REGULATORY/ COMPLIANCE RISK ASSESSMENT OVERVIEW FOR FAIR PRACTITIONERS

DISCLAIMER: This document is a compilation of requirements from various regulatory and compliance entities. It is intended to be used as an overview of risk assessment requirements, including commonalities amongst entities. It is a point-in-time document; therefore, users are responsible for keeping up with new and changing requirements.

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
PCI-DSS	Implement a risk-assessment process that: • Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.), • Identifies critical assets, threats, and vulnerabilities, and • Results in a formal, documented analysis of risk.	"at least annually and upon significant changes to the environment"	Discussed but no specific recommendation	Yes PCS DSS Risk Assessment Guidelines discuss "Risk Evaluation" as a way to "determine the significance of risks in order to prioritize mitigation efforts" and that using numerical values in the risk assessment can result in more objective results	Yes PCS DSS Risk Assessment Guidelines identifies a "need for the continuous monitoring of risks throughout the year"	Compliance activity details for numerous requirements are to be determined by the annual risk assessment.	FAIR, NIST SP 800-30, OCTAVE, ISO 27005
COBIT 2019	Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive	Not Specified	Yes	Yes	Yes	Define a balanced set of project proposals	CMMI Cyber Maturity Platform; COSO ERM;

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
	management. Source: COBIT 2019 Management Objective AP012 – Managed Risk.		Recommends articulating risk scenarios and providing decision makers with probabilities, ranges of loss, and confidence levels.	Estimate the frequency and magnitude of loss associated with risk scenarios while taking into account risk factors. Example metrics include "percent of critical business objectives and services covered by risk assessment", "business cost of incidents", "significant incidents not identified in risk assessments"	Based on all risk profile data, define a set of risk indicators that allow the quick identification and monitoring of current risk and risk trends.	designed to reduce risk and/or projects that enable strategic enterprise opportunities, considering costs, benefits, effect on current risk profile and regulations.	ISO/IEC 27005:2011; NIST CSF; NIST 800-53
SEC – Cybersecurity Disclosures	Organizations should consider the following in evaluating cybersecurity risk factor disclosure: • the occurrence of prior cybersecurity incidents, including their severity and frequency;	Risk factors are included in an annual report.	Yes References that "financial reporting and	Yes Frequency (probability) and magnitude of	Yes "Disclose specified information on a	Public disclosure/ reporting	Not specified

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
	• the probability of the occurrence and magnitude of cybersecurity incidents; the adequacy of preventative actions to reduce cybersecurity risks and the associated costs • the cost of the aspects of the company's business and operations that give rise to material cybersecurity risks; • the costs associated with maintaining cybersecurity protections, including insurance coverage; • the potential for reputational harm; • associated cost of existing or pending laws and regulations relating to cybersecurity • litigation, regulatory investigation, and remediation costs associated with cybersecurity incidents.		control systems would be designed to provide reasonable assurance that information about the range and magnitude of the financial impacts of a cybersecurity incident"	prior and future cybersecurity incidents. Adequacy of and associated costs with: Preventative actions taken to reduce cyber risks; Aspects of business that give rise to material cyber risks; Maintaining protections (e.g., insurance)	regular and ongoing basis." This includes timely and ongoing information regarding "material cybersecurity risks and incidents that trigger disclosure obligations"		
NIST CSF v1.1 **NIST CSF v1.1 (cont'd)**	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. The organization analyzes the operational environment in order to discern the likelihood of a cybersecurity event and the impact that the event could have on the organization. It is important that organizations identify emerging risks and use cyber threat information from internal and external sources to gain a better understanding of the likelihood and impact of cybersecurity events.	Not specified It supports "recurring" risk assessments and validation of business drivers to help organizations select target states for cybersecurity activities that reflect desired outcomes.	Not specified	Yes References that it is often more valuable to predict whether a cybersecurity risk may occur, and the impact it might have, using a leading measure.	Yes Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify	Develop an action plan to strengthen existing cybersecurity practices and reduce cybersecurity risk and reprioritize resources. (may reveal that an organization is overinvesting to achieve certain outcomes). Progression to higher framework	COBIT, CIS Controls, (ANSI/ISA)-62443-2-1 (99.02.01)-2009, ANSI/ISA-62443-3-3 (99.03.03)-2013, ISO/IEC 27001, NIST SP 800-53 Rev. 4 - NIST Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
					the effectiveness of protective measures.	implementation tiers is encouraged when a cost-benefit analysis indicates a feasible and cost-effective reduction of cybersecurity risk.	Information Systems and Organizations
ISO/IEC 27001 **ISO/IEC 27001 (cont'd)**	Section 6.1.2 of the Standard states the risk assessment process must: a. Establish and maintain certain information security risk criteria*; b. Ensure that repeated risk assessments "produce consistent, valid and comparable results"; c. "Identify risk associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system"; d. Identify the owners of those risks; and e. Analyze and evaluate information security risks according to certain criteria. *Criteria includes: • The organization's assets • The business, legal and contractual requirements relevant to the identified assets; • The value of the identified assets in terms of their confidentiality, integrity and availability	At least annually	Discussed but no specific recommendation. States that the importance is that organizations understand the scoring in business terms.	Yes At minimum, requires documentation of the measurement structure for all KPIs.	Yes Develop, implement and continuously improve a framework whose purpose is to integrate the process for managing risk into the organization's overall governance, strategy and planning, management, reporting processes,	Once the risk assessment has been conducted, the organization needs to decide how it will manage and mitigate those risks, based on allocated resources and budget.	Not specified; however, should take into account the requirements outlined in the first column.

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
	• The threats and vulnerabilities that affect the security of those assets; • The impact on the organization should the assets be compromised; and • The likelihood of them being compromised.				policies, values and culture.		
NYDFS	Each Covered Entity shall conduct a periodic Risk Assessment of the Covered Entity's Information Systems sufficient to inform the design of the cybersecurity program.	"as reasonably necessary to address changes to the Covered Entity's Information Systems, Nonpublic Information or business operations"	Not specified	Yes NYDFS 500.09 specifies that criteria be used for evaluations that includes "adequacy of existing controls in the context of the identified risk"	Yes CISO must report annually	"… requirements describing how identified risks will be mitigated or accepted based on the Risk Assessment and how the cybersecurity program will address the risks."	Not specified
GDPR	"The GDPR introduces a risk-based approach that involves assessing the risks presented by data processing activities and responding appropriately. This should take into account the nature, scope, context, purpose of the processing and the potential risks to the rights and freedoms of individuals. Assessments should include a systematic description of the processing operation, its purpose and assess the risks to the rights and freedoms of individuals. It should also include the measures that could be taken	Whenever processing is likely to result in a high risk to the rights and freedoms of individuals	Not specified	Yes To assess the level of risk, you must consider both the likelihood and the severity of any impact on individuals. High	Yes Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data	Conduct data protection impact assessments (DPIAs) to identify and reduce the data protection risk within projects and systems, and thereby reduce the likelihood of privacy	Article 29 Working Party Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is 'likely to result in a high risk' for the purposes of Regulation (EU)

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
	to mitigate these risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with the GDPR. The relevant obligations for 'high risk' processes are notifications of breaches, conducting a data protection impact assessment and prior consultations with Data Protection Authorities			risk could result from either a high probability of some harm, or a lower possibility of serious harm.	protection impact assessment at least when there is a change of the risk represented by processing operations.	harms to affected EU citizens.	2016/679, 4 April 2017 Articles 35 and 36 and Recitals (89) to (96) of the GDPR
GLBA	Identify vulnerabilities in electronic systems containing customer data, assess likelihood and impact of threats, and assess sufficiency of controls to mitigate those risks.	At least once a year, or more frequently in response to material changes in the environment.	Not specified	Not specified	Yes Recommended monitoring through optional what-if scenarios.	Output includes assigning a risk rating to each technology and mapping of controls to address each of the identified risks.	Not specified; however, should be logical, supportable, and appropriate for the institution.
Federal Information Processing Standards (FIPS) Publication 200	A risk-based process for selecting the security controls necessary to satisfy the minimum security requirements for information and information systems supporting the executive agencies of the federal government.	Not specified	Not specified	Not specified	Yes Leveraging established security baselines	Establish minimum levels of due diligence for information security and as an approach for selecting security controls for information systems that meet minimum security requirements.	Not specified

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
FFIEC	Management should identify, measure, mitigate, monitor, and report IT risks that threaten the safety and soundness of an institution. An effective ITRM process is regularly updated and aligns IT and business objectives. This process should have a higher level of formality in more complex institutions.	Not specified Exam frequency is as follows: -"A" ranking = 24 months -"B" ranking = 36 months -"C" ranking = 48 months	Yes Management should estimate the likelihood of occurrence and severity of the impact of the identified risk. When analyzing the potential impact, management should consider financial, reputation, etc.	Yes The specific metrics reported, and the frequency with which they are reported, depend on the institution's IT environment.	Yes Risk monitoring is ongoing and should include reviews of metrics (e.g., threat intelligence), performance benchmarks, SLAs, and compliance with internal policies.	Manage risk within limits. Improve controls.	Cybersecurity Assessment Tool (CAT)
HITRUST CSF	Perform an impact analysis on all systems with health information (criticality); (2) Categorize & valuate systems based on sensitivity & criticality; (3) Select an appropriate framework baseline set of controls; (4) Apply an overlay and/or tailor based on a targeted risk analysis; (5) Evaluate residual risk using control maturity & impact ratings; (6) Rank risks and determine risk treatments; (6) Make contextual adjustments to likelihood & impact, if needed, as part of the corrective action planning process.	Specified in Risk Assessment Criteria of the CSF	Not specified	Yes Specified in the "measured" evaluation criteria	Yes Specified in the "managed" evaluation criteria	Used as an approach to ensure that established controls are fully aligned with the risks to which an organization is exposed.	myCSF Risk Assessment

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
HIPAA Security & Privacy Rules	Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the organization [Security Rule] / covered entity or business associate [Privacy Rule].	HHS does not provide guidance on the frequency of reviews other than to suggest they may be conducted annually depending on an organization´s circumstances.	Not specified HHS acknowledges that there is no specific risk analysis methodology. This is due to Covered Entities and Business Associates varying significantly in size.	Not specified This is due to Covered Entities and Business Associates varying significantly in size.	No HHS does not provide guidance on the frequency of reviews other than to suggest they may be conducted annually depending on an organization´s circumstances.	The final stage of a HIPAA privacy risk assessment should be the development and implementation of a HIPAA privacy compliance program.	HIPAA Security Risk Assessment Tool NIST HIPAA Security Rule Toolkit
SSAE 18	Risk Assessment Procedures: The practitioner should obtain an understanding of the subject matter and other engagement circumstances sufficient to a. enable the practitioner to identify and assess the risks of material misstatement in the subject matter and b. provide a basis for designing and performing procedures to respond to the assessed risks and to obtain reasonable assurance to support the practitioner's opinion.	At least annually	Not specified	Yes AICPA states that the risk assessment, "may include estimating the significance of identified risks, assessing the likelihood of their occurrence, and deciding about	Yes If material changes are identified during the period between risk assessments, a revised assessment should be performed (ref: par. A31– A32)	Output is used to identify controls to test in the SOC report to mitigate the identified risks. The output of the risk assessment may also influence the nature, timing and extent of audit procedures.	Not specified

	Language for risk assessment requirements	Frequency of risk assessment	Recommends quantifying risk?	Recommends measuring risk / use of metrics?	Monitor changing risk levels over time?	Intended use of assessment	Framework(s) or tools cited by entity
				actions to address them."			
FHFA **FHFA (cont'd)**	The Information Security Management (ISM) program should include policies and processes that address: Information Security Risk Assessment – a process to identify threats, vulnerabilities, attacks, probabilities of occurrence, and outcomes. A security risk assessment gathers data regarding the information and technology assets of the organization, threats to those assets, vulnerabilities, existing security controls and processes, and the current security standards and requirements; analyzes the probability and effect associated with the known threats and vulnerabilities to institution assets; and prioritizes the risks present due to threats and vulnerabilities to determine the appropriate level of training, controls, and assurance necessary for effective mitigation.	An initial risk assessment may involve a significant one-time effort, but the risk assessment process should be an ongoing part of the ISM program.	Discussed but no specific recommendation	Yes Evaluate the standards used for measurement, the information measures and repeatability of measured processes, and appropriateness of the measurement scope. (Are the metrics accurate, timely, complete, relevant, and consistent?)	Yes Include an assessment of the adequacy of an institution's monitoring of risk and establishment of internal controls to mitigate risk. Identify areas requiring follow-up examination activities or monitoring.	The resulting information is used to develop strategies to mitigate those risks to the availability, integrity, confidentiality, and accountability of information and information systems.	Not specified

Sources

- **PCI-DSS**: https://www.pcisecuritystandards.org/documents/PCI_DSS_v2_Risk_Assmt_Guidelines.pdf
- **COBIT 2019:** http://www.isaca.org/COBIT/Pages/COBIT-2019-Framework-Governance-and-Management-Objectives.aspx
- **SEC – Cybersecurity Disclosures:** https://www.sec.gov/rules/interp/2018/33-10459.pdf
- **NIST CSF v1.1**: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- **ISO/IEC 27001**: https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en; https://www.itgovernance.co.uk/iso27001/iso27001-risk-assessment; https://www.isaca.de/sites/pf7360fd2c1.dev.team-wd.de/files/isaca_2017_implementation_guideline_isoiec27001_screen.pdf; www.iso27001security.com/ISO27k_Guideline_on_ISMS_audit_v1.docx
- **NYDFS:** https://www.dfs.ny.gov/legal/regulations/adoptions/dfsrf500txt.pdf
- **GDPR:** https://gdpr-info.eu/art-35-gdpr/; www.gdpr.associates/gdpr-requirements/
- **GLBA:** https://www.sans.org/reading-room/whitepapers/auditing/conducting-electronic-information-risk-assessment-gramm-leach-bliley-act-compliance-1053; https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-35a.pdf
- **FIPS 200**: https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf
- **FFIEC**: https://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management.aspx
- **HITRUST CSF:** https://hitrustalliance.net/; https://hitrustalliance.net/documents/mycsf/mycsf_information/MyCSFRiskAssessment.pdf
- **HIPAA Privacy Rule**: https://www.hipaajournal.com/hipaa-risk-assessment/
- **HIPAA Security Rule**: https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html?language=es#1951
- **SSAE 18**: https://www.aicpa.org/content/dam/aicpa/research/standards/auditattest/downloadabledocuments/ssae-no-18.pdf
- **FHFA**: https://www.fhfa.gov/SupervisionRegulation/Documents/Information_Technology_Risk_Management_Program_Module_Final_Version_1.1.pdf