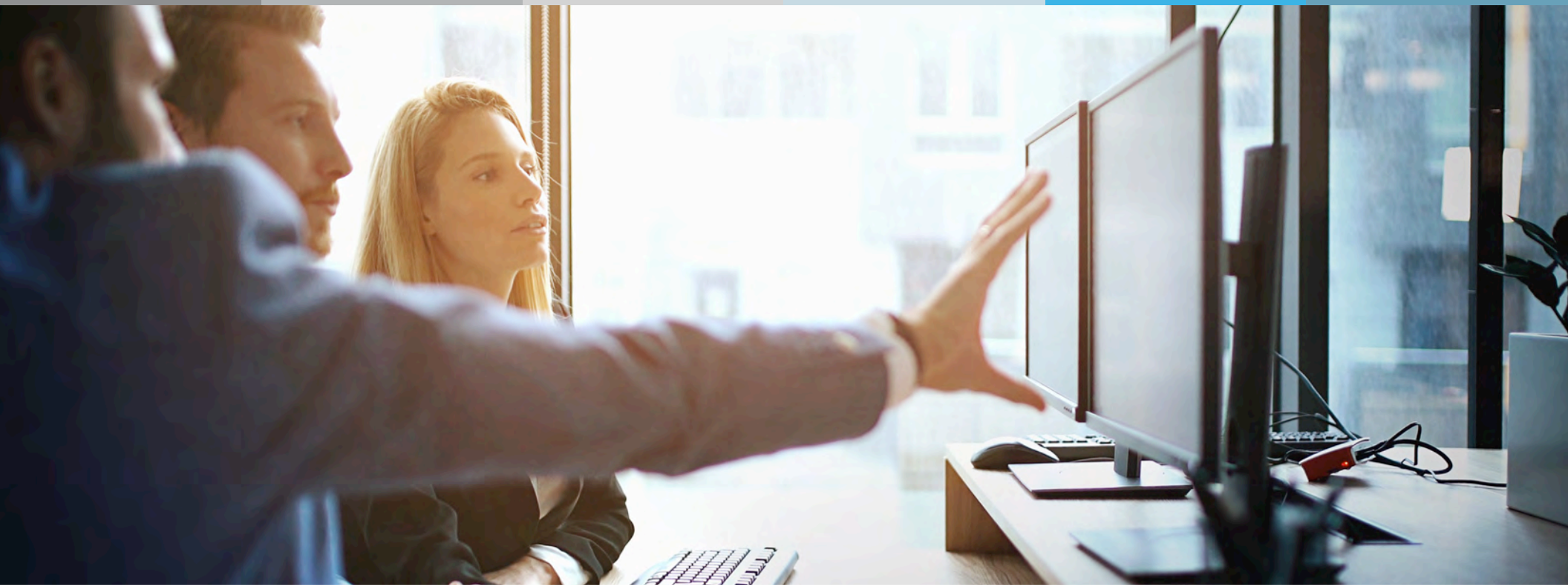
DATABANK
Data Center Evolved™

DATABANK'S GUIDE TO DATA CENTER COMPLIANCE

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

TABLE OF CONTENTS

DATABANK



OVERVIEW

Navigating the complexity and ever-changing nature of compliance is difficult regardless of industry or company size. It's why so many industry-leading clients turn to DataBank to enable security and compliance for their infrastructure platform, applications, and web sites.

As a supplier of secure **FedRAMP, HIPAA/HITECH**, **PCI-DSS**, and **GDPR** compliant data centers, cloud and colocation solutions, we hold an Authority to Operate (ATO) from multiple U.S. Federal Agencies. We support a variety of Federal agencies, healthcare organizations, financial services companies, merchants and SaaS providers, helping them to keep their infrastructure, websites and applications compliant with our Managed Cloud platform and **SSAE 18 SOC 1** and **SOC 2** tested colocation facilities.

But, what do these compliance designations really mean? What is required to be considered "compliant"? And who is responsible for which compliance actions?

This guide will help clarify the designations and the actions that DataBank takes on your behalf to ensure your business meets the requirements for each designation.

FedRAMP

WHAT IS FedRAMP?

The Federal Risk and Authorization Management Program (**FedRAMP**) is a government-wide program designed to empower government agencies to transform their infrastructure and encourage secure cloud adoption. It provides a standardized framework for security assessment, authorization, and continuous monitoring for cloud products and services.[1]

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 exception is private cloud deployments that are designed for single organizations, implemented completely within federal facilities, which then FISMA would be required.

Three key entities are involved with **FedRAMP**: agencies, cloud service providers, 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 on an ongoing basis. Once the assessment is complete an Authority To Operate (ATO) is issued and the real work of deployment and operations begins.

HOW DATABANK SUPPORTS FEDERAL AGENCIES SUBJECT TO FedRAMP

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

The DataBank CloudPlus platform is **FedRAMP** certified as both 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.

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 have trusted partners that know DataBank's platform and will assist customers with writing their portion of the System Security Plan (SSP) and associated supporting documentation as part of professional services engagements.

On an annual basis, DataBank will conduct a Continuous Monitoring (ConMon) assessment with an authorized 3PAO. DataBank's ConMon assessment is conducted between March and June of each year.

SSAE 18

SOC 1, SOC 2, & SOC 3

WHAT IS SSAE 18?

Statement on Standards for Attestation Engagements (**SSAE 18**), is a set of auditing standards published by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA), put in place to continuously redefine and update how service organizations report on compliance.[2]

The **SSAE 18** is used by auditors to report the finding of controls, including security, within organizations such as data centers, internet service providers, and other entities required to establish information security controls.

A SOC 1 Report (System and Organization Controls Report) is a report on controls at a service organization relevant to user entities' internal control over financial reporting.

The purpose of the SOC 2 report is for "management of service organization, user entities and other specified parties" to receive a CPA's opinion on the controls (AICPA).[3] A SOC 2 report will provide three key components:

1. Description of the system
2. Opinion on the fairness of the presentation of the description
3. Description of the service auditors' tests of controls and results

The purpose of a SOC 3 report is to provide "interested parties" (i.e. DataBank's customers) a CPA's opinion about the controls.

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

The difference lies in a couple of key areas, the purpose and components of the report itself. The purpose of the SOC 2 report is for "management of service organization (like DataBank), user entities and other specified parties"[4] to receive a CPA's opinion on the controls. The purpose of a SOC 3 report is to "provide interested parties" an CPA's opinion about the controls. When you look at the statements, there is literally nothing different between the results of the two except the SOC 2 spells out who the interested parties may be (ex: Management, user entities etc.)

The components differences are also slight in words, but mighty in results. A **SOC 2** report will provide three key components, 1) a description of the system, 2) opinion on the fairness of the presentation of the description, and 3) a description of the service auditors tests of controls and results. In a **SOC 3,** only equivalent to the SOC 2 part 2) an opinion on whether the entity maintained effective controls of the system. Parts 1) and 3) are not reported in a SOC 3. However, the details of part 3) are what is important to a DataBank customer because they show what was tested, how it was tested and the results of the testing.

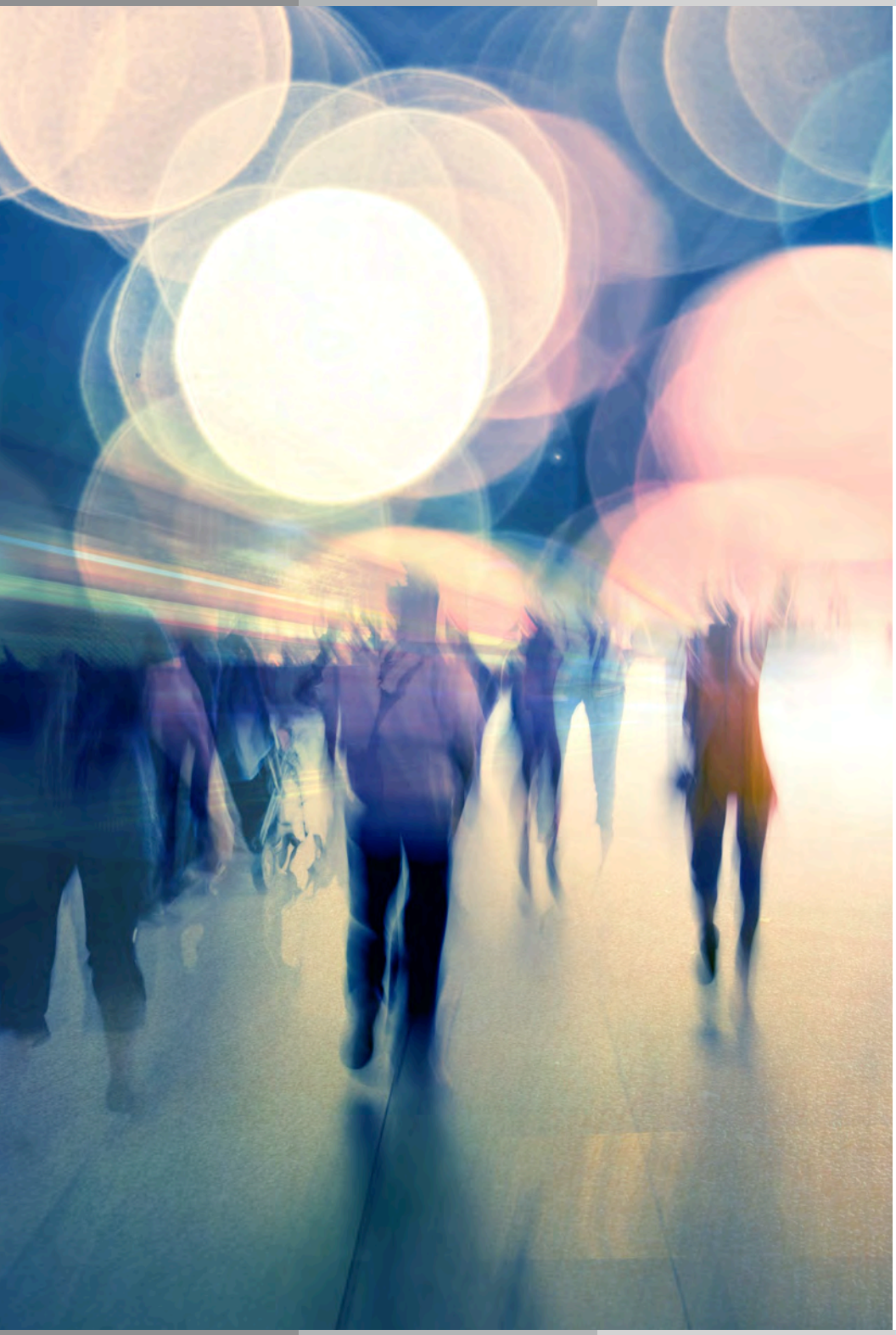
In conclusion, a **SOC 2** report shows everything and then some of a **SOC 3** report. A security evaluation of a vendor should seek the SOC 2 over the SOC 3 report. The SOC 2 report would provide assurance and knowledge of what was tested, how it was tested and the results of each individual testing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

Note: Both **SOC 2** and **SOC 3** reports are based upon 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.

DOES SSAE 18 APPLY TO YOUR ORGANIZATION?

SSAE 18 applies primarily to “service organizations” which are otherwise known as outsourced data centers. They are organizations hired by another entity to process transactions and data, which are usually confidential. Service organizations are considered part of the users’ internal control and typically perform functions such as:

- Accounting
- Benefits
- Billing
- Clearing house
- Collection
- Finance
- Insurance
- Investment
- Information technology (IT)
- Market research
- Payroll



HOW DATABANK SUPPORTS ORGANIZATIONS SEEKING AN SSAE 18 COMPLIANT DATA CENTER:

DataBank commits to performing an annual **SSAE 18 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 of each year. Audits are conducted by an impartial independent third party. Annual reports are published between December 15 and 31 of each year. All reports are available from the DataBank portal on a self-service download basis. DataBank also provides Bridge Letters in the same location.

Note: DataBank does not currently have plans to conduct **SOC 3** testing. SOC 3 compliance can be demonstrated through the **SOC 2** compliance report. Via SOC 2, DataBank has been audited and reported on for the same controls and functions. SOC 2 is more detailed and presents a complete, clear picture of the services provided, the testing conducted against the services, and results.

NIST 800-53R4, NIST 800-171 VS. ISO

WHAT IS ISO?

ISO, or the International Standards Organization, is an international standard-setting body. The ISO is not a government standard, and compliance is voluntary. The ISO standard is designed to assist organizations in keeping assets, both physical and logical, secure.

ISO 27001 is an information security standard published by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). This family of standards is designed to guide organizations in managing security of assets, including intellectual property, financial information, employee information, or private third-party information and provide requirements for an information security management system.[5]

ISO 27002 provides guidelines for organizational information security standards and information security management practices including selection, implementation and management of controls, taking into consideration the information security risk environment(s).[6]

It is designed for organizations that intend to:

1. Select controls within the process of implementing an ISMS based on ISO/IEC 27001
2. Implement commonly accepted information security controls
3. Develop internal information security management guidelines

NIST 800 series

There are several competing standards to the **ISO** series, including the equally relevant National Institute of Standards and Technology (**NIST**) standard. NIST is a non-regulatory agency of the U.S. Federal Government, that operates a physical sciences lab which tests standards prior to publication. Security and IT standards can be found within the 800 series, with the **NIST SP800-53R4** being the current, relevant and comprehensive security control set. This control set, unlike ISO, has three levels of assignment based upon risk, a low, moderate or high. Most systems are categorized as moderate and thus have 325 controls assigned to secure them.

Within **NIST SP800-53R4**, there are 18 control families ranging from access control, awareness and training to supply chain acquisition and physical and environmental controls.

NIST SP800-53R4 is 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 SP800-53R4** Moderate standards for the corporate security baseline and methodology.

NIST SP800-171 is a the collection of controls and requirements that non-Federal computer systems must utilize in order 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 is designed to address several deficiencies in managing and protecting unclassified information to include inconsistent markings, inadequate safeguarding, and needless restrictions, both by standardizing procedures and by providing common definitions through a CUI Registry. The purpose of -171 is to provide federal agencies with recommended security requirements for protecting the confidentiality of CUI when the CUI is resident in a nonfederal system and organization; when the nonfederal 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.

DO ISO 27001/ISO 27002,NIST 800-53R4, 800-171 APPLY TO YOUR ORGANIZATION?

As mentioned, **ISO** is an international non-government affiliated standard-setting body that offers voluntary guidance for information security management and practices. No organization is subject to obligatory compliance because ISO is not a regulatory body and can't issue compliance mandates.

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.

WHY DATABANK IS NIST SP800-53R4 CERTIFIED, RATHER THAN ISO 27001 OR ISO 27002 CERTIFIED:

DataBank is **NIST SP800-53R4** certified with multiple **FedRAMP** Authority to Operate (ATO) designations by the U.S. Federal Government.

DataBank has selected the **NIST SP800-53R4** control methodology because:

1. It is a U.S.-based standard.
2. It is a government regulated and tested standard, rather than a non-aligned organization.
3. It is the basis for U.S. healthcare laws (**HIPAA and HITECH**).
4. DataBank must meet these controls for hosting of federal, state and local government information systems.

HOW DATABANK SUPPORTS ORGANIZATIONS SEEKING A NIST SP800-53R4 DATA CENTER:

DataBank commits to performing an annual, Third Party Assessment Organization (3PAO) continuous monitoring assessment for Data Centers that are **FedRAMP** certified (currently BWI1, DFW3, and MSP2). For those Data Centers not under FedRAMP certification, DataBank conducts annual third party **SSAE18 SOC 1** and **SOC 2**, **HIPAA** and **PCI-DSS** assessments that test the security controls of these facilities. All DataBank facilities and systems use the **NIST SP800-53R4** methodology as their base security methodology. For **FISMA** customers, DataBank works and cooperates with the assigned agency assessor. When a agency needs to send an Assessor for the annual Continuous Monitoring efforts, DataBank requires at least three weeks advance notice to ensure the right persons are present to represent DataBank.

3PAO assessments include the completion of a Security Assessment Report (SAR) that is provided to the **FedRAMP** PMO annually for review. **SSAE18**'s and **HIPAA** reports 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 of each year. Audits are conducted by an impartial independent third party. 3PAO Annual reports are provided to the FedRAMP PMO in early July of each year. SSAE18 and HIPAA annual reports are published between December 15 and 31 of each year. SSAE18 and HIPAA reports are available from the DataBank portal on a self-service download basis. DataBank also provides Bridge Letters in the same location.

ITAR

WHAT IS ITAR?

The International Traffic in Arms Regulation (**ITAR**) is a U.S. Federal law designed to regulate and limit 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 used for accounting of 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 Secretary of State).

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)**, SSAE 18 SOC 1** and **SOC 2**. The FedRAMP ATO is most applicable to an ITAR registered organization. The FedRAMP ATO audit is conducted by a federally authorized 3PAO.

DOES ITAR APPLY TO YOUR ORGANIZATION?

ITAR compliance is required for organizations that "engage in the United States in the business of manufacturing or exporting or temporarily importing defense articles, or furnishing defense services."[6] Defense Services are further defined in e-CFR Title 22, Chapter I, Subchapter M, Part 120.9.[7] The "Munitions List" is specific as to the items that are controlled under ITAR.[8]

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

Note: ITAR requires a registration process for organizations with products that fall within the ITAR "Munitions List." There is not an ITAR certification that can be obtained by a manufacturer or service provider of a manufacturer of munitions.

HIPAA

WHAT IS 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.[9]

The HIPAA Privacy Rule requires healthcare providers and 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 who transmit health information in electronic form in connection with transactions for which the Secretary of HHS has adopted standards under HIPAA (the "covered entities").[10]

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. Customers subject to the **HIPAA** Privacy Rule can trust their IT equipment is housed within a top-tier facility adhering to the most stringent audit requirements in the industry. Our shared risk model and BAA allows 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 designed to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of personal information. The standard was created in 2004 cooperatively by Discover, American Express, Visa, and MasterCard.[11]

DOES PCI-DSS APPLY TO YOUR ORGANIZATION?

All organizations who 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:

- Organizations accepting or processing payment transactions
- Software developers of applications used in payment transactions
- Manufacturers of devices used in those transactions[12]

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO PCI-DSS:

DataBank provides the facility and critical infrastructure which complies with **PCI-DSS**. DataBank holds a Qualified Security Assessor (QSA) Report of Compliance (ROC) that is 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. PRIVACY SHIELD

WHAT IS GDPR?

The European Union's (EU's) 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 of 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.[13]

Privacy Shield was designed by the U.S. Department of Commerce and the European Commission to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union and Switzerland to the United States in support of transatlantic commerce.

DOES GDPR OR PRIVACY SHIELD 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 as having adequate data protection laws. Currently, GDPR applies to citizens/members of and corporations that directly have a presence within the EU. This is an evolving regulatory mandate.

Privacy Shield 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, Privacy Shield allows U.S. companies, or EU companies working with U.S. companies, to meet this specific requirement of the General Data Protection

HOW DATABANK SUPPORTS ORGANIZATIONS SUBJECT TO GDPR:

DataBank demonstrates compliance with regulations, including the **GDPR**, through the **SSAE 18 SOC 1** and **SOC 2** reporting conducted on an annual basis. The SSAE18, through the management attestation and system description section, describes the boundary in which DataBank is responsible for services that may apply to the GDPR regulations 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 which determined that DataBank complies with and prepared for articles in 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 demonstrated that its customer privacy procedures comply with the **Privacy Shield** 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.

REFERENCES

1. https://www.fedramp.gov/faqs/
2. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/comparision-soc-1-3.pdf
3. https://searchcloudsecurity.techtarget.com/definition/SSAE-16
4. https://www.aicpa.org/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/comparision-soc-1-3.pdf
5. https://www.iso.org/isoiec-27001-information-security.html
6. https://www.iso.org/standard/54533.html
7. E-CFR Title 22, chapter I, subchapter M part 122.1 – Registration Requirements
8. E-CFR Title 22, chapter I, subchapter M part 120.9 – Registration Requirements
9. E-CFR Title 22, chapter I, subchapter M part 121 – Registration Requirements
10. https://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.00WhatisHIPAA.aspx
11. https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html
12. https://searchfinancialsecurity.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard
13. https://www.pcisecuritystandards.org/

DATABANK
Data Center Evolved™

www. databank.com
800.840.7533

sales@databank.com