DATABANK
Data Center Evolved™

DataBank's Guide to Data Center Compliance

FedRAMP

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations™

HIPAA HITECH Compliant

PCI

INFORMATION SECURITY MANAGEMENT SYSTEM
ISO 27001
CERTIFIED
360 ADVANCED
ASSESSED BY 360 ADVANCED

CR20230728-01

A CONCISE OVERVIEW OF THE DEFINITIONS, METHODOLOGIES AND RESPONSIBILITIES THAT COMPLIANCE DEMANDS OF YOU AND YOUR SOLUTION PROVIDER

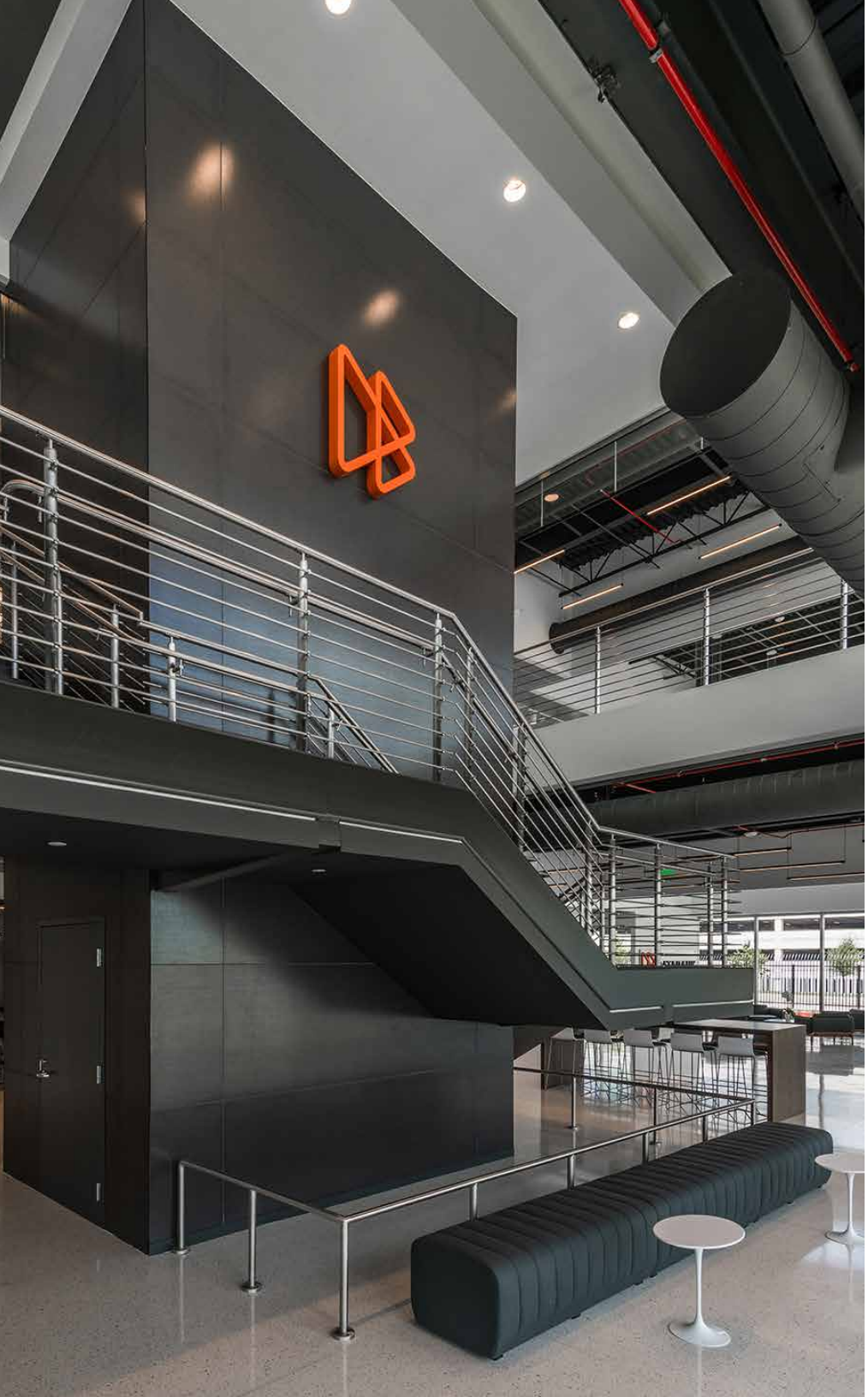


TABLE OF CONTENTS

DATABANK

NAVIGATING THE WORLD OF COMPLIANCE

Navigating the complexity and the ever-changing nature of compliance is challenging, regardless of industry or company size. That's why many industry-leading clients turn to DataBank to enable security and compliance for their infrastructure platforms, applications, and websites.

As a supplier of secure **FISMA, FedRAMP, FISMA, CMMC, ISO 27001, NIST, ITAR, HIPAA/HITECH,** and **PCI-DSS** compliant data centers, cloud services, and colocation solutions, we hold an Authority to Operate (ATO) from multiple U.S. Federal Agencies.

We also support a variety of federal agencies, healthcare organizations, financial services companies, merchants, and SaaS providers. This enables us to keep customer infrastructures, websites, and applications compliant with our Managed Cloud platform and **SSAE SOC 1 Type 2** and **SOC 2 Type 2** compliant colocation facilities.

What do these compliance designations really mean? What is required to be considered "compliant" with a designation? And who is responsible for each compliance action?

This guide answers these questions and clarifies the designations and actions DataBank takes on your behalf to ensure your business meets the requirements for each designation.

DEFINITIONS AND CLARIFICATION OF TERMS

Identifying compliance programs pertaining to your business and working towards meeting the requirements helps to understand the various terminology. Here's a rundown of the key concepts to guide you in your journey.

AUDITS VS. ASSESSMENTS

Both audits and assessments are essential to a comprehensive information security program:

- Audits verify compliance with regulations and assure stakeholders (customers, vendors, employees, company executives, and the board of directors) that you fully meet the requirements of the regulations.
- Assessments help you understand and improve your organization's security posture and overall state of compliance.

AUDIT

- Formal process that occurs regularly (usually annually).
- Independent evaluation conducted by a third party.
- Typical scoring is Pass/Fail in meeting the specific requirements.

ASSESSMENT

- Informal process conducted by internal or external resources.
- Identifies vulnerabilities, weaknesses, and risks to understand the overall security posture.
- Flexible scope (broad or narrow, full or partial).
- Periodic frequency (structured or internally defined).
- Provides results and recommendations in a detailed report.

COMPLIANT VS. CERTIFIED

Achieving both compliant and certified status indicates adherence to the requirements of a regulation or standard, and both are critical to building a strong information security program. Certifications hold more weight as they achieve formal recognition from a third party.

COMPLIANCE

- The environment adheres to specific guidelines, standards, or regulations.
- Determined internally or by a third-party assessment after examining systems, processes, and controls.
- An ongoing state: regular audits or assessments may be required to maintain compliance.
- Demonstrates at the time of the assessment that the requirements were met for the regulation or standard.

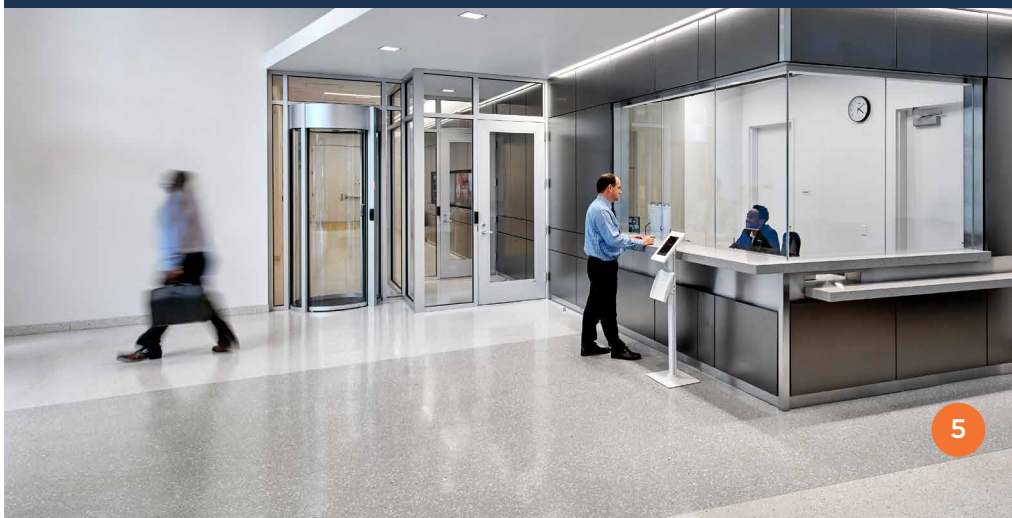
CERTIFICATION

- Rigorous process with formal acknowledgment by a third party that criteria/standards are met.
- External audit by an accredited body examining processes, controls, and systems against specific standards.
- The certification has an expiration date (usually) and requires periodic re-assessment or audit (usually annually).
- Provides a higher level of assurance to stakeholders.
- Demonstrates standards are not only met but also vetted by an external, accredited third party.

REGULATIONS VS. STANDARDS

- Regulations are detailed instructions issued by a governing body on how to carry out and enforce security policies. For organizations that a regulation pertains to, they essentially carry the force of law. Their application is mandatory, and failure to comply can result in stiff penalties.

- Standards guide organizations in implementing security policies and making informed decisions on strengthening security postures. They also provide a method to ensure security controls are applied consistently across organizations that choose to follow them. Complying with a standard is not mandated by a governing body. However, a customer or vendor may require compliance with specific standards, and doing so demonstrates to stakeholders that you have a strong security posture.



WHY COMPLIANCE MATTERS

Compliance is critically important in today's data center environment for several reasons:

- **Data Protection –** More and more information is stored in the cloud and needs to be protected from breaches, leaks, and unauthorized access.
- **Regulatory Requirements –** Many industries have or are creating regulations that mandate levels of data protection; non-compliance can result in hefty fines.
- **Reputation and Trust –** Security breaches can be devastating to a reputation. Once customers lose trust in a company's ability to secure their data, it's tough to regain.
- **Economic Considerations –** Breaches can be expensive, not only in direct cost but also in lost business and the cost of remediation.
- **Shared Responsibility –** Security is often a shared responsibility between a cloud provider and a customer. Cloud providers secure infrastructure while customers handle applications and data.
- **Vendor Management –** Compliance ensures vendors at third-party cloud providers follow best practices for vendor management.
- **Data Sovereignty and Residency –** Different countries have different regulations; cloud service providers understand and maintain the complexities of international compliance requirements.
- **Business Continuity –** Compliance encompasses not only protection against breaches but also assurance of the availability of disaster recovery capabilities.
- **Incident Response –** It's not if but when there is an incident; implementing a plan for incident response and recovery is vital.

FedRAMP

WHAT IS FedRAMP?

The Federal Risk and Authorization Management Program **(FedRAMP)** empowers government agencies to transform their infrastructure and encourage secure cloud adoption. The program provides a standardized framework for security assessment, authorization, and continuous monitoring of cloud products and services. By focusing on standardization processes and the identification and mitigation of risk across all agencies, FedRAMP uniquely positions the federal government to reduce costs and resources associated with employing security measures.

DOES FedRAMP APPLY TO YOUR ORGANIZATION?

FedRAMP is required for federal agency cloud deployments and service models at low, moderate, and high-risk impact levels. The only exceptions are private cloud deployments for single organizations implemented entirely within federal facilities. In this case, FISMA would then be required, which applies to all information systems operated by a U.S. federal agency or contractor.

Three key entities are involved with FedRAMP: agencies, cloud service providers (CSP), and third-party assessment organizations (3PAO). The process is quite extensive. First, an agency selects a cloud service provider that is FedRAMP Ready or FedRAMP Authorized. It's important to note that FedRAMP Ready systems are not FedRAMP Authorized and thus must undergo an authorization process.

Next, the 3PAO assesses the CSP and provides evidence of compliance to ensure FedRAMP requirements are followed continuously. Once the assessment is complete, an Authority To Operate (ATO) is issued, and the real work of deployment and operations begins.

HOW DATABANK SUPPORTS AGENCIES SUBJECT TO FedRAMP

DataBank offers a versatile, cost-effective cloud solution for government agencies and their systems integrators and SaaS providers that meets the robust security requirements outlined by FedRAMP.

DataBank cloud platforms are FedRAMP certified as Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). DataBank provisions public and private FedRAMP-compliant cloud environments quickly, enabling existing and new applications to function within FedRAMP's comprehensive security framework.

In addition, DataBank assists customers with their requirements for SaaS authorizations by providing business partners to conduct gap analysis and remediation of the SaaS platform. Although DataBank is not a 3PAO or consultant, we collaborate with trusted partners who know our platform, and we assist customers with writing their portion of the System Security Plan (SSP) and associated supporting documentation as part of our professional services engagements.

On an annual basis, DataBank also conducts a Continuous Monitoring (ConMon) assessment with an authorized 3PAO. The DataBank ConMon assessment is conducted between March and June of each year.

WHAT IS FISMA?

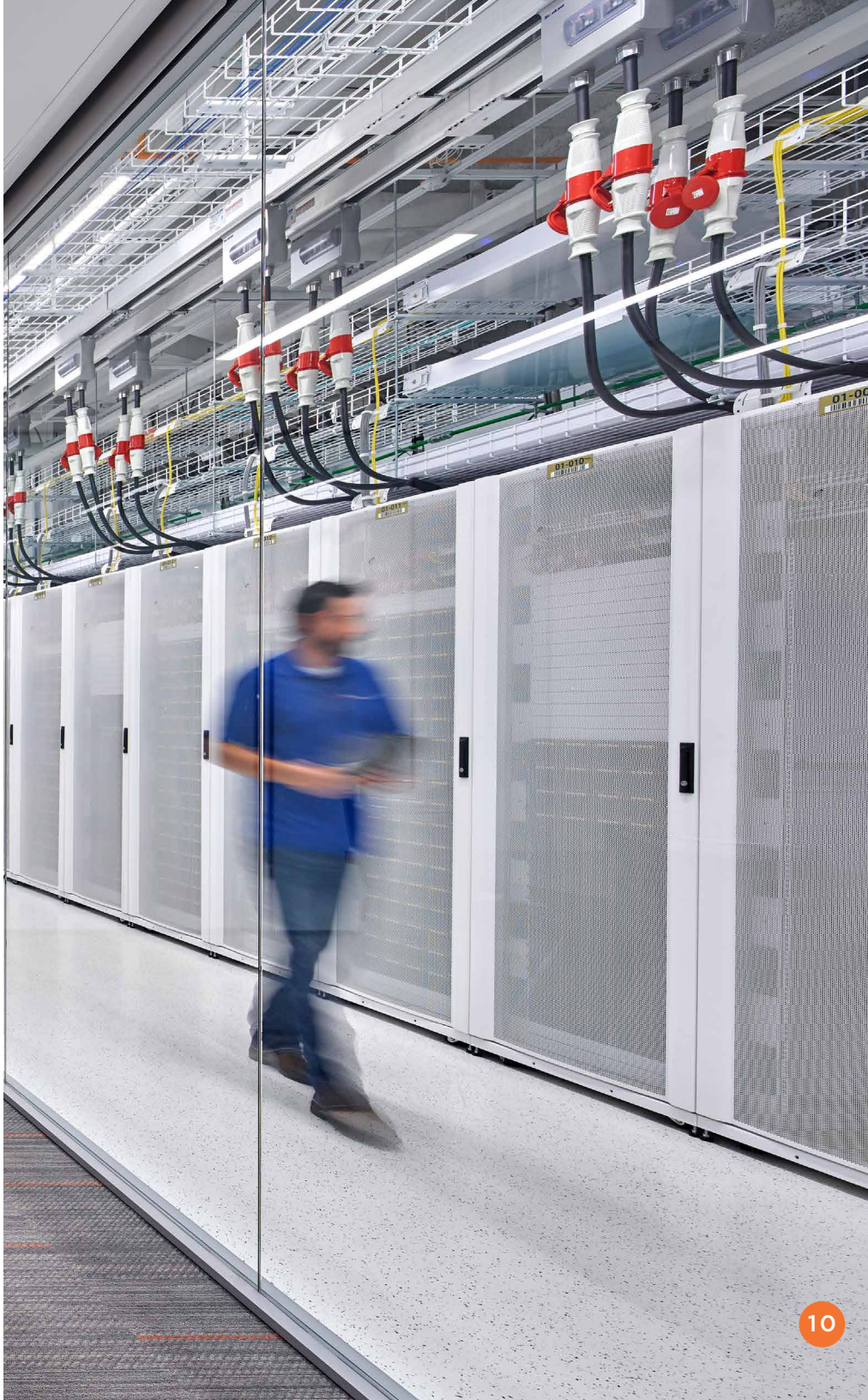
The Federal Information Security Management Act **(FISMA)** is a United States federal law enacted as part of the Electronic Government Act of 2002. FISMA bolsters computer and network security within the federal government and affiliated parties (such as government contractors) by mandating a comprehensive framework to protect government information, operations, and assets against natural or man-made threats.

FISMA

DOES FISMA APPLY TO YOUR ORGANIZATION?

Organizations should comply with FISMA for several reasons:

1. Legal Requirement: For federal agencies and organizations that contract with the federal government, compliance with FISMA is mandatory. Failure to comply can result in legal and financial consequences.
2. Enhanced Security: FISMA establishes a set of guidelines and standards to protect information systems and data, which can significantly enhance an organization's security posture.
3. Risk Management: FISMA emphasizes a risk-based approach to security, requiring organizations to assess and mitigate risks to their information systems. This can help organizations prioritize their security efforts and resources effectively.
4. Trust and Credibility: Compliance with FISMA can enhance an organization's reputation and credibility, demonstrating a commitment to securing sensitive government data. This can be particularly important for organizations seeking to do business with the federal government.
5. Incident Response and Recovery: FISMA requires organizations to have plans for incident response and recovery, ensuring that they can respond effectively to security incidents and minimize damage.



CMMC

WHAT IS CMMC?

Cybersecurity Maturity Model Certification **(CMMC)** 2.0 streamlines the original CMMC framework by reducing the levels of cybersecurity maturity from five to three:

- Level 1 (Foundational)
- Level 2 (Advanced)
- Level 3 (Expert)

Each level corresponds to a set of cybersecurity practices and processes that contractors must implement, with the requirements becoming more stringent as the levels progress.

WHO IS REQUIRED TO COMPLY WITH CMMC?

DoD contractors, subcontractors, and other companies doing business with the DoD supply chain must comply with the CMMC 2.0 framework. The specific level of certification depends on the sensitivity of the defense information that the contractor handles or processes:

- Level 1 (Foundational): Companies at this level deal with Federal Contract Information (FCI) and must implement 17 basic cybersecurity practices.
- Level 2 (Advanced): Contractors that handle or process Controlled Unclassified Information (CUI) must meet the requirements of Level 2, which aligns with the NIST SP 800-171 standard, plus a small number of additional practices and processes.
- Level 3 (Expert): This level is reserved for companies that work on high-priority defense programs and technologies. The requirements for this level are more advanced and are intended to protect information critical to national security.

CMMC 2.0 ensures a uniform cybersecurity standard across the Defense Industrial Base to protect against increasing cyber threats and safeguard national security. Compliance with CMMC 2.0 is becoming a prerequisite for bidding on DoD contracts, making it essential for contractors and subcontractors in the defense sector to achieve the necessary level of certification.

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO CMMC

Cloud service providers (CSPs) are not directly certified under CMMC 2.0. Instead, the DoD contractors who use cloud services must ensure that their CSPs meet the necessary CMMC 2.0 requirements relevant to the data they process or store. DataBank demonstrates the compliance of its data centers through FedRAMP (Federal Risk and Authorization Management Program) certifications and alignments with NIST (National Institute of Standards and Technology) standards, such as NIST SP 800-171, which are integral to CMMC Level 2 compliance.

WHAT IS ISO/IEC 27001?

ISO 27001

The International Standards Organization (ISO) and the International Electrotechnical Commission (IEC) are standards-setting bodies. **ISO/IEC 27001** is the world's best-known standard for information security management, and the standard defines the requirements that security management systems must meet to prove they keep physical and logical assets secure.

ISO/IEC 27001 is not a government standard; compliance is voluntary. To verify compliance, independent assessors audit an organization's information security management systems to ensure policies and procedures protect internal IT systems and data center infrastructures used by customers, vendors, partners, and other third parties. The standard also guides organizations in managing the security of intellectual property, financial information, employee information, and private information.

DOES ISO/IEC 27001 APPLY TO YOUR ORGANIZATION?

ISO and IEC are not regulatory bodies. They are international, non-government affiliated standard-setting organizations that offer voluntary guidance for information security management and practices. Neither ISO nor IEC can issue compliance mandates. Consequently, no organization is subject to obligatory ISO/IEC 27001 compliance.

However, compliance helps organizations avoid potentially costly security breaches. Organizations can also protect and enhance their reputation by demonstrating to customers, partners, vendors, and shareholders how they have taken steps to protect data in case of a breach.

This also helps win business while minimizing the financial and reputational damage caused by a data breach. In addition, compliance with ISO/IEC 27001 ensures the selection of adequate and proportionate security controls that help protect information in line with increasingly rigid regulatory requirements such as the General Data Protection Regulation (GDPR) and the Network and Information Systems (NIS) regulation.

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO ISO/IEC 27001

DataBank follows the ISO/IEC 27001 certification requirements to promote a holistic approach to information security—vetting people, policies, and technology—to ensure we implement information security management systems according to this standard for risk management, cyber-resilience, and operational excellence.

DataBank received certification from ISO/IEC for our internal corporate IT systems and all our colocation data centers in the U.S. and UK hosting customer IT infrastructures. Conformity with ISO/IEC 27001 signifies that DataBank has established and implemented information security management systems while continuing to maintain and improve our systems. Compliance with the standard also demonstrates DataBank has implemented a system to manage risks related to the security of our data, and the system follows all the best practices and principles enshrined in the standard.

Implementing the information security framework specified in the ISO/IEC 27001 standard enables DataBank to achieve multiple objectives in support of our customers:

- Reduces vulnerabilities to the growing threat of cyberattacks.
- Enables fast responses to evolving security risks.
- Ensures assets such as financial statements, intellectual property, employee data, and information entrusted by customers and vendors remain undamaged, confidential, and available.
- Provides a centrally managed framework that secures all information in one place.
- Prepares people, processes, and technology throughout our organization to face technology-based risks and other threats.
- Secures information in all forms, including paper-based, cloud-based, and digital data.

By receiving ISO/IEC 27001 certification, DataBank demonstrates to stakeholders and customers across the globe that we are committed and able to manage information securely and safely.

SSAE

SOC 1, SOC 2, & SOC 3

WHAT IS SSAE?

Statement on Standards for Attestation Engagements **(SSAE)** is a set of auditing standards published by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). The standards continuously redefine and update how service organizations report on compliance.

Intro continued on next page.

Auditors use SSAE to report on the finding of controls—including security—within organizations such as data centers, Internet service providers, and other entities required to establish information security controls. SSAE includes three types of System and Organization Controls reports—SOC 1 Type 2, SOC 2 Type 2, and SOC 3:

The controls at a service organization are relevant to user entities' internal control over financial reporting.

SOC 2 is for the management of a service organization, user entities, and other specified parties to receive a CPA's opinion on the controls (AICPA).

A SOC 2 report provides three key components:

- Description of the system.
- Opinion on the fairness of the presentation of the description.
- Description of the service auditor tests of controls and results.

SOC 3 provides interested parties (i.e., DataBank customers) with a CPA's opinion about the controls.

Both SOC 2 and SOC 3 reports are based upon the same attestation principles (testing criteria)—the AT101. The engagement (audit) is performed and defined the same. SOC 2 and SOC 3 also both report on controls related to security, availability, processing integrity, confidentiality, privacy, or a subset of these.

The difference between SOC 2 and SOC 3 lies in a couple of key areas—the purpose and components of the report itself. The SOC 2 report is for managing a service organization (like DataBank), user entities, and other specified parties to receive a CPA's opinion on the controls. The SOC 3 report provides interested parties with a CPA's opinion about the controls. When you look at the statements, there is nothing different between the results of the two except that SOC 2 spells out who the interested parties may be, e.g., management and user entities.

The component differences are also slight in words but mighty in results. A SOC 2 report provides three key components:

1. A description of the system.
2. An opinion on the fairness of the presentation of the description.
3. A description of the service auditor's tests of controls and results.

SOC 3 is equivalent to SOC 2 part 2, where an opinion is rendered on whether the entity maintained effective system controls. Parts 1 and 3 are not reported in SOC 3. However, the details of part 3 are important to a DataBank customer because they show what was tested, how it was tested, and the testing results.

In conclusion, a SOC 2 report shows everything and then some of a SOC 3 report. A vendor's security evaluation should seek the SOC 2 over the SOC 3 report because the SOC 2 report provides assurance and knowledge of what was tested, how it was tested, and the results of each individual testing function. This provides a greater understanding of the organization your data is entrusted to.

Note: SOC 2 and SOC 3 reports are based on the same attestation principles. The audit function is performed and defined in the same fashion. They both report on controls related to security, availability, processing integrity, confidentiality, or privacy (or a subset of these).

DOES SSAE APPLY TO YOUR ORGANIZATION?

SSAE applies primarily to service organizations otherwise known as outsourced data centers. Another entity hires them to process transactions and data, which are usually confidential. The service organizations are considered part of the users' internal control and typically perform these functions:

- Accounting
- Benefits
- Billing
- Clearinghouse
- Collection
- Finance
- Insurance
- Investment
- Information Technology
- Market research
- Payroll

HOW DATABANK SUPPORTS ORGANIZATIONS SEEKING AN SSAE COMPLIANT DATA CENTER:

DataBank commits to performing an annual SSAE SOC 1 and SOC 2 audit in every data center. Certification includes service auditor reports on the fairness of management's description of the service organization's system controls, design, and operating effectiveness over a one-year period—spanning from October 1 through September 30 each year.

Audits are conducted by an impartial independent third party. Annual reports are published between December 15 and 31 of each year and are available on a self-service download basis. DataBank also provides a bridge letter in the same location to cover the gap between the date of issuance on the report and the next audit completion.

THE NIST 800 SERIES

NIST

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Federal Government that operates a physical sciences lab to test standards before publication. Security and IT standards can be found within the 800 series, with the **NIST SP800-53R5** being the current, relevant, and comprehensive security control set.

Intro continued on next page.

This control set has three levels of assignment based upon risk: low, moderate, or high. Most systems are categorized as moderate and thus have 323 controls assigned to secure them.

Within NIST SP800-53R5, there are 18 control families, ranging from access control to awareness, training, supply chain acquisition, and physical and environmental controls. NIST SP800-53R5 is also the basis for a comprehensive security program to comply with HIPAA/HITECH and secure U.S.-based medical information systems.

The Department of Health and Human Services (DHHS) uses these NIST standards to determine whether a healthcare entity has met security standards when issuing fines for breached data. DataBank utilizes NIST SP800-53R5 moderate standards for the corporate security baseline and methodology.

NIST SP800-171 is the collection of controls and requirements that non-federal computer systems must utilize to store, process, or transmit Controlled Unclassified Information (CUI). SP800-171 compliance is currently used by the Department of Defense under DFARS 2525.204-7012.

The CUI Program addresses several deficiencies in managing and protecting unclassified information, including inconsistent markings, inadequate safeguarding, and needless restrictions—both by standardizing procedures and providing common definitions through a CUI Registry.

The purpose of SP800-171 is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI when the CUI resides in a non-federal system or organization when the non-federal organization is not collecting or maintaining information on behalf of a federal agency or using or operating a system on behalf of an agency; and where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or government-wide policy for the CUI.

DOES NIST 800-53 OR 800-171 APPLY TO YOUR ORGANIZATION?

Use of NIST standards is compulsory when securing federal (including Department of Defense) data. The use of NIST standards is a preferred methodology for securing state and local data.

HOW DATABANK SUPPORTS ORGANIZATIONS SEEKING A NIST SP800-53 DATA CENTER:

DataBank commits to performing annual continuous monitoring for its data centers that are FedRAMP certified (currently DFW1, DFW3, MSP2, and MSP3). For those data centers not under FedRAMP certification, DataBank conducts annual third-party SSAE SOC 1 Type 2 and SOC 2 Type 2, HIPAA, PCI-DSS, and ISO 27001 assessments that test the security controls of these facilities.

All DataBank facilities and systems use the NIST SP800-53 methodology as their base security methodology. DataBank also maintains FISMA-authorized data centers in addition to the above to allow customers to utilize our colocation spaces to build their own environments.

3PAO assessments include completing a Security Assessment Report (SAR) provided to the FedRAMP PMO annually for review. SSAE and HIPAA reports include service auditor reports on the fairness of management's description of the service organization's system controls, design, and operating effectiveness over one year—spanning from October 1 through September 30 each year. An impartial, independent third party conducts the audit.

3PAO annual reports are then provided to the FedRAMP program management office in early June each year, while SSAE and HIPAA annual reports are published between December 15 and 31 of each year. SSAE, PCI-DSS, and HIPAA reports are available on a self-service download basis. DataBank provides a bridge letter in the same location to cover the gap between the date of issuance on the report and the next audit completion.

ITAR

WHAT IS ITAR?

The International Traffic in Arms Regulation **(ITAR)** is a U.S. federal law that regulates and limits the export, import, sale, and distribution of defense-related technologies to or from foreign (non-U.S.) agents, governments, and entities. Defense-related items, called munitions under ITAR, can be identified as anything from encryption algorithms and computer software for accounting defense items to bombs, guns, ships, tanks, and airplanes. ITAR is governed by 22 U.S.C. 2778 of the Arms Export Control Act and Executive Order 13637 (delegates to the Secretary of State).

DOES ITAR APPLY TO YOUR ORGANIZATION?

ITAR compliance is required for organizations that engage with the United States in the business of manufacturing or exporting defense articles, temporarily importing defense articles, or furnishing defense services. Six defense services are further defined in e-CFR Title 22, Chapter I, Subchapter M, Part 120.9. The Munitions List is specific regarding the items controlled under ITAR.

In other words, if your organization doesn't manufacture, export, or temporarily import products on the munitions list of furnishing defense services, ITAR doesn't apply to you. ITAR is a federal law that affected organizations cannot easily overlook.

Note: ITAR requires a registration process for organizations with products that fall within the ITAR Munitions List. There is no ITAR certification that a manufacturer or service provider of a manufacturer of munitions can obtain.

HOW DATABANK SUPPORTS ITAR REGISTERED CUSTOMERS:

DataBank fully supports the efforts of ITAR and ensures compliance and security protocols are in place for ITAR-registered customers. DataBank demonstrates security capabilities through annual audits by third parties. Relevant certifications held by DataBank include a FedRAMP Authority to Operate (ATO) and SSAE SOC 1 Type 2 and SOC 2 Type 2. The FedRAMP ATO is most applicable to an ITAR-registered organization. A federally-authorized 3PAO conducts the FedRAMP ATO assessment.

WHAT IS HIPAA?

HIPAA

HIPAA is the Healthcare Insurance Portability and Accountability Act, passed by Congress in 1996. It serves four main purposes:

1. **Privacy of health information:** Requires the protection and confidential handling of protected health information.
2. **Security of electronic records:** Reduces healthcare fraud and abuse.
3. **Administrative simplification:** Mandates industry-wide standards for health care information on electronic billing and other processes.
4. **Insurance portability:** Provides the ability to transfer and continue health insurance coverage for millions of American workers and their families when they change or lose their jobs.

Intro continued on next page.

The HIPAA Privacy Rule requires healthcare providers, organizations, and their business associates to comply with mandated procedures that ensure the confidentiality and security of protected health information (PHI) and electronic protected health information (e-PHI) when it is transferred, received, handled, or shared.

DOES THE HIPAA PRIVACY RULE APPLY TO YOUR ORGANIZATION?

The HIPAA Privacy Rule applies to health plans, healthcare clearinghouses, and healthcare providers (the Covered Entities) who transmit health information electronically in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA.

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO HIPAA:

DataBank is a trusted Business Associate and service provider to Covered Entities who manage electronic Protected Health Information (e-PHI) or provide services to companies that manage e-PHI in their applications. DataBank performs several annual audits in each data center.

This allows customers subject to the HIPAA Privacy Rule to trust their IT equipment is housed within a top-tier facility that adheres to the most stringent audit requirements in the industry. Our shared risk model and Business Associate Agreement (BAA) allow customers to transfer as much as 80% of HIPAA controls to DataBank to unburden IT teams and make compliance easier.

PCI-DSS

WHAT IS PCI-DSS?

The Payment Card Industry Data Security Standard **(PCI-DSS)** is a set of security controls for optimizing the security of credit, debit, and cash card transactions and to protect cardholders against misuse of personal information. The standard was cooperatively created in 2004 by Discover, American Express, Visa, and MasterCard.

DOES PCI-DSS APPLY TO YOUR ORGANIZATION?

All organizations that store, process, or transmit cardholder data are required to maintain payment security via guidance provided within PCI security standards. These standards determine technical and operational requirements for these entities:

- Organizations accepting or processing payment transactions
- Software developers of applications used in payment transactions
- Manufacturers of devices used in those transactions

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO PCI-DSS:

DataBank provides facilities and critical infrastructure that comply with PCI-DSS. DataBank holds a Qualified Security Assessor (QSA) Report of Compliance (RoC) issued annually to our facilities. The RoC ensures we meet or exceed all audit controls and PCI compliance. Organizations subject to PCI-DSS turn to DataBank to conduct credit card business within secure facilities.

GDPR VS. DATA PRIVACY FRAMEWORK

WHAT IS GDPR?

The European Union (EU) General Data Protection Regulation **(GDPR)** took effect on May 25, 2018. Announced in 2016, the EU gave organizations two years to shore up privacy processes in preparation for the deadline, upon which some of the most robust personal privacy protection laws created would be put into effect. GDPR regulates the storage and processing of personal data relating to individuals in the EU by an individual, a company, or an organization.

WHAT IS THE EU-U.S. DATA PRIVACY FRAMEWORK?

The EU-U.S. Data Privacy Framework is a new agreement that facilitates the transfer of personal data from the European Union to the United States while also ensuring the data is protected in accordance with the high privacy standards required by the European Union. This framework replaces the previous Privacy Shield framework, which was invalidated by the Court of Justice of the European Union (CJEU) in July 2020 due to concerns over the adequacy of U.S. data protection measures, especially in relation to U.S. government surveillance practices. The framework addresses the concerns raised by the CJEU by providing stronger data protection safeguards and enforcement mechanisms.

Key framework elements:

- Enhanced Protections: Introduces enhanced protections for personal data transferred from the EU to the U.S., including stricter obligations on companies handling the data and more robust mechanisms to ensure compliance.
- Government Access Limitations: Limits access to data by U.S. intelligence agencies to what is necessary and proportionate for national security purposes, addressing one of the main concerns of the European Court.
- Redress Mechanisms: Provides EU citizens with improved avenues for redress in cases of data misuse, including a new Data Protection Review Court composed of judges independent of the U.S. government.
- Regular Reviews: Ensures ongoing adequacy by including provisions for regular reviews of the framework's functioning and effectiveness, involving both EU and U.S. authorities.

The development and implementation of the EU-U.S. Data Privacy Framework are critical for companies that rely on transatlantic data flows for their operations. It provides a legal mechanism for transferring personal data from the EU to the U.S. while ensuring compliance with EU data protection laws. The framework is also significant in the broader context of international data transfers and digital trade, highlighting ongoing efforts to reconcile different approaches to privacy and data protection across jurisdictions.

DOES GDPR OR EU-U.S. DATA PRIVACY FRAMEWORK APPLY TO YOUR ORGANIZATION?

The GDPR has specific requirements referencing the transfer of data out of the EU. One of these requirements is that the transfer must only happen to those countries considered to have adequate data protection laws. Currently, GDPR applies to citizens/members of the EU and corporations that directly have a presence within the EU. This is an evolving regulatory mandate.

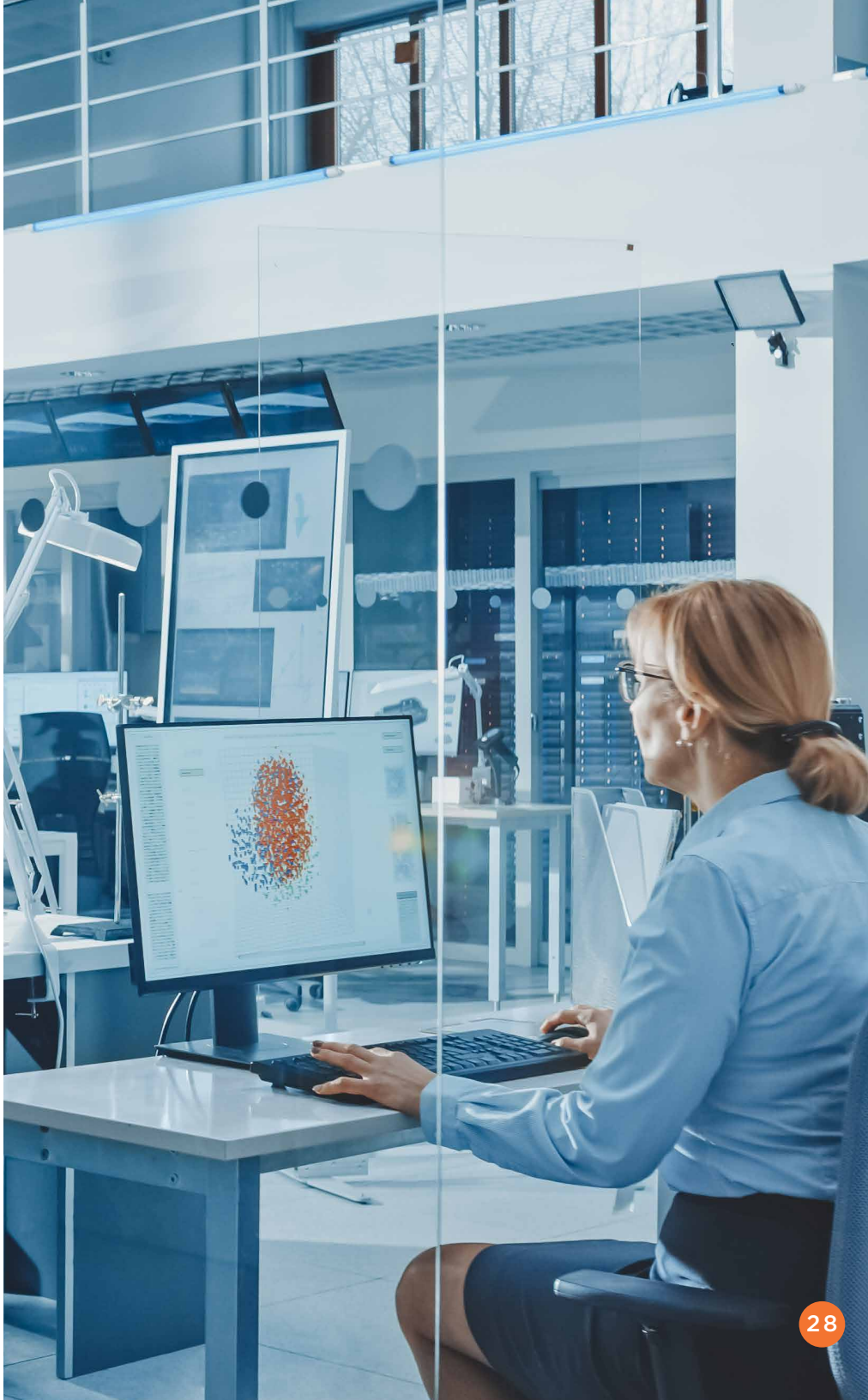
The EU-U.S. Data Privacy Framework is a voluntary program in which participating organizations are deemed as having adequate protection of transatlantic exchanges of personal data for commercial purposes between the European Union and the United States. Currently, the EU-U.S. Data Privacy Framework allows U.S. companies, and EU companies working with U.S. companies, to meet this specific requirement of the General Data Protection Regulation.

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO GDPR:

DataBank demonstrates compliance with regulations, including the GDPR, through SSAE SOC 1 and SOC 2 reporting conducted on an annual basis. The SSAE, through the management attestation and system description section, describes the boundary in which DataBank is responsible for services that may apply to GDPR and how we maintain the security of that boundary. In a typical colocation scenario, DataBank is responsible for physical and environmental security only. All other article compliance is the responsibility of the customer.

DataBank has completed a third-party attested GDPR-readiness assessment that determined DataBank complies with and prepared for articles in the scope of Databank's responsibility. This assessment will be conducted on a routine basis to ensure that results from court challenges to GDPR and other clarifying statements are considered in our determinations. Customers should seek their own legal counsel as to their own compliance status, jurisdiction requirements, and actions that may need to occur.

DataBank has also demonstrated that its customer privacy procedures comply with the EU-U.S. Data Privacy Framework Principles, which cover a range of requirements including notice, choice, accountability for onward transfer, security, data integrity and purpose limitation, access and recourse, enforcement, and liability. As a result, DataBank customers in highly regulated industries—where the company provides compliance architecture and audit support—are assured that their programs comply with these stringent privacy and security safeguards



DATABANK
Data Center Evolved™

www. databank.com
800.840.7533

sales@databank.com