# Security and Compliance Audits

**IT Security and Regulatory Compliance** is critical for every organization. With various regulatory agencies establishing standards and issuing mandates for adherence, it is vital to know where your sensitive information is at risk of being compromised - and how to address gaps in compliance requirements.

MIS Sciences Corporation, trusted by leading government agencies, performs audits that meet multiple industry compliance requirements. Data centers, infrastructure, processes and methodology - all can be assessed by MIS specialists who have expertise and experience in auditing procedures and documentation.

Audits and gap analysis can be performed on site, remotely, or both. MIS provides analysis, recommendations and mitigation strategies, in addition to audit results.

NIST 800-53 rev4 - Recommended Security Controls for Federal Information Systems and Organizations is the framework used for providing gap analysis on all systems, from point of entry to the keyboard, including:

- Network infrastructure and related appliances
- Servers and related components
- Desktop and related components
- Policies and procedures

**About MIS Sciences Corporation**

Since 1996, MIS Sciences Corporation has been delivering comprehensive technology, colocation, and hosting services for enterprise and government customers of all sizes, from startups and Fortune 500 companies to Government agencies. MIS Sciences provides managed services and hosting, development and application management services, disaster recovery, and electronic vaulting; in geographically dispersed data centers for redundancy options and risk mitigation.

MIS Sciences is a full service IT Schedule 70 Contractor authorized to provide services under SIN 132-51, SIN 132-52 and Cloud SIN 132-40.

# Security and Compliance Audits

## ● Key Acts and Regulations include:

| | |
|---|---|
| FISMA | Federal Information Security Management Act of 2002, mandating that all federal agencies develop and maintain methods of securing information systems. FISMA directs the National Institute of Standards and Technologies (NIST) to create, issue and manage compliance standards. |
| PCI DSS | The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard used by organizations that handle card payments and card holders' information. Developed and implemented by the Payment Card Industry Security Standards Council global forum, PCI DSS aims to prevent and reduce card fraud. |
| GLBA | Gramm-Leach-Bliley Act (GLBA) governs the treatment of nonpublic personal information about consumers by financial institutions. A key part is the Safeguards Rule, which requires all financial institutions to design, implement and maintain safeguards to protect customer information. |
| SOX | Sarbanes Oxley Act regulates safeguarding of company financial records. Auditable internal controls and procedures are to be in place to ensure reporting accuracy and prevent fraudulent financial activity. |
| HIPAA | Health Insurance Portability and Accountability Act. Title II is a directive to shift to electronic data as well as protect the privacy of patients. |

## ● Relevant Standards, Controls and Guides include:

| | |
|---|---|
| NIST SP 800-53 | NIST 800-53 is a publication that recommends security controls for federal information systems and organizations and documents security controls for all federal information systems, except those designed for national security. |
| NIST FIPS 200 | FIPS 200 - Minimum Security Requirements for Federal Information and Federal Information Systems is a mandatory federal standard established in response to FISMA. FIPS 200, in combination with NIST Special Publication 800-53, ensure that appropriate security requirements and security controls are applied to all federal information and information systems. |
| DISA STIGs | Security Technical Implementation Guides represent a methodology for standardized configuration of computing systems issued by the Defense Information Systems Agency to maximize security. |
| NERC CIP-007 | North American Electric Reliability Corporation, an international regulatory authority to assure the reliability of the bulk power system. CIP-007 relates to security of critical and non-critical Cyber Assets under Critical Infrastructure Protection requirements. |
| AICPA SSAE 16 | American Institute of CPAs Service Organization Controls (SOC) reports are designed to assess service delivery processes and controls for organizations that operate information systems and provide information system services. |

**Corporate Office**
2550 North Hollywood Way
Suite 404
Burbank, CA 91505
1.818.847.0213
info@mis-sciences.com

**Federal Services Office**
1655 North Fort Myer Drive
Suite 700
Arlington, VA 22209
1.703.351.3366
fedinfo@mis-sciences.com

**Las Vegas Office**
322 Karen Ave
Suite 1407
Las Vegas, NV 89109
1.725.502.3755
lvinfo@mis-sciences.co