the organization, resulting in greater risk.

263 https://www.rapid7.com/solutions/compliance/critical-controls/
264 https://www.rapid7.com/solutions/compliance/critical-controls/

C. Successful approaches: The most mature and effective cybersecurity programs we have seen incorporate a best practices approach tightly aligned to business leadership, executive stakeholders, risk management, legal, and the board. This approach allows for the compliance responsibilities to be a byproduct of normal cybersecurity operations, and produces a consistent set of both key performance indicators and key risk indicators that inform business decisions. Once those factors are incorporated into the business process, legal liability is reduced and the business can choose where to incur technology risk and where not to.

D. Common challenges: When we have seen cybersecurity programs struggle, it is usually the result of a combination of factors. The most common factor is a lack of organizational understanding of the role cybersecurity plays as a business risk area, specifically when enterprise risk management does not include a cyber component in business risk categories. The second most common is when a cybersecurity organization is viewed and treated as an IT organization. While some of the cybersecurity activities are service-oriented like IT, security is not a function of IT and should be viewed as a peer/equivalent organization to a CIO. Lastly, a very common mistake is to view cybersecurity as simply a function of compliance. While regulations do drive some of the cybersecurity work and investment decisions, regulations often only apply to a subset of the company (for example, personal data) leaving a large gap and exposure for non-regulated business systems and processes.

2. Risk Assessment

Assess internal and external cybersecurity risks and threats to the confidentiality, integrity, and availability of sensitive information and systems. This may include:

- *Periodically documenting changing risks and threats.*
- *Identifying gaps in security program maturity.*
- *Inventory and classification of assets.*

A. Operational overview: Risk assessments (self and third party) are an important part of continuously measuring where cyber threats and vulnerabilities create the potential for operational disruption, reputational problems, liability, and/or negative impact on customers. Cybersecurity risk assessments identify where the organization is most likely to incur a security control failure, at what frequency, probability, and impact level. That analysis overlays onto business systems and their importance to the organization.

B. Organizational structure: Mature risk assessment functions are generally distributed but roll up to a central function often called Enterprise Risk Management (ERM). Members of the ERM team typically include executive leadership and meet frequently enough to discuss aspects of risk and how to prioritize funding. Cyber risks in the ERM scenario are cross-cutting and are informed by members of the cybersecurity team as well as key business stakeholders. Typically we will see the ERM function under the responsibilities of a Chief Risk Officer, Chief Operations Officer, or General Counsel and cyber risk assessments fall under a Chief Information Security Officer.

C. Successful approaches: Cybersecurity leaders have the most success communicating cyber risks when they are able to map risks to impacts affecting business processes and systems. This is generally not an easy task and can create friction with the security team if security professionals do not take the proper time and effort to build their understanding of the other team's goals and needs before taking a position on how to manage their risk. Cyber programs have significant effectiveness when they map potential losses to business functions or technology systems and their importance. For example, if a business system such as email becomes disrupted or compromised due to a vulnerability and results in business disruption, manual process costs and liability from loss of sensitive data can be calculated to inform cyber strategies, create risk visibility for the business, and validate cyber investment needs.

D. Common challenges: Many organizations struggle to make the connection between cybersecurity risks and the business risks managed by an enterprise risk management team. This typically occurs when there is a challenge translating technical content such as vulnerability and threat data into information that is meaningful to business leaders.

SS

3. Security Safeguards

Implement safeguards to control the risks identified in the risk assessment. This may include:

- *Protecting sensitive information at rest and in transit.*
- *Network, software, and application security.*
- *User access controls and monitoring.*
- *Requiring third party vendors and service providers to maintain safeguards.*

A. Operational overview: Security safeguards are largely consistent whether they are exclusively compliance-driven or used in the management of cyber risk. A cybersecurity maturity assessment will identify the current state of security controls, where gaps exist, where controls are ineffective, and will provide a set of recommendations for materially improving controls to achieve better compliance and cybersecurity.

B. Organizational structure: Security safeguards are typically implemented by a cybersecurity team. However, the support and buy-in for security safeguards has to be obtained by a combination of cybersecurity teams and the teams that will use and administer the systems. There are definitely core cybersecurity capabilities that broadly apply to the entire organization, but there may also be requirements for particular systems deployed by specific business units. In these cases, it is critical to ensure all relevant personnel are educated on risk, policy and process, and are working together.

C. Successful approaches: We see the most successful approaches to security safeguard implementation when organizations have tight integration between related business and cybersecurity units. Regulatory, legal, communication, marketing, human resources, and physical security are some common areas. Another area in which alignment has become very important is overseeing security of external entities with a trusted connection to the organization, such as the supply chain, IT integrators, and critical service providers; by minimizing disruptions with those entities, the organization further reduces its own risks.

D. Common challenges: Many organizations struggle to understand where best to apply technical and policy driven controls to effect cybersecurity best practices that enable compliance requirements. While some compliance requirements are very specific, they should always tie back to a broader security plan and strategy. When the intersection of cybersecurity and compliance is not well understood, it creates potential for a failure of both.

TE

4. Testing and Evaluation

Assess the effectiveness of policies, procedures, and safeguards to control risks. This may include:

- *Regular testing of information security controls, such as through penetration tests and independent audits.*
- *Adjusting security safeguards based on testing results and changes to business operations.*

A. Operational overview: These functions of a security program are completely operational and enable the business to be informed how effectively security, compliance, and audit requirements have been implemented. Ongoing assessment and benchmarking are a key way to maintain a culture of security within an organization. Cybersecurity monitoring and penetration testing are two of the best methods to evaluate the ongoing effectiveness of control implementation and management.

B. Organizational structure: These functions are almost always implemented and governed through IT and Security teams, with cross-functional coordination between the CISO and CIO. For organizations without a formal CISO role, the CIO typically assumes operational level responsibility with governance from the most senior security role available.

Many businesses decide to leverage both internal and external parties for penetration testing, although compliance requirements often require a third party to perform these tests. Additionally, independent entities are often brought in to assess an organization's adherence to security framework or compliance requirements.

C. Successful approaches: Successful teams are continuously reviewing operational control effectiveness to ensure risk is mitigated in a way that aligns with business goals and compliance requirements. IT teams report tactical metrics through their operational leaders, which help inform risk communication through more strategic team roles. Operational effectiveness is maintained through independent reviews of security controls and processes. Technical testing is also performed, normally through penetration testing and red team activities, to determine effectiveness of security controls and responses.

D. Common challenges: Common areas of struggle often begin with a misalignment between strategic and tactical goals, and are the result of inefficient or absent risk management processes. Operational level teams are often not provided with strategic level goals and thus deploy controls in a haphazard manner, often just leaning on best practice rather than on a coordinated set of goals for the organization. Security is implemented to the minimum levels of compliance requirements without the focus of larger business goals or initiatives.

WP

5. Workforce and Personnel

Establish security roles and responsibilities for personnel. This may include:

- *Designating personnel to manage the security program.*
- *Employee training.*
- *Management approval and regular oversight of the information security program.*

A. Operational overview: Developing a capable workforce to effectively manage the cybersecurity program for a business requires knowledgeable security personnel, a security-aware workforce, and alignment with executive leadership and/or the board of directors. Without knowledgeable security personnel, security safeguards and processes may be absent or ineffectively deployed. A broader workforce that lacks security awareness risks accidental security lapses and creates targets for attackers. Without alignment with leadership, the business will struggle to understand the operational and compliance cybersecurity risks because the security team will struggle to receive the buy-in and direction needed to accomplish both tactical and strategic initiatives.

B. Organizational structure: Most businesses will choose to hire a CISO or other senior security leader to run the security program and whose primary responsibility is to align business risk to IT risk. The CISO will ensure that IT is adhering to the designated compliance frameworks and standards, and will oversee the process of hiring capable individuals for security roles. While there is much debate over to whom a CISO should report, common organizational structures see security reporting to the CFO, COO, or General Counsel.

C. Successful approaches: A trained and capable cybersecurity workforce extends beyond the defined security organization. Cybersecurity is everyone's job within a company and the indicators of a robust and mature organization will have training that is tailored to job functions, such as an IT systems administrator or a software developer. However, that tailored training also extends to the executive team as well as each and every business function. When you have a training program in place that factors in an individual business unit and their role in cyber protections, the organization has a significantly reduced risk posture and less likelihood of breaches occurring. For organizations struggling to recruit or retain skilled workers, managed services can be a successful deployment strategy, especially in areas of detection and response.

D. Common challenges: Common areas of struggle include when security roles are solely embedded as part-time responsibilities in other IT roles, or if a role like CIO is responsible for both operational IT and security. While it is important to foster a culture of security throughout the organization, there should be an independent security entity that can communicate with the executive team and board of directors.

IR

6. Incident Response

Detect, investigate, mitigate, and document cybersecurity incidents and events. This may include:

- *Monitoring systems to detect actual and attempted attacks or intrusions.*
- *Procedures to investigate incidents of unauthorized access to sensitive information or systems.*

A. Operational overview: As a business, the ability to function through cybersecurity events that could disrupt operations is essential to business continuity. To maintain this capability, businesses need processes and plans for monitoring, responding to, and recovering from cyber risks and events. An Incident Response team working in conjunction with, or as part of, a Security Operations Center will be tasked with this function. In order to be successful, it will need organizational support, along with the investment to enable ongoing operations.

B. Organizational structure: Many businesses leverage services by third parties to provide either a portion of, or the entire capability, required for incident response processes to work effectively. Other businesses coordinate incident response activities through in-house security teams (under the CISO or appropriate security leader), with functional and operational incident response team (IRT) responsibilities defined in roles throughout the organization, for example in IT, legal, and communications. As incident response requires input from a multitude of roles, IRTs are usually made up of security, IT, and business participants. Alternative structures include having IRT activities delegated and coordinated through security operations centers roles.

C. Successful approaches: Incident response functions will be most effective if they are integrated into the business processes, such as through continuity planning, tabletop exercises, and investment in technology solutions. Successful incident response programs demonstrate characteristics that include strong governance in the form of policy and a robust incident response plan. This plan should include definitions of incident severity, as well as role and responsibility definitions for those individuals who will support incident handling processes.

Incident response exercises, usually in the form of tabletop exercises, are conducted to test communication channels, decision making, and technical capabilities. Mature IRTs will also conduct after-action reviews once an incident is resolved and closed to determine root causes and drive both strategic and tactical operational level changes. Mature IRTs will include leaders from Legal and Public Relations to manage crisis communications.

D. Common challenges: Common areas of struggle include the lack of clear and concise IRT roles, and lack of definition of what incident attributes define critical incidents. This leads to confusion and a delayed response when a critical incident occurs. Immature teams also do not practice incident response scenarios and often have to discover inefficiencies in response processes in real time. Similarly, IRTs often neglect to involve the business continuity processes, operating as though incident response is purely a security based function.

Cybersecurity and Compliance Maturity Tiers

LOW TIER	MID TIER	HIGH TIER
Activities • Compliance is the only driver for cybersecurity • No dedicated security staff • No security leader • Metrics based exclusively on compliance • No security KRIs or KPIs defined • Security spend tied to compliance activities • No organizational support • Cybersecurity thought of as a "checkbox" activity	**Activities** • Realization compliance alone will not stop adverse security outcomes • Partial to dedicated security staff • Security leader not higher than manager • Security part of IT org • Security KPIs defined as subset of IT • KRIs consist of technical outcomes • Budget tied to IT goals • Some cybersecurity activities viewed as checkbox • Compliance activities not integrated fully with security	**Activities** • Compliance is a byproduct of cybersecurity • Dedicated security staff and executive leadership • Security is a peer to IT • KRIs drive IT prioritization • KPIs reflect business needs • Budget tied to business risk management • Cybersecurity measured based on risk performance over time • Compliance has moved to an activity supported by the security program
Outcomes • Board/Exec team not receiving security reports • Audit scrutiny is policy based • IT infrastructure managed ad hoc • Basic cyber hygiene in place • Compliance managed by attestations	**Outcomes** • Board/Exec team not understanding metrics • Some operational security governance • Auditing shifts to evidence • IT following routine process • Security team working against friction • Compliance evidence collected ad hoc	**Outcomes** • Proactive Board/Exec team involvement • Strong program level security governance • Business integrated with cyber risk management • Audits focused on operational security risk • Compliance achieved via routine process

Rapid7 works with customers to navigate regulatory requirements, provides solutions to help achieve compliance, and partners with organizations to put security measures and processes into operation.

For more information about Rapid7's leading security products and services for compliance, please visit: https://www.rapid7.com/solutions/compliance/