Introduction

Asset management is the cornerstone of any organization and essential for maintaining a strong cybersecurity posture. Its importance is highlighted by the CIS Top 20[1], which prioritizes asset management in its first two controls. Additionally, business asset identification is the second step in the NIST Cybersecurity Framework[2] (CSF), only after governance. Effective asset management is scientifically and authoritatively recognized as critical for achieving cybersecurity effectiveness.

TFORM is a distinguished Data Quality Management platform that can transform your asset management system. It improves the accuracy of your CMDB, making it a single source of truth. TFORM plays a crucial role in compliance and cybersecurity. Our strong reputation in asset management is supported by our engagements and publications. TFORM effectively supports critical aspects of compliance and security frameworks by directly aligning with specific requirements. The comprehensive analysis below, detailed as a checklist and features, highlights TFORM's extensive relevance and demonstrates how it fortifies your overall cybersecurity posture.

TFORM's capabilities extend beyond basic IT Asset Management (ITAM), significantly enhancing customer data security, availability, processing integrity, confidentiality, and privacy. It maintains records and audit trails of changes made to the configuration to demonstrate compliance, provide assurance, and streamline efficiency through its centrally managed, agentless, and non-intrusive service.

This document presents a comprehensive checklist detailing how TFORM's capabilities align with each of the four regulatory compliance requirements listed below. The objective is to underscore TFORM's integral role in assisting companies in achieving and maintaining these compliance standards while offering significant value in optimizing IT operations.

Compliance Standards

- TSC SOC 2
- NIST CSF
- HIPAA
- HHS Section 405(d)

[1] Center for Internet Security. "CIS Controls List." CIS, https://www.cisecurity.org/controls/cis-controls-list. Accessed 14 June 2024.

[2] National Institute of Standards and Technology. "Cybersecurity Framework." NIST, https://www.nist.gov/cyberframework. Accessed 14 June 2024.

TSC SOC 2

Trust Services Criteria (TSC) for Service Organization Control 2 (SOC 2), developed by the American Institute of CPAs (AICPA), provides a framework for managing and safeguarding customer data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy. SOC 2 compliance is crucial for service providers to ensure adequate controls and practices are in place.

A reliable CMDB provides visibility into system configurations, enabling the organization to address discrepancies and ensure configurations meet required standards, which is essential for maintaining SOC 2 compliance. TFORM is critical in ensuring that the Configuration Management Database (CMDB) serves as the organization's single source of truth.

The following table illustrates how TFORM directly supports the outcomes required for SOC 2 compliance, making it an ideal foundation for your data management and security efforts.

Table 1 - TFORM Capability Addressing the Aspect of TSC SOC 2

Requirement	Benefit	TFORM Capability
C3.1 - CC3.4	Risk Assessment	• Maintains a detailed inventory of all devices, applications, and databases. • Continuously monitors compliance for Backup systems, Patching, Monitoring tools, Antivirus software, Cybersecurity measures, and ITSM CMDB • Ensure accurate device information for incident management
CC4.1 - CC4.2	Monitoring and Detection	• Monitors and notifies technical teams of inaccuracies in the CMDB and other IT tools • Ensures devices have the latest OS patches and antivirus definition updates
CC6.1, CC6.3, CC6.5, CC6.7, CC6.8	Logical and physical access controls	N/A
CC7.1 - CC7.5	System Operations	• Ensures all devices are monitored, backed up, equipped with antivirus, patched, secured, and included in the ITSM CMDB • Maintains a detailed inventory of all devices, applications, and databases • Support contingency plan development and asset recovery during disasters • Enables cybersecurity management systems to scan and identify system gaps • Ensures monitoring systems track device status, CPU, RAM, HD space, and services
CC2.1 – CC2.2	Integrity of operating information and internal communications	
CC8.1 - CC8.2	Change Management	• Automates processes to correct inaccuracies in the ITSM CMDB • Ensure effective change management through accurate IT asset records
CC9.1 - CC9.2	Risk Mitigation, Vendor Management	N/A
A1.1 - A1.2	Processing Integrity	• Ensures a detailed inventory of all devices, applications, and databases • Continuously monitors compliance for Backup systems, Patching, Monitoring tools, Antivirus software, Cybersecurity measures, and ITSM CMDB
C1.1 - C1.2	Confidentiality	N/A
P1.1 - P1.2	Privacy	N/A

NIST CSF

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) provides a policy framework for computer security guidance. It helps private sector organizations in the US assess and improve their ability to prevent, detect, and respond to cyber-attacks. It is widely used for its flexible, risk-based approach.

Effective asset management and system configurations are essential for robust cybersecurity and for meeting the requirements of NIST CSF compliance. An accurate CMDB is the cornerstone of this requirement, and TFORM can help establish it as the definitive source of truth within an organization.

In the table below, we demonstrate how TFORM aligns with NIST CSF outcomes, ensuring your organization can effectively manage cybersecurity risks.

Table 2 - TFORM Capability Addressing NIST CSF

Requirement	Description
Govern (GV)	• Conducts assessments against the ITSM CMDB to ensure all network devices are represented • Continuously monitors compliance for backups, patching, monitoring, antivirus, cybersecurity tools, and the ITSM CMDB • Ensures proper deployment and use of IT tools on all network devices
Roles, Responsibilities, and Authorities (GV.RR):	• N/A
Identify (ID)	• Continuously maintains a detailed inventory of all devices, applications, and databases and ensures they are included in the ITSM CMDB • Improve cybersecurity posture by monitoring compliance for backups, patching, monitoring, antivirus, and cybersecurity tools • Provides insights into gaps in change management and CMDB inaccuracies • Provides the vulnerability management system with the essential information to ensure every device is identified and can be scanned for vulnerabilities.
Risk Assessment (ID.RA)	• Continuously maintains a detailed inventory of all devices, applications, and databases and ensures they are included in the ITSM CMDB • Provides the vulnerability management system with the essential information to ensure every device is identified and can be scanned for vulnerabilities • Continuously runs in the background, capturing gaps during incident, change, capacity, and problem management
Risk Management Strategy (ID.RM)	• Continuously maintains a detailed inventory of all devices, applications, and databases and ensures they are included in the ITSM CMDB • Provides the vulnerability management system with the essential information to ensure every device is identified and can be scanned for vulnerabilities • Enable port communication between devices • Identifies authorized and unauthorized software for proper deployment • Continuously supports business continuity planning with an accurate inventory, helping to make the best decisions for disaster recovery measures.
Asset Management (ID.AM)	• Discovers all IT devices on the network, including applications and databases, with automated and round-the-clock scheduling • Collects and tracks information to assist with lifecycle management. • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools • Continuously runs data quality audits in the background
Business Environment (ID.BE)	• Identifies all devices on the network to assist with business continuity planning. • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools to identify risks within the IT infrastructure
Protect (PR)	• Identifies risks within the IT infrastructure by continuously monitoring compliance for backups, patching, monitoring, antivirus, and cybersecurity tools

	• Identifies devices that are not backed up, patched, or protected by antivirus • Provides port identification to assist with network segmentation
Identity Management, Authentication, and Access Control (PR.AA):	• N/A
Detect (DE)	• Continuously ensure all applicable devices are integrated with the appropriate IT tools for backups, patching, monitoring, antivirus, and cybersecurity
Adverse Event Analysis (DE.AE):	• N/A
Respond (RS)	• Identifies unauthorized and missing software, as well as gaps in the ITSM CMDB and other IT tools
Incident Analysis (RS.AN):	• N/A
Recover (RC)	• An accurate inventory is the foundation of a business continuity plan. TFORM helps ensure the best decisions for disaster recovery measures and ensures all devices are managed and protected for recovery
Incident Recovery Plan Execution (RC.RP):	

HIPAA

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 sets the standard for protecting sensitive patient data. Organizations managing protected health information (PHI) must implement and adhere to all required physical, network, and process security safeguards. A reliable CMDB satisfies asset management requirements and ensures correct system configurations, thus supporting ePHI protection in accordance with HIPAA. TFORM solidifies the CMDB as the single source of truth within a healthcare organization

TFORM's capabilities extend beyond basic IT Asset Management (ITAM), enhancing the security and privacy of ePHI. It maintains records and audit trails to demonstrate compliance, provide assurance, and streamline efficiency through its centrally managed, agentless, and non-intrusive service.

In the following table, we demonstrate how TFORM's capabilities align with HIPAA compliance requirements, ensuring your organization meets the stringent standards for safeguarding patient information.

Table 3 - TFORM Capability Addressing the Aspect of HIPAA

HIPAA Security Rule	Benefit	How TFORM Supports It
Security Management Process (§ 164.308(a)(1))	Risk Analysis	• Maintains a detailed inventory of all devices, applications, and databases • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools, including the ITSM CMDB • Ensures devices are included in the cybersecurity management system for scanning and patching • Supports incident management by ensuring device accuracy
Security Management Process (§ 164.308(a)(1))	Risk Management	• Delivers timely and proactive risk management by maintaining current and accurate asset records throughout their lifecycle • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools, including the ITSM CMDB. • Ensures devices are included in the cybersecurity management system for scanning and patching
Assigned Security Responsibility (§ 164.308(a)(2))	Accountability	• Ensures data uniformity and precision across all IT tools • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools, including the ITSM CMDB • Reviews data neutrally, identifying discrepancies and ensuring they are addressed
Workforce Security (§ 164.308(a)(3))	Access Control	• N/A
Information Access Management (§ 164.308(a)(4))	Access Authorization	• N/A
Security Awareness and Training (§ 164.308(a)(5))	Asset management related training	• Discovers every IP-connected device on the network, including hardware, software, network, and medical devices • Ensures your CMDB remains accurate with an API connection directly to your ITSM platform • Assists with lifecycle management and conducts regular audits for data accuracy • Dramatically improves change management and tracking • Ensures all devices are integrated with proper tools for patching, antivirus, etc. • Utilizes TFORM's end-of-life module for servers and desktops • Improve MTTR for incident management, perform asset tagging, and more
Security Incident Procedures (§ 164.308(a)(6))	Incident Response	• Provides an accurate CMDB that provides essential asset details, ensuring a higher probability of successful closure, better MTTR, and effective root cause determination

Contingency Plan (§ 164.308(a)(7))	Asset Recovery	• Maintains a detailed inventory of all devices, applications, and databases to support contingency plan development and asset recovery during disasters • Minimizes security risks by ensuring antivirus, patching, end-of-life management, and cybersecurity tools are properly configured and maintained
Facility Access Controls (§ 164.310(a))	Physical Asset Security	• Support physical security by ensuring all assets are accounted for
Workstation Use (§ 164.310(b))	Usage Policies	• Ensures workstation policies are delivered and enforced by delivering an accurate CMDB
Access Control (§ 164.312(a))	User Identification	• N/A
Audit Controls (§ 164.312(b))	Logging and Monitoring	• Supports tracking, access, and usage of ePHI by ensuring all assets are included in audit and monitoring systems
Integrity (§ 164.312(c))	Data Integrity	• TFORM's 3-way correlation engine supports asset configuration to protect ePHI integrity. • Ensures all systems with or without ePHI are being backed up and included in the ITSM CMDB
Person or Entity Authentication (§ 164.312(d))	Authentication Mechanisms	• N/A
Transmission Security (§ 164.312(e))	Secure Communication	• N/A
Policies and Procedures (§ 164.316(a))	Asset Policies	• Discovers every IP-connected device on the network, including hardware, software, network, and medical devices • Ensure your CMDB remains accurate with an API connection directly to your ITSM platform • Assists with lifecycle management and conducts regular data accuracy audits • Dramatically improves change management and tracking by providing an accurate and complete asset management inventory • Ensures all devices are integrated with proper tools for patching, antivirus, etc. • Leverages TFORM's end-of-life module for servers and desktops, including asset tagging • Supports the development of policies and procedures with all collected data
Documentation (§ 164.316(b))	Record Keeping	• Supports HIPAA documentation requirements by ensuring all devices are known, managed, protected, and reported on
Sanctions (§ 164.530(e))	Enforcement	• N/A
Mitigation (§ 164.530(f))	Risk Mitigation	• Maintains a detailed inventory of all devices, applications, and databases • Continuously monitors compliance for backups, patching, monitoring, antivirus, and cybersecurity tools, including the ITSM CMDB • Ensures devices are in the cybersecurity management system for scanning and patching • Assists with business continuity planning

HHS Section 405(d)

The Cybersecurity Act[3] became law in 2015, establishing a standing Task Group under Section 405(d) to develop communication products that align with healthcare industry security approaches. This initiative created a website and publication that serve as primary references for healthcare-focused cybersecurity resources.

In the table below, we illustrate how TFORM directly supports the outcomes established by the 405(d) Task Force and why it should play a crucial role in your cybersecurity efforts. TFORM's capabilities extend beyond basic IT Asset Management (ITAM), significantly enhancing the security and privacy of ePHI, aiding in the auditing of CI records to demonstrate compliance, providing assurance, and streamlining efficiency through its centrally managed, agentless, and non-intrusive service.

Table 4 - TFORM Capability Addressing HHS Section 405(d)

Requirement	Area	TFORM Capability
Cybersecurity Practice #1:	Email Protection Systems	• N/A
Cybersecurity Practice #2:	Endpoint Protection Systems	• Ensures your CMDB is accurate by capturing all devices on your network that need protection • Ensures all applicable devices are protected by antivirus software and included in your vulnerability management system for OS patch deployment • Assists with network port communication for segmentation purposes • Identifies unauthorized deployed applications
Cybersecurity Practice #3:	Access Management	• N/A
Cybersecurity Practice #4:	Data Protection and Loss Prevention	• Ensures your CMDB is fully accurate to protect all applicable devices • Focuses on regular data backups and identifies devices that are not being backed up • Identifies systems not properly protected with antivirus, vulnerability management, and network security measures, including port communication • Detects unauthorized software on both on-premises and public cloud environments
Cybersecurity Practice #5:	Asset Management	• Discovers every IP-connected device on the network, including hardware, software, network, and medical devices • Ensures your CMDB remains accurate with an API connection directly to your ITSM platform • Assists with lifecycle management and continually conducts data accuracy audits • Dramatically improves change management and tracking • Ensures all devices are integrated with proper tools for patching, antivirus, and other protections • Leverages TFORM's end-of-life module for servers and desktops • Improves MTTR for incident management and performs asset tagging
Cybersecurity Practice #6:	Network Management	• Assists with the segmentation of medical devices, servers, and other vulnerable devices • Provides detailed information on port communication • Ensures an accurate CMDB that aligns with the vulnerability management system and OS patching • Ensure all network devices are represented in the CMDB and integrated with the appropriate tools. • Performs continual audits to ensure compliance with TFORM

[3] U.S. Department of Health and Human Services. "Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients." 405(d) Aligning Health Care Industry Security Approaches, https://405d.hhs.gov. Accessed 15 June 2024.

Cybersecurity Practice #7:	Vulnerability Management	• Identifies every device on the network, ensuring the CMDB is accurate • Audits your vulnerability management system to ensure all in-scope devices are managed • Enables scanning, updating, and protection for all devices. • Significantly improves the MTTR
Cybersecurity Practice #8:	Incident Response	• Provides an accurate CMDB that provides essential asset details, ensuring a higher probability of successful closure, better MTTR, and effective root cause determination
Cybersecurity Practice #9:	Network Connected Medical Devices	• Discovers every IP-connected device on the network, including hardware, software, network, and medical devices • Identifies risks with IoMT devices and ensures compliance with manufacturer guidelines • Assists with segmentation planning and device identification
Cybersecurity Practice #10:	Cybersecurity Oversight and Governance	• Participates in risk management and continuous monitoring and auditing • Heavily involved in the incident management process to ensure high asset accuracy within the CMDB • Assists with compliance, audits, and regulatory requirements

Notice to Reader: This document details how TFORM can enhance your compliance efforts. TFORM and similar tools are crucial for secure operations, reducing risks, and providing successful audit evidence. However, they must be supported by established management practices tailored to your organization's unique risks and needs. TFORM plays a supportive role in risk management. While using TFORM alongside recognized standards and frameworks is important, it alone will not fulfill all cybersecurity requirements.

Please contact us for more details on how TFORM can assist with your Regulatory Compliance requirements.

(972) 746-4604
Info@tform.io
www.tform.io