IT Vendor Management: Data Security Standards and Regulations Overview

Independent Industry Standards

Control Objectives for Information and Related Technologies (COBIT)	The Information Systems Audit and Control Association (ISACA) created a security framework for IT best practices that include risk management, governance, and information security guidance and controls.
Center for Internet Security (CIS)	This nonprofit organization of information security professionals acts as a governing community. CIS offers a set of controls organized into 20 different groups and ranked as basic, fundamental, and organizational levels. CIS control sets are available for free download.
Common Security Framework (CSF)	This is a for-profit organization created by the HITRUST Alliance. This set of controls was initially intended for healthcare organizations to assess HIPAA privacy and security standard adherence. Non-healthcare organizations now use it to determine the maturity of their information security.

Governmental Security and Privacy Regulations

The Federal Information Security Management Act (FISMA)	FISMA defines security frameworks that comprehensively protect government data, assets, and operations against human-created or natural threats.
Family Educational Rights and Privacy Act of 1974 (FERPA)	This law shields student education record privacy and applies to schools that take in funds under the U.S. Department of Education, an applicable program.
Health Insurance Portability and Accountability Act (HIPAA)	This federal law protects patient health information from being disclosed without patient knowledge or consent. Healthcare providers and their vendors establish three types of controls for electronic patient data: administrative, physical, and technical.

The Sarbanes-Oxley Act of 2002	This federal law determined the wide-ranging financial and auditing regulations that apply to publicly held companies to protect the public, shareholders, and employees from fraudulent financial practices and accounting errors.
California Consumer Privacy Act of 2018 (CCPA)	The CCPA enhances personal information privacy rights and consumer protections for California residents.
The Gramm-Leach-Bliley Act (GLB Act or GLBA)	By this law, financial institutions must communicate how customers' sensitive data is shared, inform customers of their right to opt out of personal data sharing with third parties, and apply specified protections on customers' private data.

Finance and Payment Security Specific Regulations and Protocols

Payment Card Industry Data Security Standard (PCI-DSS)	PCI-DSS is the security standard for organizations that handle major credit cards.
PCI-3DS	This is a messaging protocol that enables e-commerce purchasers to authenticate themselves with their card issuer. The additional security layer prevents unauthorized transactions and protects the merchant from exposure to fraud.
P2PE	The PCI Security Standards Council established this standard. With a credit card swipe, a payment security solution converts confidential payment card data into unreadable code.

International Frameworks and Regulations

HITRUST CSF	Originally created for healthcare, the framework for regulatory compliance and risk management now applies to all data. HITRUST CSF is customizable through various factors, including organization type, size, systems, and regulatory requirements.

Personal Information Protection and Electronic Documents Act (PIPEDA)	Used in Canada, PIPEDA regulates how businesses in the private sector collect, utilize, and disclose personal information.
General Data Protection Regulation (GDPR)	The GDPR is a legal security framework for collecting and processing individuals' personal information within the European Union (EU). GDPR is critical to corporate compliance officers at banks, insurers, and other financial company regulators.
ITIL, formerly an acronym for Information Technology Infrastructure Library	Mostly used in the United Kingdom, ITIL offers tasks, processes, checklists, and procedures that are not organization- or technology-specific but can guide IT management and implementation in organizations to support business needs. ITIL application demonstrates compliance and improvement measurement.
ISO 27000 Standards	This is a series of standards to guide information security and risk management. ISO 27000 informs GDPR requirements and is used mostly outside the United States. The standard offers an extensive catalog of controls. Specifically, ISO 27001 is the framework for information security management systems (ISMS) used to ensure legal compliance, availability of information, confidentiality, and content integrity.

Public Accounting Security Standards | Governed by the American Institute of Certified Public Accountants (AICPA)

SAS 70	An audit using SAS 70 verifies data center controls and processes apply. There is no SAS 70 certification; rather, it refers to an auditing process.
SSAE 16 (Statements on Standards for Attestation Engagements No. 16)	The audit verifies processes and controls, and it requires a written report about the operating effectiveness and reviewed controls' design.

System and Organization Controls (SOC) Levels 1, 2, and 3

Independent, third-party auditors provide SOC reports to examine various company aspects and ensure that they operate in a compliant and ethical manner.

A SOC 1 audits internal controls at a service organization that may affect financial reports for their clients' internal controls. A SOC 1, Type 2 report includes Type 1 and an audit on the controls' effectiveness over specific periods, usually less than a year.

An SOC 2 is intended for services storing customer data in the cloud. It applies to nearly all software-as-a-service companies and businesses that keep customer data in the cloud.

Both SOC 2 and 3 offer pre-defined, standard benchmarks for controls related to availability, processing integrity, security, privacy, or systems confidentiality.

A SOC 3 report is intended for general use and provides certification to assure data center users of security, process integrity, and high availability.

U.S. Government Security Standards and Frameworks

NIST 800 Series (National Institute of Standards and Technology)

The NIST 800 Series documents describe U.S. federal government computer security procedures, policies, and guidelines. These standards pertain to information security and privacy guidelines, and they are used to help secure U.S. federal government infrastructure and by private industry.

NIST Special Publication 800-53

The NIST Special Publication 800-53 is a catalog of security controls for every non-national-security U.S. federal information system. Published by the National Institute of Standards and Technology, 800-53 is the basis of many compliance frameworks. The NIST Cybersecurity Framework is a U.S. standard.