Compliance checklist

To review compliance regulations and standards, read the controls, frameworks, and compliance documents.

- ☑ **The Federal Energy Regulatory Commission - North American Electric Reliability Corporation (FERC-NERC)**

  The FERC-NERC regulation applies to organizations that work with electricity or that are involved with the U.S. and North American power grid. Organizations have an obligation to prepare for, mitigate, and report any potential security incident that can negatively affect the power grid. Organizations are legally required to adhere to the Critical Infrastructure Protection Reliability Standards (CIP) defined by the FERC.

  Explanation:

The FERC-NERC (Federal Energy Regulatory Commission - North American Electric Reliability Corporation) regulation is a set of regulatory measures designed to ensure the reliability and security of the electricity infrastructure in the United States and parts of North America. These regulations primarily target organizations that are involved in the generation, transmission, and distribution of electric power, as well as those entities responsible for overseeing the overall functioning of the power grid.

The primary objective of the FERC-NERC regulation is to maintain the stability and integrity of the power grid, which is crucial for ensuring the availability of electricity to consumers and supporting essential services and industries. This becomes especially important given the interconnected and interdependent nature of the electricity grid.

Key points of the FERC-NERC regulation include:

Security Incident Preparedness and Mitigation: Organizations within the scope of these regulations are obligated to proactively prepare for potential security incidents that could impact the power grid. This involves implementing measures to prevent, detect, and respond to cybersecurity threats and other potential disruptions. By being proactive in their approach, these organizations can minimize the risks associated with security incidents and maintain grid stability.

Reporting of Security Incidents: If a security incident occurs that could potentially compromise the reliability of the power grid, organizations are required to promptly report

these incidents to appropriate authorities. This allows for a coordinated response to mitigate the impact of the incident and prevent further disruptions.

Critical Infrastructure Protection Reliability Standards (CIP): The FERC-NERC regulation mandates adherence to a set of standards known as the Critical Infrastructure Protection Reliability Standards (CIP). These standards define specific requirements and guidelines that organizations must follow to ensure the cybersecurity and overall reliability of their operations. These standards cover various aspects of cybersecurity, including access controls, monitoring, incident response, and more.

Enforcement and Compliance: FERC is the federal agency responsible for overseeing compliance with these regulations. It has the authority to enforce penalties and sanctions against organizations that fail to comply with the established standards. This enforcement mechanism encourages organizations to take their obligations seriously and prioritize the security of the power grid.

Overall, the FERC-NERC regulation is a crucial component of the broader effort to safeguard the reliability and security of the U.S. and North American power grid. By imposing specific requirements on organizations within the electricity sector, these regulations aim to prevent and mitigate potential threats, minimize disruptions, and ensure the continued availability of electricity for consumers and critical infrastructure.

☑ General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation:

The General Data Protection Regulation (GDPR) is a comprehensive data protection and privacy regulation enacted by the European Union (EU) to safeguard the rights and privacy of its citizens' personal data. This regulation applies to any organization that processes the personal data of EU citizens, regardless of whether the organization is located within or outside the EU territory. The GDPR came into effect on May 25, 2018, replacing the earlier Data Protection Directive.

Key features of the GDPR include:

Protection of Personal Data: The GDPR places a strong emphasis on the protection of personal data. It defines personal data broadly, encompassing any information that can directly or indirectly identify an individual, such as names, addresses, email addresses, identification numbers, and even online identifiers like IP addresses and cookies.

Data Subjects' Rights: The GDPR grants significant rights to individuals whose data is being processed. These rights include the right to access their own data, the right to rectify inaccurate data, the right to erasure (also known as the right to be forgotten), the right to restrict processing, the right to data portability, and the right to object to processing.
Lawful Basis for Processing: Organizations are required to have a lawful basis for processing personal data. These lawful bases include consent, contract performance, legal obligations, vital interests, public task, and legitimate interests. Organizations must clearly communicate the purpose of data processing to individuals and ensure that the processing is fair and transparent.
Consent: The GDPR sets stricter standards for obtaining consent from individuals for processing their data. Consent must be freely given, specific, informed, and unambiguous. Individuals have the right to withdraw their consent at any time.
Data Breach Notification: One of the significant aspects of the GDPR is the requirement for organizations to report data breaches that may compromise the security of personal data. If a data breach occurs that is likely to result in a risk to individuals' rights and freedoms, the organization must notify the relevant supervisory authority (a data protection authority) within 72 hours of becoming aware of the breach.
Penalties and Enforcement: The GDPR introduces substantial penalties for non-compliance. Organizations that violate the regulation can be fined up to 4% of their global annual revenue or €20 million, whichever is higher, depending on the severity of the violation.
Data Protection Officers (DPOs): Some organizations are required to appoint a Data Protection Officer, an individual responsible for overseeing data protection activities within the organization and ensuring compliance with the GDPR.
Cross-Border Data Transfers: The GDPR includes provisions for the transfer of personal data outside the EU to ensure that data protection standards are upheld in such transfers.

In summary, the GDPR is a comprehensive regulatory framework designed to give individuals greater control over their personal data and to ensure that organizations handle personal data responsibly and securely. Its provisions extend beyond the borders of the EU, impacting any organization that processes the personal data of EU citizens, regardless of its location. The regulation underscores the importance of data protection and privacy in today's digital age.

☑ Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure the secure handling, storage, processing, and transmission of credit card information. It is an international standard developed to protect sensitive cardholder data and prevent data breaches within organizations that handle credit card transactions. The PCI DSS is intended to create a secure environment for payment card data and to maintain consumer trust in the security of payment card transactions.

Key points about PCI DSS include:

Scope of Application: The PCI DSS applies to any organization that handles credit card data, including merchants, service providers, financial institutions, and other entities involved in the payment card ecosystem. This includes both physical point-of-sale systems and online payment gateways.

Data Security Requirements: The PCI DSS outlines a comprehensive set of security requirements and best practices that organizations must follow to ensure the security of payment card data. These requirements cover areas such as network security, access controls, encryption, vulnerability management, and regular security testing.

Protection of Cardholder Data: A primary focus of the PCI DSS is the protection of cardholder data, which includes the full range of sensitive information associated with payment cards, such as card numbers, expiration dates, cardholder names, and security codes (CVV/CVC).

Security Controls: The standard defines a set of security controls that organizations must implement, including:

- Building and maintaining a secure network infrastructure.
- Implementing access controls to restrict access to cardholder data.
- Encrypting sensitive data during transmission and storage.
- Regularly monitoring and testing security systems and processes.
- Maintaining a strong security policy to guide security practices within the organization.

Compliance Validation: Organizations that handle payment card data are required to undergo periodic assessments to validate their compliance with the PCI DSS. The assessment type depends on factors such as transaction volume and the level of cardholder data exposure. Common assessment methods include self-assessment questionnaires and external audits conducted by Qualified Security Assessors (QSAs).

Levels of Compliance: PCI DSS compliance is categorized into different levels based on the volume of transactions handled by the organization. The higher the volume, the more stringent the compliance requirements become.

Consequences of Non-Compliance: Failure to comply with the PCI DSS can have serious consequences, including financial penalties, reputational damage, and potential loss of the ability to process credit card payments. Data breaches resulting from non-compliance can also lead to legal and regulatory consequences.

Ongoing Compliance: PCI DSS compliance is not a one-time effort but an ongoing process. Organizations must continuously monitor and update their security practices to address evolving threats and vulnerabilities.

In summary, the Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized framework that ensures the secure handling of credit card data and helps prevent data breaches that could compromise cardholder information. By implementing the security controls and best practices outlined in the standard, organizations can reduce the risk of data breaches, protect consumer information, and maintain the trust of their customers in the security of their payment card transactions.

☑ The Health Insurance Portability and Accountability Act (HIPAA)

HIPAA is a federal law established in 1996 to protect U.S. patients' health information. This law prohibits patient information from being shared without their consent. Organizations have a legal obligation to inform patients of a breach.

Explanation: The Health Insurance Portability and Accountability Act (HIPAA) is a federal law enacted in 1996 in the United States to safeguard the privacy and security of patients' health information. HIPAA establishes standards and regulations for how healthcare providers, health plans, and other covered entities handle and protect individuals' protected health information (PHI).

Key points about HIPAA include:

Patient Privacy Protection: HIPAA places a strong emphasis on protecting the privacy of patients' health information. Covered entities are required to implement safeguards to ensure that patients' PHI is kept confidential and not disclosed without proper authorization.

Authorization and Consent: Under HIPAA, covered entities are generally prohibited from sharing patients' PHI without their explicit authorization or consent. This means that healthcare providers and other entities need to obtain written consent from patients before disclosing their health information for purposes other than treatment, payment, and healthcare operations.

Protected Health Information (PHI): PHI includes any individually identifiable health information, such as medical records, diagnoses, treatments, prescriptions, and other health-related data. This information is protected under HIPAA regardless of its format, whether it's in electronic, paper, or oral form.

Minimum Necessary Standard: Covered entities are required to follow the "minimum necessary" principle, meaning they should only access, use, or disclose the minimum

amount of PHI necessary to accomplish a specific purpose. This helps limit unnecessary exposure of sensitive information.
Breach Notification: HIPAA mandates that covered entities and their business associates (third-party organizations that handle PHI on behalf of covered entities) must notify affected individuals and the U.S. Department of Health and Human Services (HHS) in the event of a breach of unsecured PHI. Breach notification must occur without unreasonable delay and no later than 60 days after the discovery of the breach.
Enforcement and Penalties: HIPAA violations can lead to substantial penalties, both civil and criminal, depending on the severity of the violation. Penalties can range from fines to criminal charges, and they are determined based on factors such as the nature of the violation and the organization's efforts to prevent and address the breach.
HIPAA Privacy Rule and Security Rule: HIPAA consists of multiple rules, with the Privacy Rule and the Security Rule being two of the most prominent. The Privacy Rule addresses the use and disclosure of PHI, while the Security Rule establishes standards for the security of electronic PHI (ePHI).
Business Associate Agreements: Covered entities that share PHI with third-party organizations, known as business associates, must establish a Business Associate Agreement (BAA) to ensure that the business associate also complies with HIPAA regulations and protects the security and privacy of the shared PHI.

In summary, HIPAA is a federal law designed to protect patients' health information and ensure their privacy rights are upheld when it comes to the use, disclosure, and security of their protected health information. Covered entities and their business associates are legally obligated to follow HIPAA regulations, and breaches of PHI must be reported to affected individuals and regulatory authorities in a timely manner.

☑ System and Organizations Controls (SOC type 1, SOC type 2)

The SOC1 and SOC2 are a series of reports that focus on an organization’s user access policies at different organizational levels. They are used to assess an organization’s financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation:

SOC1 and SOC2 are important audit and reporting frameworks that assess an organization's internal controls related to various aspects of financial compliance, risk management, and data security. They provide assurance to stakeholders about the effectiveness of an organization's control environment.

SOC1 (Service Organization Control 1): SOC1 reports, also known as SSAE 18 reports (Statements on Standards for Attestation Engagements No. 18), are designed to evaluate the internal controls that impact financial reporting. They are particularly relevant for organizations that provide services that could affect the financial statements of their clients. SOC1 reports come in two types:

- Type 1: This report assesses the design of an organization's internal controls as of a specific date. It determines whether the controls are suitably designed to achieve their intended objectives.
- Type 2: This report not only evaluates the design of controls but also assesses their operating effectiveness over a specified period. It includes testing to determine if the controls are functioning as intended.

SOC2 (Service Organization Control 2): SOC2 reports are focused on an organization's non-financial internal controls, specifically those related to security, availability, processing integrity, confidentiality, and privacy. SOC2 reports are based on the Trust Services Criteria, which address the principles of security, availability, processing integrity, confidentiality, and privacy. SOC2 reports are essential when an organization's services involve handling sensitive customer data or providing cloud-based services. SOC2 reports also come in two types:

- Type 1: Similar to SOC1, this report evaluates the design of controls at a specific point in time.
- Type 2: This report assesses both the design and operating effectiveness of controls over a defined period, verifying that controls are consistently implemented and producing the desired outcomes.

Both SOC1 and SOC2 reports are relevant for different purposes and audiences:

- Financial Compliance and Risk Assessment: SOC1 reports are primarily used to assess the impact of a service organization's processes on the financial statements of its clients. They help clients evaluate the risk of material misstatement in their financial reports due to the services provided by the service organization.
- Data Security and Control Environment: SOC2 reports focus on an organization's security, availability, processing integrity, confidentiality, and privacy controls. They are crucial for organizations that handle sensitive data and need to assure clients and stakeholders about the security and privacy of their operations.
- Fraud Prevention and Control Failures: Control failures in the areas covered by SOC2, such as security, availability, and data privacy, can indeed lead to vulnerabilities that could be exploited for fraudulent activities. The reports help identify these vulnerabilities and enable organizations to take corrective actions.

In summary, SOC1 and SOC2 reports are essential tools for organizations to demonstrate their adherence to specific control standards. While SOC1 assesses financial controls, SOC2 focuses on broader areas of security and operational effectiveness. Both reports play a vital role in building trust with clients, partners, and stakeholders and ensuring the overall integrity, security, and compliance of an organization's operations.