# Table of Contents

- **Introduction** .......................................................... 3
- **Requirements for Data Protection** ............................................ 4
  - Encryption of Data at Rest ................................................. 7
  - Encryption of Data in Transit ............................................. 10
  - Removable Media Controls ............................................. 21
- **Verifying Data Protection Controls** ........................................... 26
- **Encryption Benefits** .......................................................... 34
- **Learn More** ....................................................................... 35
Introduction

Organizations that handle sensitive data, such as healthcare and credit card information, are required to audit their data protection controls on an annual basis. Tenable dashboards and reports help management ensure that data is protected in accordance with business risk posture for Confidentiality, Integrity and Availability (CIA). The information provided in Tenable dashboards and reports enables Risk Managers and Chief Privacy Officers to demonstrate to third parties and regulatory bodies that sensitive data is protected in accordance with Data Loss Prevention requirements. Tenable has created a Tenable Security Center dashboard template titled *Maintaining Data Protection Controls* that summarizes the data for this control.
Requirements for Data Protection

Compliance requirements vary among different industries and geographic locations. New legislation and industry regulations are continually developed that change the standards for compliance audits in these industries. Familiarity with multiple compliance standards is necessary, even if they do not seem to be required at the moment. Changing legislation or shifts in an organization’s business offerings require that managers keep abreast of audit criteria in other industries. The goal of compliance requirements is to avoid breaches of regulatory, statutory, or contractual obligations related to information security and of any security requirements. This section provides an overview of three of the common security compliance requirements: HIPAA, ISO 27001, and PCI DSS. These requirements are a small sample of many security compliance initiatives that have overlapping controls. Please refer to the Tenable Research Audits page for a list of audit files that address many of these compliance initiatives.

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) provides a set of rules for the protection and privacy of electronic Patient Health Information (ePHI) for U.S. citizens. The HIPAA rules apply to Covered Entities and Business Associates of Covered Entities. Covered Entities are those who perform the functions of processing data for the release and transmission of funds for medical services and include:

- **Health Plans** - entities that provide or pay for the cost of medical care
- **Health Care Clearinghouses** - organizations that process health care transactions for providers and insurers
- **Health Care Providers** - professionals trained and licensed to give, bill and be paid for health care services and do so via electronic transactions
- **Business Associates of Covered Entities** - organizations that serve in a support capacity for Covered Entities and may not necessarily be in the health care business. Examples of Business Associates include:
  - Attorneys
  - Accountants
  - Consultants
ISO 27001 Overview

ISO 27001 is a collection of standards set by the **International Organization for Standardization (ISO)**, an independent international organization with a **membership** of 167 national standards bodies. Organizations use these standards to guide their Information Security Management System (ISMS) in a manner that reduces risk to the Confidentiality, Availability, and Integrity (CIA) of data.

Many organizations choose to obtain certification from an accredited ISO certification registrar, who audits the program and submits evidence documents to the ISO governing body. The certification process includes a primary audit, followed by a secondary audit that evaluates the effectiveness of the organization’s Information Security Management System (ISMS) and determines if the controls meet all the requirements of the standard. Once the process is complete, the ISO certification registrar issues one of the following: a certification; a conditional certification; or a rejection. The ISO governing body sets the standard, but the accredited ISO certification registrar issues the certification. The ISO certification registrar must be objective and impartial, which means they cannot write documentation or provide consulting services to help the organization address gaps. Accreditation is not mandatory, but provides independent confirmation of competence, which helps large organizations negotiate Service Level Agreements (SLAs) with third parties.

PCI DSS Overview

The **Payment Card Industry Data Security Standard (PCI DSS)** is a comprehensive set of security standards established by the founding members of the PCI Security Standards Council, including Visa, American Express, Discover Financial Services and MasterCard. The PCI DSS is intended to provide a common baseline to safeguard sensitive cardholder data for all bankcard brands and is used by e-commerce vendors who accept and store credit card data. The PCI DSS specifies a variety of high-level guidelines for running a secure network that leads to variations in how auditors interpret these recommendations.

The PCI DSS mandates **12 high-level requirements** that e-commerce organizations must perform to be considered in compliance with the standard. Such organizations must also have a comprehensive vulnerability audit of any internet-facing system that handles credit card transactions. This vulnerability audit is required to look for the following items:
• Any vulnerability with a CVSS score of 4 or larger
• Any cross-site scripting or SQL injection type of vulnerability
• Any evidence of outdated SSL encryption
Encryption of Data at Rest

The NIST Special Publication 800-111, “Guide to Storage Encryption Technologies for End User Devices,” provides guidance for encrypting data at rest. Data at rest is data that is not in motion and may or may not require encryption, depending on the requirements for securing that data. For example, encryption is required for mobile devices, but may not be for servers and desktops which have other data protection controls in place. Encryption requirements for servers and desktops may be required by specific compliance requirements, depending on the sensitivity of the data. This section describes how to use Tenable Compliance & Audit Files to assess various Operating Systems and platforms for encryption of data at rest.

The following audit files contain encryption checks for data at rest. There are additional audit files that can be used to assess various platform versions:

- CIS_Apple_macOS_12
- CIS_Juniper_OS
- CIS_Kubernetes_v1.6.1
- CIS_MS_Windows_10_Enterprise_Bitlocker
- CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker
- CIS_MS_Windows_10_Enterprise_Level_2_Bitlocker
- CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker_Next_Generation_Windows_Security
- CIS_MS_Windows_10_Enterprise_Level_2_Bitlocker_Next_Generation_Windows_Security
- CIS_OSX_10.11
- DISA_STIG_Apple_iOS_12_v1r2-AirWatch
- DISA_STIG_Apple_iOS_12_v1r2-MobileIron
- DISA_STIG_MSSQL_2016_Database
- DISA_STIG_Samsung_Android_7_with_Knox_2.x_v1r1-AirWatch
- DISA_STIG_Samsung_Android_7_with_Knox_2.x_v1r1-MobileIron

As shown below, the CIS_MS_Windows_10_Enterprise_Level_1_Bitlocker audit file contains a check to ensure that hardware-based encryption is enabled for fixed drives. The description is the
audit check name, which becomes the Plugin Name in Tenable Security Center. The Cross References that this audit check maps to are also listed at the bottom in the reference section.

```
<custom_item>
    Name: CONFIG_SYSTEM
    Description: 18.9.11.1:18 Ensure 'Configure use of hardware-based encryption for fixed data drives' is set to 'Enabled'
    Note: The 'Choose drive encryption method and cipher strength' policy setting does not apply to hardware-based encryption. The encryption algorithm used by hardware-based encryption is set when the drive is partitioned. By default, BitLocker uses the algorithm configured on the drive to encrypt the drive. The 'Restrict encryption algorithms and cipher suites allowed for hardware-based encryption option enables you to restrict the encryption algorithms that BitLocker can use with hardware encryption. If the algorithm set for the drive is not available, BitLocker will disable the use of hardware-based encryption.
    Encryption algorithms are specified by object identifiers (OID). For example:
    AES 128 in CBC mode OID: 2.16.840.1.101.3.4.1.2
    AES 256 in CBC mode: 2.16.840.1.101.3.4.1.42
    The recommended state for this setting is: Enabled.

    Rationale:
    From a strict security perspective the hardware-based encryption may offer the same, greater, or less protection than what is provided by BitLocker's software-based encryption depending on how the algorithms and key lengths compare.

    Impact:
    Hardware-based encryption can improve performance of both read and write operations to the storage drive.

    Computer Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Configure use of hardware-based encryption for fixed data drives
    Note: This Group Policy path may not exist by default. It is provided by the Group Policy template VolumeEncryption.admx/adml that is included with the Microsoft Windows 8.0 & Server 2012 (non-R2) Administrative Templates (or newer).

    Default Value:
    BitLocker will use hardware-based encryption with the encryption algorithms set for fixed drives. If hardware-based encryption is not available, BitLocker software-based encryption will be used instead.

    <value_type>POWAL.amazonaws.com</value_type>
    <value_data>1</value_data>
    <reg_key>HKLM\SOFTWARE\Policies\Microsoft\FVE</reg_key>
    <reg_item>CAN_MUST_BE_NULL</reg_item>
</custom_item>
```

The audit check displayed below is from the CIS_Apple_macOS_12.0_Monterey audit file. The Cross References are highlighted for this check, which ensures FileVault is Enabled.
FileVault may also be enabled using command-line using the fdesetup command. To use this functionality, consult the Der Flounder blog for more details:

https://derflounder.wordpress.com/2015/02/02/managing-yosemites-filevault-2-with-fdesetup/
https://derflounder.wordpress.com/2019/01/15/unlock-or-decrypt-your-filevault-encrypted-boot-drive-from-the-command-line-on-macos-mojave/

Rationale:
Encrypting sensitive data minimizes the likelihood of unauthorized users gaining access to it.

Impact:
Mounting a FileVault encrypted volume from an alternate boot source will require a valid password to decrypt it.

solution: "Perform the following to enable FileVault:

Graphical Method:
Open System Preferences
Select Security & Privacy
Select FileVault
Select Turn on FileVault

Additional Information:
FileVault may not be desirable on a virtual OS. As long as the hypervisor and file storage are encrypted the virtual OS does not need to be. Rather than checking if the OS is virtual and passing the control regardless of the encryption of the host system the normal check will be run. Security officials can evaluate the comprehensive controls outside of the OS being tested."
Encryption of Data in Transit

Data in transit is considered to be data that is moving across a network. The NIST Special Publication titled "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" provides guidance to cryptographically protect data in transit. This Special Publication provides guidance for the selection and configuration of TLS protocol implementations, leveraging Federal Information Processing Standards (FIPS) and NIST-recommended cryptographic algorithms. This section discusses dashboard templates and plugins related to encryption of data in transit, such as certificates and protocols.

The Data Protection - Certificate Status Tenable Security Center dashboard component template uses many of the plugins described in this section to display certificate information for scanned assets.

Certificate Information: Displays the SSL certificate information.

- 10863 | SSL Certificate Information

SSL Certificate Information Detection in Tenable Vulnerability Management
Protocol Detection: The remote service encrypts traffic using a protocol with known weaknesses.

- 8184 | TLS v1.2 Traffic Negotiation Detection
- 8185 | TLS v1.1 Traffic Negotiation Detection
- 8549 | SSLv3 Protocol Detection
- 9129 | SSLv2 Client Connection Request
- 20007 | SSL Version 2 and 3 Protocol Detection
- 56984 | SSL / TLS Versions Supported
- 84470 | TLS Version 1.0 Protocol Detection (PCI DSS)
- 104743 | TLS Version 1.0 Protocol Detection
- 121010 | TLS Version 1.1 Protocol Detection
- 136318 | TLS Version 1.2 Protocol Detection
- 138330 | TLS Version 1.3 Protocol Detection
- 139414 | TLS Version 1.1 Protocol Detection (PCI DSS)
- 700105 | TLS 1.0 Detection
- 700106 | TLS 1.1 Detection
- 700107 | TLS 1.2 Detection
- 700108 | TLS 1.3 Detection
- 700110 | TLS 1.1 Detection (UDP)
- 700111 | TLS 1.2 Detection (UDP)
- 700112 | SSL/TLS Detection
- 700113 | SSL/TLS Detection (UDP)

Note: There are several non-informational plugins that detect deprecated TLS and SSL protocols, such as the following:
- 132675 | SSL/TLS Deprecated Ciphers Unsupported
- 157288 | TLS Version 1.1 Protocol Deprecated

Note: The results from the following plugins can often help find hidden services running TLS.

- 22964 | Service Detection (HTTP Banner)
- 25221 | Remote listeners enumeration (Linux / AIX)
- 83875 | SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
- 110483 | Unix / Linux Running Processes Information

### TLS Version 1.x Detection in Tenable Vulnerability Management

![Finding Table]

**Certificate Issues & Concerns**: Checks for common issues or concerns with certificates. Some issues, such as no certificate, Common Name, or Subject are not required, but offer broader compatibility if used. Other items, such as Self-Signed certificates, may present larger concerns if used in production environments.

- 35297 | SSL Service Requests Client Certificate
- 45410 | SSL Certificate 'commonName' Mismatch
- 45411 | SSL Certificate with Wrong Hostname
- 51356 | Well-known SSL Certificate Used in Remote Device
- 56284 | SSL Certificate Fails to Adhere to Basic Constraints / Key Usage Extensions
- 56471 | SSL Certificate Chain Not Sorted
- 56472 | SSL Certificate Chain Contains Unnecessary Certificates
• 57571  | SSL Certificate Chain Analysis

• 57582  | SSL Self-Signed Certificate

• 121008 | SSL / TLS Certificate Known Hard Coded Private Keys

• 139546 | Improper Check for Certificate Revocation (FG-IR-19-144)

• 139547 | Improper Check for Certificate Revocation (FG-IR-19-144)

• 159544 | SSL Certificate with no Common Name

• 159545 | SSL Certificate with no Subject

Certificate Issues & Concerns displayed in Tenable Vulnerability Management

Black Listed Certificate: An SSL certificate has been detected that is either fraudulent, no longer secure due to leaked or compromised private keys, or was issued from a Certificate Authority that is considered to be untrustworthy.

• 52963  | Blacklisted SSL Certificate

Certificate Expiration/Revocation: Certificates that are active that are not within their validity period, are expired, or will be expiring soon.

• 15901  | SSL Certificate Expiry

• 42980  | SSL Certificate Expiry - Future Validity

• 42981  | SSL Certificate Expiry - Future Expiry

• 72459  | Certificate Revocation List Expiry

• 83298  | SSL Certificate Chain Contains Certificates Expiring Soon

• 121009 | SSL Certificate Validity - Duration
Certificates that are not yet valid or have an invalid duration set

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Severity</th>
<th>Last Updated</th>
<th>Name</th>
<th>IPV4 Address</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>42980</td>
<td>info</td>
<td>06/07/2022 at 03:13 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42980</td>
<td>info</td>
<td>05/11/2022 at 03:12 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42980</td>
<td>info</td>
<td>05/08/2022 at 03:10 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42980</td>
<td>info</td>
<td>04/20/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42980</td>
<td>info</td>
<td>04/07/2022 at 03:11 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>42980</td>
<td>info</td>
<td>04/05/2022 at 03:12 AM</td>
<td>SSL Certificate Expiry - Future Validity</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Certificates that will expire soon, or have expired

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Severity</th>
<th>Last Updated</th>
<th>Name</th>
<th>IPV4 Address</th>
<th>Asset</th>
</tr>
</thead>
<tbody>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 08:20 AM</td>
<td>SSL Certificate Expiry</td>
<td>5.3</td>
<td>5.3</td>
</tr>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry</td>
<td>5.3</td>
<td>5.3</td>
</tr>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry</td>
<td>5.3</td>
<td>5.3</td>
</tr>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry</td>
<td>5.3</td>
<td>5.3</td>
</tr>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry</td>
<td>5.3</td>
<td>5.3</td>
</tr>
<tr>
<td>15961</td>
<td>Medium</td>
<td>06/08/2022 at 03:09 AM</td>
<td>SSL Certificate Expiry - Future Expiry</td>
<td>5.3</td>
<td></td>
</tr>
</tbody>
</table>

Certificate Weaknesses: Certificates that contain weak RSA keys, RSA keys with fewer than 2048 bits, are using a weak hashing algorithm, or are susceptible to spoofing.

- [35291](#) | SSL Certificate Signed Using Weak Hashing Algorithm
- [42053](#) | SSL Certificate Null Character Spoofing Weakness
- [60108](#) | SSL Certificate Chain Contains Weak RSA Keys
- [73459](#) | SSL Certificate Chain Contains RSA Keys Less Than 2048 bits (PCI DSS)
- [86067](#) | SSL Certificate Signed Using SHA-1 Algorithm
- [95631](#) | SSL Certificate Signed Using Weak Hashing Algorithm (Known CA)
Tenable provides dashboard component templates in Tenable Security Center to identify deprecated cryptographic protocols of data in transit, such as the *Encryption - Cryptographic Compliance Concerns* component in the image below.

### Encryption - Cryptographic Compliance Concerns

<table>
<thead>
<tr>
<th>PLUGIN ID</th>
<th>NAME</th>
<th>SEVERITY</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>42873</td>
<td>SSL Medium Strength Cipher Suites Supported (SWEET32)</td>
<td>Medium</td>
<td>2440</td>
</tr>
<tr>
<td>65821</td>
<td>SSL RC4 Cipher Suites Supported (Bar Mitzvah)</td>
<td>Medium</td>
<td>681</td>
</tr>
<tr>
<td>35291</td>
<td>SSL Certificate Signed Using Weak Hashing Algorithm</td>
<td>Medium</td>
<td>665</td>
</tr>
<tr>
<td>69551</td>
<td>SSL Certificate Chain Contains RSA Keys Less Than 2048 bits</td>
<td>Low</td>
<td>312</td>
</tr>
<tr>
<td>70658</td>
<td>SSH Server CBC Mode Ciphers Enabled</td>
<td>Low</td>
<td>291</td>
</tr>
</tbody>
</table>

The *Encryption - Cryptographic Compliance Concerns* Tenable Security Center dashboard component template uses the filter combination below, as shown in the following two images:

- **Plugin Name Regex Match**: `(\skey\s)(\[Kk\]eys\s)(\[Cc\]rypto\s)(\[Aes\]\s)(\[AES\]\s)(\[DES\]\s)(\[TripleDES\]\s)(\[Pp\]\[Gg\]\[Pp\])(\[Cc\]ipher\s)(\[Hh\]ash\s)(\[Ss\]\[Ss\]\[Ll\])(\[Tt\]\[Ll\]\[Ss\])`

- **Severity**: Critical, High, Medium, Low

**Component Configuration for Encryption - Cryptographic Compliance Concerns:**
Details when clicking View Data from the Encryption - Cryptographic Compliance Concerns component:

The SSL/TLS Discovery - SSL/TLS Vulnerabilities By Type dashboard component template in the Tenable Security Center feed displays a count of systems with SSLv2, SSLv3, and TLS discovered actively with Nessus and passively with Nessus Network Monitor.
The following images show detailed results of the cells in the Systems column of the SSL/TLS Discovery - SSL/TLS Vulnerabilities by Type Tenable Security Center dashboard component displayed above. The Systems column displays the number of systems that meet the search criteria, rather than the total number of vulnerabilities that meet the search criteria. The Active and Passive columns display the number of vulnerabilities that meet the search criteria. These columns use the Plugin ID filters for only Active or Passive plugins, respectively. The Systems column uses both Active and Passive plugins to show all systems that meet the criteria.

**SSLv2 [Systems Column]:**

- **Plugin ID** = 20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113

- **Vulnerability Text contains** sslv2,SSL 2.0,SSL version 2

**SSLv3 [Systems Column]:**
- **Plugin ID** = 20007, 56984, 84470, 104743, 22964, 25221, 83875, 110483, 121010, 136318, 138330, 139414, 8185, 8184, 8549, 9129, 700105, 700106, 700107, 700108, 700110, 700111, 700112, 700113

- **Vulnerability Text** contains sslv3, SSL 3.0, SSL version 3

**Vulnerabilities**

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Severity</th>
<th>Total</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>20007</td>
<td>SSL Version 2 and 3 Protocol Detection</td>
<td>Critical</td>
<td>343</td>
<td>Service detection</td>
</tr>
<tr>
<td>83875</td>
<td>SSL/TLS Diffie-Hellman Modulus &lt;= 1024 Bits (Logjam...)</td>
<td>Low</td>
<td>9</td>
<td>Misc.</td>
</tr>
<tr>
<td>56984</td>
<td>SSL / TLS Versions Supported</td>
<td>Info</td>
<td>343</td>
<td>General</td>
</tr>
<tr>
<td>22964</td>
<td>Service Detection</td>
<td>Info</td>
<td>3</td>
<td>Service detection</td>
</tr>
</tbody>
</table>

**TLS 1.0 (Deprecated) [Systems Column]:**

- **Plugin ID** = 84470, 104743, 700105

- **Vulnerability Text** Contains TLSv1

**Vulnerabilities**

<table>
<thead>
<tr>
<th>Plugin ID</th>
<th>Name</th>
<th>Severity</th>
<th>Total</th>
<th>Family</th>
</tr>
</thead>
<tbody>
<tr>
<td>104743</td>
<td>TLS Version 1.0 Protocol Detection</td>
<td>Medium</td>
<td>2492</td>
<td>Service detection</td>
</tr>
</tbody>
</table>

**TLS 1.1 [Systems Column]:**

- **Plugin ID** = 20007, 56984, 84470, 104743, 22964, 25221, 83875, 110483, 121010, 136318, 138330, 139414, 8185, 8184, 8549, 9129, 700105, 700106, 700107, 700108, 700110, 700111, 700112, 700113

- **Vulnerability Text** Contains TLSv1.1
TLS 1.2 [Systems Column]:

- **Plugin ID** =
  20007,56984,84470,104743,22964,25221,83875,110483,121010,136318,138330,139414,8185,8184,8549,9129,700105,700106,700107,700108,700110,700111,700112,700113

- **Vulnerability Text Contains** TLSv1.2

TLS 1.3 [Systems Column]:

- **Plugin ID** =

---

- 19 -
2007, 56984, 84470, 104743, 22964, 25221, 83875, 110483, 121010, 136318, 138330, 139414, 8184, 8549, 9129, 700105, 700106, 700107, 700108, 700110, 700111, 700112, 700113

- **Vulnerability Text** **Contains** TLSv1.3
Removable Media Controls

Data stored on removable media is susceptible to unauthorized disclosure and needs to be secured. Removable media, by design, is designed to be portable and is particularly susceptible to data loss. This section describes security concerns for removable media and how Tenable products can determine if controls are in place that align with the organization’s policy on removable media.

Removable media has both “read” and “write” access controls. Many organizations restrict write access to prevent data from being written to removable media. Exceptions may be made on a case by case basis.

If write access is permitted, encryption can be enforced at the file or device level, depending on the solutions in place and the company policy. The NIST Special Publication 800-111, “Guide to Storage Encryption Technologies for End User Devices,” provides guidance for encrypting data on removable media.

Data Loss Prevention controls can be used to prevent particular types of data (such as credit card numbers) from being written to removable media, even if write access is permitted.

The following image displays an audit check from the CIS_MS_Windows_10_Enterprise_Bitlocker audit file, which ensures that hardware-based encryption for removable data drives is enabled.
Unix-based systems support file system mount options that can provide additional security controls, such as ‘nodev,’ ‘noexec,’ and ‘nosuid,’ as described below:

- **nodev** - Restricts character and blocks special devices from being accessed on the filesystem. Character and block special devices are those that permit access to a file that is attached to a device that is not part of the file system, such as a USB drive. Use the ‘nodev’ mounting option for filesystems that contain sensitive data to prevent data exfiltration. Removable media containing character or block special devices could be used to bypass security controls by allowing non-root users to access sensitive device files such as /dev/kmem or raw disk partitions.

- **noexec** - Prevents executable files from running on a file system. Use the ‘noexec’ option for removable media to prevent malware from being run when the media is attached to the system.
• **nosuid** - Disables the ability to elevate privileges on a file system. Use the ‘nosuid’ option for world-writable file systems and removable media.

The Data Protection - Removable Media noexec, nosuid, nodev Compliance Tenable Security Center dashboard component template uses the following filters:

• **Plugin Type:** Compliance


The following image displays an audit check from the **CIS_CentOS_8_Server** audit file, which displays the mount options that are used on the file system.

Note: This is a manual check, requiring a review of the output by IT staff who are familiar with the correct settings for the system. See "Manual Review Required" in the expect section of the image.
Tenable provides dashboard component templates in the Tenable Security Center feed, such as the *Removable Media and Content Audits - CDROM, Floppy, Other Storage Audit* component shown below.

<table>
<thead>
<tr>
<th>Passed</th>
<th>Manual</th>
<th>Failed</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitLocker</td>
<td>BitLocker</td>
<td>BitLocker</td>
</tr>
<tr>
<td>CDROM</td>
<td>CDROM</td>
<td>CDROM</td>
</tr>
<tr>
<td>Remote Storage</td>
<td>Remote Storage</td>
<td>Remote Storage</td>
</tr>
<tr>
<td>Removable Media</td>
<td>Removable Media</td>
<td>Removable Media</td>
</tr>
<tr>
<td>Removable Storage</td>
<td>Removable Storage</td>
<td>Removable Storage</td>
</tr>
<tr>
<td>floppy</td>
<td>floppy</td>
<td>floppy</td>
</tr>
</tbody>
</table>

In Tenable Security Center, the audit check name corresponds to the Plugin Name, so searches can be performed using the *Plugin Name* filter. For example, the search below can be used in Tenable Security Center to find results from audit scans [also called compliance scans] with check names containing ‘removable media’ and ‘nodev’ from various audit files.

- **Plugin Name Regex Match** (`nodev.*[Rr]emovable [Mm]edia)(([Rr]emovable [Mm]edia.*nodev)`
- **Plugin Type**: compliance
In the Tenable Vulnerability Management *Host Audits Findings*, the *Audit Name* filter can be used to display results from various audit files. For example, the search below displays any scan results from audit checks containing "Removable Media."

- *Audit Name* is equal to *Removable Media*
Verifying Data Protection Controls

The National Institute of Standards (NIST) Special Publication 800-53 provides comprehensive guidance for a secure infrastructure. This section describes NIST guidance for data protection controls and how Tenable solutions help validate that appropriate encryption controls are implemented within the organization.

The NIST Cybersecurity Framework (CSF) is a control framework, whose high level controls align with ISO 27001, NIST SP 800-53, and others. The Cybersecurity Framework’s prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. Many regulating bodies accept evidence documentation of compliance with the NIST CSF as assurance that the organization has effective controls in place to meet their security requirements. The HIPAA Security Rule Crosswalk to NIST Cybersecurity Framework is an example of alignment with NIST.

Tenable audit checks contain a reference field that points to specific controls in a standard (ISO 27001), framework (NIST Cybersecurity Framework), or regulation (HIPAA) and is used by nearly all plugins. Any external reference can be identified using the Cross References field. References can be used to search or filter in Tenable Security Center. For example, the following References define requirements for the encryption of data at rest:

- 800-171 - 3.13.16
- 800-53 - SC-28

Security Requirement 3.13.16 in the NIST Special Publication 800-171 Revision 2 provides guidance to protect the confidentiality of Controlled Unclassified Information (CUI) at rest and maps to Security Control SC-28 of NIST Special Publication 800-53, which provides guidance for Protection of Information at Rest. Security Requirements specify what action needs to be taken. For example, HIPAA requires that Personal Health Information (PHI) be encrypted when traversing internal networks. Security controls specify how to meet the requirement, such as “enable switch to switch encryption on internal network segments.”

Data at rest is data that is stored on a device and not in process or transmission. Encryption requirements for data at rest depend on the sensitivity of the data and other protection controls that may be in place. For example, data stored on mobile devices has a greater risk since the device is exposed to unsecured networks. Data stored on secure servers in a protected data center has a
lower risk of unauthorized access. NIST Special Publication 800-171 provides recommended requirements to protect the confidentiality of controlled unclassified information.

The 800-53:SC-28 mapping aligns with the following regulatory controls:

- 800-171: NIST 800-171 (Standard)
- csf: NIST Cybersecurity Framework (CSF) (Framework)
- hipaa: HIPAA (Regulation applying a standard)
- isoiec-27001: ISO 27001 (Standard)
- pci-dss: PCI-DSS (Standard)
- cobit5: COBIT (Standard)

Control mappings, shown as “reference” in the following audit check image, identify encryption algorithms and cipher suites that the audit check verifies. Audit checks can map to multiple controls across multiple standards. For example, the audit check shown in the image below verifies compliance with the following controls:

- NIST SP 800-53 - RA-2
- CIS Critical Security Controls (CSC) v6 - 13.2
- CSC v7 - 13.6
- CSC v8 -3.6
- CSF - ID.AM-5, ID.RA-4, ID.RA-5
- General Data Protection Regulation (GDPR) - 32.1, 32.1.d
- HIPAA - 164.306(a)(1)
- Overview of IT Security Risk Management: A Lifecycle Approach (ITSG-33) - RA-2
- LEVEL|BitLocker Automated (BLA)
- National Electronic Security Authority (NESA) - M2.2.1, T1.3.1
- QCSC-v1|6.2
- QCSC-v1|11.2
The Data Protection - Confidentiality of Protected Information Concerns Tenable Security Center dashboard component template uses the Cross References mentioned above in the filters for the component, shown in the next two images:

- **Cross References** = 800-53|RA-2,CSCv6|13.2,CSCv7|13.6,CSCv8|3.6,CSF|ID.AM-5,CSF|ID.RA-4,CSF|ID.RA-5,GDPR|32.1.b,GDPR|32.1.d,HIPAA|164.306(a)(1),ITSG-33|RA-2,LEVEL|BLA,NESA|M2.2.1,NESA|T1.3.1,QCSC-v1|6.2,QCSC-v1|11.2

- **Plugin Type**: Compliance

- **Severity**: High, Medium
The table below displays the Cross Reference display formats in Tenable Security Center and Tenable Vulnerability Management:

<table>
<thead>
<tr>
<th>NAME</th>
<th>SEVERITY</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>5.2 Client Encryption</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>5.1 Inter-node Encryption</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>4.1 Ensure that logging is enabled: - logback.xml</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>4.1 Ensure that logging is enabled: - nodetool getlogginglevels</td>
<td>High</td>
<td>4</td>
</tr>
<tr>
<td>3.5 Ensure that Cassandra only listens for network connections on authorized interfaces</td>
<td>High</td>
<td>4</td>
</tr>
</tbody>
</table>

In Tenable Security Center, the Cross References are displayed in Scan Results

In Tenable Vulnerability Management, the Cross References are displayed in a
The expected filter format syntax for searching, filtering, and querying in Tenable Security Center <XREF TYPE>\|<XREF ID> uses a pipe, "\|", rather than a colon, ":". In the GUI the XREF Type and ID are separated by a ":". Please note in the filter, you must use a pipe, "\|". Using an example from above, 800-171 is the XREF Type, and 3.13.16 is the XREF ID. A search with proper syntax in Tenable Security Center that matches any item in the comma separated list is shown below, as used...
in the *Data Protection - Data at Rest - Encryption Compliance* Tenable Security Center dashboard component template.

<table>
<thead>
<tr>
<th>NAME</th>
<th>SEVERITY</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.14 Ensure Configuration File Encryption is Set</td>
<td>High</td>
<td>3</td>
</tr>
<tr>
<td>1.5.9 Ensure NIST FIPS-validated cryptography is configured - rpm</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>1.5.9 Ensure NIST FIPS-validated cryptography is configured - proc</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>1.5.9 Ensure NIST FIPS-validated cryptography is configured - grub</td>
<td>High</td>
<td>1</td>
</tr>
<tr>
<td>1.5.9 Ensure NIST FIPS-validated cryptography is configured - etc</td>
<td>High</td>
<td>1</td>
</tr>
</tbody>
</table>

Note: Spaces can be included or omitted after commas.

- *Cross References* = 800-171|3.13.16, 800-53|SC-28
- *Plugin Type*: Compliance
- *Severity*: Medium, High
The following table displays valid Cross References that can be found in Tenable Vulnerability Management and Tenable Security Center:

<table>
<thead>
<tr>
<th>Non-Compliance</th>
<th>Compliance</th>
</tr>
</thead>
</table>
Below are some Cross Reference search examples that can be used in Tenable Security Center (xref refers to the Cross References filter):

- `xref = 800-53|AC*`
  - Would be a match for AC-1, AC-2, etc.
- `xref = 800-53|AC-1`
  - Would be a match for AC-1, but not AC-11
- `xref = 800-53|AC-1*`
  - Would be a match for AC-1, AC-11, AC-12, etc.
- `xref = 800-53|SC-7 (5), 800-53|SC-8`
  - Would match 800-53|SC-7 (5) and 800-53|SC-8
- `xref = 800-53|SC-7*`
  - Would match 800-53|SC-7 (5), 800-53|SC-7, 800-53|SC-71, etc.
- `xref = 800-53|*`
  - Would match anything with 800-53 any xref ID
- `xref = 800-53|*7`
  - Would match anything with XREF ID ending in 7
- `xref = 800-53|S*-7`
  - Would match anything with XREF ID beginning with S and ending with "-7"
# Encryption Benefits

Encryption has garnered quite a lot of attention in recent years as cyber criminals have leveraged encryption to lock organizations out of their data through [ransomware attacks](#). Many companies have learned the hard way that encryption is very effective and difficult to break without the correct key. Organizations should take their queue from cyber criminals and leverage encryption themselves to protect their data from unauthorized access. Encryption costs very little to implement, but does require that a process be developed and implemented to manage encryption keys and ensure that multiple business owners have access to encryption keys. Encryption is required by many data protection regulations, such as PCI DSS and HIPAA, which levy heavy fines for violations. The migration to remote work requires an efficient, encrypted communication system, such as a VPN to protect data in transit.

Encrypting everything is not practical, since personnel still need to be productive. Developing a strategy for encryption can go a long way towards protecting data and saving the organization from costly data breaches and fines.
Learn More

COBIT (An ISACA Framework)

ISO About Us: Members

ISO/IEC 27001 Information Security Management

NIST Compliance FAQs: Federal Information Processing Standards (FIPS)

NIST Computer Security Resource Center (CSRC) Publications

NIST Cybersecurity Framework (CSF)

NIST Special Publication 800-52 Rev. 2 "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations"

NIST Special Publication 800-53 Rev. 5 "Security and Privacy Controls for Information Systems and Organizations"

NIST Special Publication 800-111 "Guide to Storage Encryption Technologies for End User Devices"

PCI Document Library

Tenable Compliance and Audit Files Download

Tenable Host Audits Findings Details

Tenable Plugins Search

U.S. Department of Human & Health Services Health Information Privacy (HIPAA)