AMERICAN
TECHNOLOGY
SERVICES

Compliance Handbook

Security and Integrity with ATS

FAIRFAX

2751 Prosperity Ave
Suite 600
Fairfax, VA 22031

NEW YORK

250 Broadway
Suite 610
New York, NY 10007

ATLANTA

4360 Chamblee
Dunwoody Rd, Suite
517 Atlanta, GA 30341

CONTACT

+1 888 876 0302
info@networkats.com
networkats.com

Navigating Compliance

Compliance is not just a legal obligation but a critical element in protecting sensitive data, maintaining operational integrity, and adhering to regulatory requirements. For organizations across most sectors—healthcare, retail, finance, defense, and beyond—meeting compliance standards is fundamental to trust and security. It's necessary, and we're here to help you meet it.

American Technology Services (ATS) provides comprehensive IT compliance services. Our expertise spans multiple regulatory frameworks and industry-specific requirements, ensuring our clients are informed and protected against potential risks and vulnerabilities. We will guide you through the complexities of IT security compliance, HIPAA for healthcare, PCI DSS for businesses handling credit card information, CMMC and NIST 800-171 for Department of Defense contractors, and more.

If you're seeking to grasp the fundamentals of compliance, design a compliance program, or prepare for an audit, ATS provides the insights and proven strategies you need to confidently and clearly navigate the complex landscape of IT compliance.

Understanding IT Security Compliance

IT security compliance is an aspect of organizational risk management that involves following regulatory requirements and industry standards to protect data and systems. It focuses on maintaining the confidentiality, integrity, and availability of information. Proper compliance helps organizations avoid legal penalties, financial losses, and reputation damage.

Components of IT Security Compliance

Penetration Testing

This proactive measure involves simulated cyberattacks by ethical hackers. These controlled tests identify vulnerabilities in an organization's IT infrastructure, offering insights into potential security weaknesses. By uncovering these issues early, organizations can strengthen their cyber defenses and reduce risks.

Vulnerability Assessments

These systematic examinations of IT systems detect a wide range of vulnerabilities. Security professionals use automated tools and manual techniques to identify software, hardware, and network configuration weaknesses. Vulnerability assessments also prioritize issues based on their potential impact, allowing organizations to address the most pressing concerns first.

Security Policy Management

Developing and enforcing security policies is fundamental to any compliance program. These policies establish guidelines for IT resource use, data handling, access controls, and incident response. Consistent security practices across the organization create a culture of security awareness among employees.

Understanding IT Security Compliance

IT Security Compliance Relevance

IT security compliance varies across industries, each with its own regulatory landscape and security challenges. Health Insurance Portability and Accountability Act (HIPAA) is highly important in healthcare compliance. HIPAA regulations require strict protections for patient information, mandating healthcare providers and their associates to implement strong security measures for electronic protected health information (ePHI).

Organizations handling credit card information must comply with the Payment Card Industry Data Security Standard (PCI DSS). This standard, established by major credit card companies, outlines requirements for securing payment card information throughout its lifecycle.

Cybersecurity Maturity Model Certification (CMMC) and NIST Special Publication 800-171 are essential in defense. These frameworks secure sensitive defense information and set cybersecurity requirements for Department of Defense contractors.

ATS IT Security Compliance Services

1. Vulnerability Assessments and Penetration Testing (VAPT)

ATS conducts regular tests to identify and address risks proactively, simulating real-world attack scenarios.

2. Continuous Security Monitoring (CSM)

ATS helps organizations maintain an up-to-date understanding of their security posture through ongoing monitoring and assessment.

3. Security Policy Management

ATS develops and manages customized security policies aligned with specific operational needs and compliance requirements.

Understanding IT Security Compliance

Benefits of IT Security Compliance

Better Data Protection

Following stringent security standards reduces the risk of unauthorized access and data breaches.

Meeting Regulatory Requirements

Compliance helps organizations adhere to legal and industry standards, avoiding potential fines and legal issues.

Improved Reputation

A solid compliance stance builds client, partner, and stakeholder trust.

Increased Efficiency

While initially demanding, compliance streamlines security processes, reducing the likelihood of costly incidents and improving operations.

IT security compliance is an essential part of modern business operations. By implementing thorough compliance measures, organizations can protect their assets, meet regulatory requirements, and build trust that supports long-term growth.

HIPAA Compliance for Healthcare Organizations

The Health Insurance Portability and Accountability Act (HIPAA) is a cornerstone of patient privacy and data security in the United States healthcare system. This section explores HIPAA's key aspects and its significance for healthcare organizations.

What is HIPAA?

HIPAA, enacted in 1996, sets national standards for protecting sensitive patient information. It requires healthcare providers, health plans, and healthcare clearinghouses to implement strong safeguards for patient data confidentiality, integrity, and availability.

Key Provisions of HIPAA

Privacy Rule

This rule protects individuals' medical records and other personal health information. It sets limits on the use and disclosure of health information without patient authorization. The Privacy Rule gives patients rights over their health information, including the right to examine and obtain a copy of their health records and to request corrections.

Security Rule

The Security Rule focuses on electronic protected health information (ePHI) and mandates appropriate administrative, physical, and technical safeguards to protect its confidentiality, integrity, and security. This includes measures such as access controls, encryption, and audit trails.

Breach Notification Rule

This rule requires covered entities and their business associates to notify patients, the U.S. Department of Health and Human Services (HHS), and, in some cases, the media, following a breach of unsecured protected health information. It defines specific timeframes and methods for notification, helping to mitigate potential harm from data breaches.

HIPAA Compliance for Healthcare Organizations

Benefits of HIPAA Compliance

Adhering to HIPAA regulations offers several advantages for healthcare organizations.

Protection of Patient Information

HIPAA compliance significantly reduces the risk of unauthorized access, use, or disclosure of sensitive health information. This protection extends to both physical and electronic records, safeguarding patients' privacy and maintaining their trust in the healthcare system.

Legal and Regulatory Adherence

By complying with HIPAA, healthcare organizations meet federal requirements and avoid potential fines and penalties. The Office for Civil Rights (OCR) can impose substantial fines for HIPAA violations, ranging from $100 to $50,000 per violation (or per record), with a maximum penalty of $1.5 million per year for each violation.

Trust and Credibility

Demonstrating a commitment to data protection through HIPAA compliance builds trust with patients, partners, and the wider community. In an age where data breaches are increasingly common, a strong track record of protecting patient information can be a significant differentiator for healthcare providers.

Operational Efficiency

While achieving HIPAA compliance requires initial investment and ongoing effort, it often leads to improved operational efficiency in the long run. By streamlining data management processes and implementing strong security measures, healthcare organizations can reduce the risk of costly data breaches and improve overall information management.

HIPAA compliance is not a one-time achievement but an ongoing process that requires continuous attention and adaptation. As technology evolves and new threats emerge, healthcare organizations must regularly review and update their HIPAA compliance strategies to avoid potential risks.

For many healthcare organizations, partnering with experienced IT security firms like ATS can be invaluable in navigating the complexities of HIPAA compliance. ATS' expertise in healthcare IT security can help organizations implement effective compliance strategies, conduct regular risk assessments, and stay up to date with evolving HIPAA requirements.

PCI DSS Compliance for Businesses Handling Credit Card Information

The Payment Card Industry Data Security Standard (PCI DSS) plays a crucial role in safeguarding credit card information and preventing fraud. This chapter examines PCI DSS, its key requirements, and the benefits of compliance for businesses that handle payment card data.

What is PCI DSS?

PCI DSS is a set of security standards designed to protect credit card information during transactions. Developed by the Payment Card Industry Security Standards Council (PCI SSC), these standards apply to all companies that accept, process, store, or transmit credit card information. PCI DSS aims to create a secure environment for payment card transactions, reducing the risk of data breaches and fraud.

Key Requirements of PCI DSS

PCI DSS outlines six primary objectives, each with specific requirements:

1. **Build and Maintain a Secure Network and Systems**
   - Install and maintain firewalls to protect cardholder data
   - Replace vendor-supplied default passwords and security settings

2. **Protect Cardholder Data**
   - Secure stored cardholder data
   - Encrypt cardholder data transmitted across public networks

3. **Maintain a Vulnerability Management Program**
   - Use and regularly update anti-virus software
   - Develop and maintain secure systems and applications

4. **Implement Strong Access Control Measures**
   - Limit access to cardholder data on a need-to-know basis
   - Identify and authenticate access to system components
   - Restrict physical access to cardholder data

5. **Regularly Monitor and Test Networks**
   - Track and monitor all access to network resources and cardholder data
   - Regularly test security systems and processes

6. **Maintain an Information Security Policy**
   - Establish a policy addressing information security for all personnel

PCI DSS Compliance for Businesses Handling Credit Card Information

Benefits of PCI DSS Compliance

Enhanced Security

PCI DSS compliance significantly reduces the risk of data breaches and credit card fraud. By implementing strong security measures, businesses can protect sensitive payment information from unauthorized access and use.

Regulatory Adherence

Compliance with PCI DSS helps businesses meet industry standards and avoid potential fines and penalties. Payment card companies may impose hefty fines on non-compliant businesses, especially in the event of a data breach.

Customer Trust

When customers know their payment information is secure, they're more likely to trust and continue doing business with a company. PCI DSS compliance demonstrates a commitment to protecting customer data, which can be a powerful differentiator in competitive markets.

Operational Efficiency

While achieving PCI DSS compliance requires effort, it often leads to improved operational efficiency. By streamlining security processes and implementing best practices, businesses can reduce the risk of costly data breaches and improve overall data management. PCI DSS compliance is an ongoing process that requires regular assessment and updates. As cyber threats evolve, businesses must stay vigilant and adapt their security measures accordingly.

For many organizations, particularly small to medium-sized businesses, achieving and maintaining PCI DSS compliance can be challenging. This is where partnering with experienced IT security firms like ATS can be valuable. ATS' expertise in payment card security can help businesses implement effective compliance strategies, conduct regular assessments, and stay current with evolving PCI DSS requirements.

CMMC and NIST 800-171 Compliance for DoD Contractors

This section explores the Cybersecurity Maturity Model Certification (CMMC) and NIST Special Publication 800-171, two crucial frameworks for protecting sensitive information in the defense industry.

What are CMMC and NIST 800-171?

The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across the Defense Industrial Base (DIB). Its primary goal is to protect controlled unclassified information (CUI) within the defense supply chain. CMMC builds upon existing regulations, including NIST Special Publication 800-171, which provides guidelines for protecting CUI in non-federal systems and organizations.

Key Components of CMMC

CMMC is structured around five maturity levels, each representing increasing cybersecurity sophistication:

1. Basic Cyber Hygiene
2. Intermediate Cyber Hygiene
3. Good Cyber Hygiene
4. Proactive
5. Advanced/Progressive

These levels encompass 17 domains, including:

- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

Each domain contains specific practices and processes that organizations must implement to achieve certification at a given level.

CMMC and NIST 800-171 Compliance for DoD Contractors

Key Components of NIST 800-171

NIST 800-171 focuses on 14 key areas of cybersecurity:

- **Access Control:** Limiting system access to authorized users.
- **Awareness and Training:** Educating personnel about security risks and responsibilities.
- **Audit and Accountability:** Creating and protecting audit records
- **Configuration Management:** Establishing and enforcing security configurations.
- **Identification and Authentication:** Verifying identities before granting access.
- **Incident Response:** Establishing operational incident-handling capabilities.
- **Maintenance:** Performing secure system maintenance.
- **Media Protection:** Safeguarding information stored on media.
- **Personnel Security:** Screening and monitoring individuals with system access.
- **Physical Protection:** Limiting physical access to information systems.
- **Risk Assessment:** Assessing and managing risk.
- **Security Assessment:** Conducting periodic compliance assessments.
- **System and Communications Protection:** Monitoring and controlling communications.
- **System and Information Integrity:** Protecting system integrity.

CMMC and NIST 800-171 Compliance for DoD Contractors

Benefits of CMMC and NIST 800-171 Compliance

Adhering to CMMC and NIST 800-171 standards offers several advantages.

Enhanced Security

These frameworks help protect sensitive defense-related information from unauthorized access and cyber threats. By implementing comprehensive security measures, organizations can significantly reduce the risk of data breaches and cyberattacks.

Regulatory Adherence

Compliance with CMMC and NIST 800-171 is essential for meeting Department of Defense requirements. This compliance is often a prerequisite for bidding on and winning defense contracts, making it crucial for businesses in the defense sector.

Competitive Advantage

Achieving CMMC certification demonstrates a strong commitment to cybersecurity. This can enhance an organization's reputation and build trust with clients and partners in the defense industry, potentially leading to more contract opportunities.

Operational Efficiency

While implementing these standards requires initial investment, it often results in improved operational efficiency. Organizations can avoid costly incidents and potential contract losses due to non-compliance by streamlining security processes and reducing the risk of data breaches.

For many defense contractors, especially smaller businesses, achieving and maintaining compliance with CMMC and NIST 800-171 can be challenging. This is where partnering with experienced IT security firms like ATS can be invaluable. ATS' expertise in defense sector cybersecurity can help contractors implement effective compliance strategies, conduct regular assessments, and stay up-to-date with evolving requirements.

Developing and Managing Compliance Programs

This chapter focuses on the essential elements of creating and maintaining effective compliance programs. We'll explore the importance of clear policies and procedures, strategies for customization, and the benefits of well-managed compliance initiatives.

Establishing Policies and Procedures

Clear policies and procedures form the backbone of any successful compliance program. They provide a framework for maintaining compliance and help organizations:

- Set expectations for employee behavior
- Define processes for handling sensitive information
- Outline steps for responding to security incidents
- Establish guidelines for using and maintaining IT systems

Creating Customized Policies

Effective compliance policies must be tailored to specific regulatory requirements and reflect each organization's unique needs and risks. When developing policies:

- Start with a thorough understanding of relevant regulations (e.g., HIPAA, PCI DSS, CMMC)
- Assess your organization's specific risks and vulnerabilities
- Involve key stakeholders from various departments in the policy development process
- Use clear, concise language that all employees easily understand
- Include practical examples and scenarios to illustrate policy application

Implementation and Enforcement

Creating policies is only the first step. Successful compliance programs require effective implementation and consistent enforcement.

- Assign responsibility for compliance to specific individuals or teams
- Develop clear procedures for enforcing policies and handling violations
- Provide regular training to employees on compliance policies and procedures
- Conduct periodic audits to ensure adherence to policies
- Regularly review and update policies to reflect changes in regulations and business operations

Developing and Managing Compliance Programs

Benefits of a Well-Managed Compliance Program

A well-designed and properly managed compliance program offers numerous advantages.

Enhanced Security and Risk Management

Organizations can reduce their exposure to security threats and compliance violations by systematically identifying and addressing potential vulnerabilities.

Regulatory Adherence

A robust compliance program helps organizations stay current with relevant regulations, reducing the risk of penalties and legal issues.

Operational Efficiency

Streamlined compliance processes can improve operational efficiency, reduce redundancies, and minimize the likelihood of costly mistakes or violations.

Employee Engagement

When employees understand the importance of compliance and their role in maintaining it, they're more likely to participate actively in security efforts. This creates a culture of compliance that extends beyond mere rule-following.

Reputation and Trust

A strong commitment to compliance can enhance an organization's reputation among clients, partners, and regulators. This can lead to increased trust, potentially opening up new business opportunities.

Developing and managing an effective compliance program is an ongoing process that requires dedication and resources. For many organizations, particularly those dealing with complex regulatory environments, partnering with experienced IT security firms like ATS can be invaluable.

ATS can assist in developing customized compliance programs, conducting risk assessments, and providing ongoing support to maintain compliance. Our deep expertise helps organizations navigate the complexities of various regulatory frameworks while aligning compliance efforts with broader business objectives.

Audit and Assessment Services

This section explores the critical role of audit and assessment services in maintaining regulatory compliance. We'll discuss strategies for preparing for regulatory inspections, conducting gap analyses, and addressing post-audit remediation efforts.

Preparing for Regulatory Inspections

Regulatory inspections are crucial for verifying that organizations adhere to relevant laws and standards. Proper preparation can help avoid penalties, fines, and operational disruptions.

Mock Audits

- Simulate real regulatory inspections to identify potential non-compliance areas
- Provide detailed feedback and recommendations for improvement
- Develop strategies to address identified issues before actual inspections

Preparation Strategies

- Update and organize all relevant documentation and records
- Train staff on inspection procedures and their roles during audits
- Review and update policies and procedures to align with current regulations

Audit and Assessment Services

Conducting Gap Analyses

Gap analyses help organizations identify discrepancies between their current practices and regulatory requirements, providing a roadmap for achieving compliance.

Process of Conducting Gap Analyses

1. **Initial Assessment:** Evaluate the organization's current compliance status
2. **Identify Gaps:** Compare existing practices with regulatory standards
3. **Actionable Recommendations:** Provide detailed suggestions to address identified gaps, prioritized by risk and impact business objectives.

Continuous Improvement

- Regularly conduct gap analyses to maintain compliance
- Adapt to changes in regulations and business operations

Audit and Assessment Services

Assisting with Remediation Efforts Post-Audit or Enforcement Action

Post-Audit Remediation

- Review findings from audits and regulatory inspections
- Develop and implement a remediation plan to address identified issues
- Monitor progress to ensure timely completion of corrective actions

Enforcement Action Response

- Analyze the reasons for enforcement actions and their implications
- Create and implement a response plan to address raised issues
- Maintain thorough documentation of remediation efforts
- Provide regular reports to regulators and stakeholders

Benefits of Audit and Assessment Services

- Proactive Compliance Management: Identify and address compliance issues early
- Improved Risk Management: Reduce the risk of penalties and operational disruptions
- Enhanced Operational Efficiency: Streamline compliance processes
- Increased Confidence and Trust: Demonstrate commitment to compliance
- Continuous Improvement: Support ongoing compliance and operational excellence

---

Partnering with experienced firms like ATS for audit and assessment services can be invaluable for many organizations, especially those in highly regulated industries. ATS' expertise can help organizations navigate complex regulatory landscapes, conduct thorough audits and assessments, and implement effective remediation strategies.

Conclusion

We have explored the critical aspects of IT compliance and how ATS supports organizations in navigating these complex requirements. We've covered a range of topics, from the basics of IT security compliance to sector-specific regulations and practical strategies for maintaining compliance.

Recap of Key Points

IT Security Compliance

We discussed the importance of penetration testing, vulnerability assessments, and security policy management in maintaining a strong security posture.

HIPAA Compliance

For healthcare organizations, we outlined strategies to protect patient information through risk assessments, policy development, and staff training.

PCI DSS Compliance

We explored methods for protecting payment card information, including gap analyses, security assessments, and compliance reporting.

CMMC and NIST 800-171 Compliance

For defense contractors, we discussed approaches to secure sensitive information through compliance program development, risk assessments, and continuous monitoring.

Developing and Managing Compliance Programs

We covered the establishment of clear policies and procedures, conducting risk assessments, ongoing monitoring, and employee training.

Audit and Assessment Services

We examined strategies for preparing for regulatory inspections, conducting gap analyses, and assisting with post-audit remediation efforts.

Conclusion

Next Steps for Organizations

Achieving and maintaining compliance is an ongoing process that requires continuous attention. Here are the next steps organizations should consider:

Engage with ATS for a Comprehensive Assessment

Begin with an initial consultation to evaluate your current compliance status and define the scope of required services.

Develop a Customized Compliance Program

Work with ATS to create tailored policies and procedures that meet your specific regulatory requirements.

Implement and Monitor Security Measures

Conduct risk assessments, vulnerability scans, and penetration tests to identify and address potential threats.

Train and Educate Employees

Ensure all staff members understand their roles in maintaining compliance through ongoing training and awareness programs.

Prepare for and Respond to Audits

Utilize ATS's audit and assessment services to prepare for regulatory inspections and respond effectively to any findings or enforcement actions.

By taking these steps, organizations can build a modern compliance program that meets regulatory requirements and enhances overall security and operational efficiency.

For further information and to discuss how ATS can support your compliance needs, please get in touch with us at info@networkats.com. Our team is prepared to guide you through the intricacies of IT compliance, helping you establish a secure and operationally excellent IT environment.

Appendices

Glossary of Compliance Terms

This glossary defines key terms and concepts used throughout this eBook on IT compliance. It serves as a quick reference to help readers understand the technical language and industry-specific terminology. Terms are organized alphabetically within categories for easy navigation. Cross-references to relevant chapters are provided where applicable.

Regulations and Standards

CMMC (Cybersecurity Maturity Model Certification): A unified standard for implementing cybersecurity across the Defense Industrial Base (DIB) to protect controlled unclassified information (CUI).

HIPAA (Health Insurance Portability and Accountability Act): A U.S. law designed to provide privacy standards to protect patients' medical records and other health information provided to health plans, doctors, hospitals, and other healthcare providers.

NIST 800-171: A set of guidelines designed to protect controlled unclassified information (CUI) in non-federal systems and organizations.

PCI DSS (Payment Card Industry Data Security Standard): A set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment.

Compliance Processes

Audit: A systematic evaluation of an organization's adherence to regulatory guidelines, standards, or contractual obligations.

Compliance: Adherence to laws, regulations, guidelines, and specifications relevant to an organization's business processes.

Gap Analysis: A method of assessing the differences in performance between a business's information systems or software applications to determine whether business requirements are being met and, if not, what steps should be taken to ensure they are met successfully.

Internal Audit: An organizational self-review of processes, procedures, and operations to ensure compliance and identify improvement areas.

Mock Audit: A simulated audit conducted to prepare an organization for a real audit, identifying potential areas of non-compliance and providing feedback for improvement.

Risk Assessment: The process of identifying, evaluating, and estimating the levels of risk involved in a situation, followed by the identification of appropriate measures to control and mitigate the impact of the risk.

Appendices

Technical Concepts

Access Control: The process of granting or denying specific requests to obtain and use information and related information processing services.

Data Breach: An incident where information is stolen or taken from a system without the knowledge or authorization of the system's owner.

Incident Response: A structured methodology for handling security incidents, breaches, and cyber threats.

Penetration Testing: An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system.

Security Policy Management: The process of creating, implementing, and maintaining a set of policies and procedures to manage and protect an organization's information security.

Threat Modeling: A process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized.

Vulnerability Assessment: The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.

Specific Compliance Terms

Breach Notification Rule: A requirement under HIPAA that mandates covered entities to notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media of a breach of unsecured protected health information.

CUI (Controlled Unclassified Information): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies.

ePHI (Electronic Protected Health Information): Protected health information that is created, stored, transmitted, or received electronically.

Compliance Checklists

Compliance Program Development Checklist

☐ **Initial Steps**

- Conduct an initial risk assessment to understand the current security posture.
- Define the scope of the compliance program based on regulatory requirements.
- Identify key stakeholders and assign roles and responsibilities.

☐ **Policy and Procedure Development**

- Develop and document policies that align with regulatory requirements.
- Create procedures to enforce policies consistently across the organization.
- Establish a process for regular review and updating of policies and procedures.

☐ **Risk Assessment and Management**

- Conduct a comprehensive risk assessment.
- Identify and document vulnerabilities and threats.
- Prioritize risks based on their potential impact.
- Develop and implement mitigation strategies for identified risks.

☐ **Employee Training and Education**

- Design initial training programs for new employees.
- Schedule regular refresher training sessions.
- Create role-specific training modules.
- Develop awareness campaigns to keep employees informed about compliance updates.

☐ **Ongoing Monitoring and Reporting**

- Implement continuous monitoring tools.
- Establish regular internal audit schedules.
- Develop automated reporting systems.
- Create a compliance dashboard for real-time monitoring.

☐ **Audit and Assessment Preparation**

- Schedule and conduct mock audits.
- Prepare and organize all necessary documentation.
- Develop a plan to address any findings from mock audits.

Compliance Checklists

HIPAA Compliance Checklist

☐ **Initial Assessment**

- Conduct an initial HIPAA risk assessment.
- Identify all ePHI data sources.
- Document current security measures.

☐ **Policies and Procedures**

- Develop HIPAA-compliant policies and procedures.
- Implement access control measures.
- Establish procedures for data encryption and secure transmission.
- Create incident response plans.

☐ **Training and Awareness**

- Conduct initial HIPAA training for all employees.
- Schedule regular refresher training.
- Distribute HIPAA compliance materials and updates.

☐ **Technical Safeguards**

- Implement encryption for ePHI.
- Install and maintain firewalls.
- Use secure methods for data transmission.
- Regularly update antivirus software.

☐ **Monitoring and Reporting**

- Implement continuous monitoring for HIPAA compliance.
- Conduct regular internal audits.
- Prepare and maintain detailed documentation.
- Develop a breach notification procedure.

Compliance Checklists

PCI DSS Compliance Checklist

☐ **Scoping and Initial Assessment**

- Define the scope of the PCI DSS compliance effort.
- Identify all locations where cardholder data is stored, processed, or transmitted.
- Conduct an initial gap analysis.

☐ **Security Measures**

- Install and maintain a firewall configuration.
- Change default system passwords and settings.
- Protect stored cardholder data.
- Encrypt cardholder data transmissions.
- Use and regularly update antivirus software.

☐ **Access Control**

- Restrict access to cardholder data to those who need to know.
- Assign unique IDs to each person with computer access.
- Restrict physical access to cardholder data.

☐ **Monitoring and Testing**

- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain an information security policy.

☐ **Documentation and Reporting**

- Prepare required documentation for PCI DSS compliance.
- Complete Self-Assessment Questionnaires (SAQs) as needed.
- Submit Reports on Compliance (RoCs) if required.

Compliance Checklists

CMMC and NIST 800-171 Compliance Checklist

☐ **Initial Steps**

- Conduct a preliminary risk assessment.
- Define the scope of the compliance effort.
- Identify all systems and data subject to CMMC and NIST 800-171 requirements.

☐ **Policy and Procedure Development**

- Develop policies for access control, incident response, and system maintenance.
- Establish procedures for secure handling of CUI.
- Create and document incident response plans.

☐ **Implementation of Security Controls**

- Implement access control measures.
- Encrypt data in transit and at rest.
- Install and maintain firewalls and intrusion detection systems.
- Apply multi-factor authentication for system access.

☐ **Employee Training and Awareness**

- Conduct initial training on CMMC and NIST 800-171 requirements.
- Provide ongoing training and awareness programs.
- Develop materials and resources to support continuous learning.

☐ **Monitoring and Continuous Improvement**

- Implement continuous monitoring tools.
- Conduct regular audits and assessments.
- Document and report on compliance status.
- Regularly update policies and procedures based on audit findings and regulatory changes.

AMERICAN
TECHNOLOGY
SERVICES

FAIRFAX

2751 Prosperity Ave
Suite 600
Fairfax, VA 22031

NEW YORK

250 Broadway
Suite 610
New York, NY 10007

ATLANTA

4360 Chamblee
Dunwoody Rd, Suite
517 Atlanta, GA 30341

CONTACT

+1 888 876 0302
info@networkats.com
networkats.com