An IT Auditor's Guide to Security Controls & Risk Compliance

Understanding Compliance Control Policies & 6 Controls for Managing Regulated Systems

Bit9 + CARBON BLACK

TABLE OF CONTENTS

INTRODUCTION

Governance, Risk and Compliance professionals face multiple challenges. They must, of course, ensure that their organizations are meeting the minimum requirements of the appropriate standards. Many organizations must comply with multiple standards covering privacy, corporate financial data, Protected Health Information and credit card data. Fortunately, the overlapping standards agree on a single concept; implementing appropriate security controls to protect information from improper disclosure.

However, GRC requirements do not exist in a vacuum. Organizational objectives must also be supported. Critical functions can be disrupted if business needs are not considered when establishing compliance activities. In addition, providing evidence that the appropriate controls are in place and enforced is a requirement of any audit. Investing in selecting the right policies, controls and solutions leads to more successful audits and security that is more reliable.

A Simple, Effective Approach

Bit9's approach to compliance is simple. Organizations should include relevant stakeholders in building Compliance Control Policies to meet regulatory standards while supporting business goals. Control Policies dictate which assets are covered by each Standard and what actions users can execute for each asset. By grouping similar classes of assets and users, policies can be logical to users, enforcement is automatic and audits are simplified.

This paper will review creating Compliance Control Policies and six key controls supported by Bit9:

1. Configuration Change Monitoring and Chain of Custody
2. File Integrity Control and Monitoring
3. Malware Prevention and Continuous Compliance Visibility
4. Compliance Risk Analysis and Measurement
5. Security Policy Awareness, Enforcement and Audit
6. Portable Device Usage and Control

These Compliance Control Policies are relevant to all major compliance standards. They focus on preventing unwanted changes to systems within an organization (whether through modifications to key files, infections through malware or simply unauthorized executables), monitoring changes from the approved configurations and ensuring that only authorized users can add, modify or remove critical data from covered systems.

CONTROL POLICIES FOR COMPLIANCE

For compliance professionals, regulatory standards translate into operational "controls" used to ensure that an organization is taking appropriate steps to prevent unauthorized actions, monitoring those actions to detect anomalies and providing documentation that the organization has integrated these controls as part of its "Business as Usual" activities. Like any security activity, these controls must map back to corporate goals, and these goals should be expressed in terms of Compliance Control Policies.

Compliance Control Policies, based on the applicable regulatory standard, determine users' privileges and device controls throughout an organization. In an audit, a Control Policy provides a benchmark against which auditors can measure compliance and security risk, the key deliverable of any audit.

BLACKLISTING V. COMPLIANCE CONTROL POLICIES

Blacklisting refers to a defensive position against previously identified malware, as is typical in traditional anti-virus software. Signatures are generated for the known malware and added to endpoints through updates (the blacklist). Whenever an executable requests access to the device's CPU, the antivirus software generates a signature for that executable and compares it in memory to the millions of signatures of previously identified malware. While this is obviously processor-intensive, from a compliance standpoint it is always a step behind the attackers. Any new attacks, not yet identified by the anti-virus vendors or added to endpoints, are free to run and infect devices.

Instead, Bit9 uses Compliance Control Policies as the basis for all application, file and device controls. Control Policies provide a simple method for determining which assets are in-scope for a particular standard, what software is required on those devices and who can make changes to the software and/or files on those devices. Once established, Control Policies will automatically enforce applicable compliance standards and provide auditable logs for evidence of compliance. If an executable is not on a controlled list of allowed software, it will not run.

MAPPING CONTROLS TO COMPLIANCE

Bit9 Control Policies reflect compliance, security and business requirements of each class of assets and users. Controls provide rules for each asset or user to allow full user control, restricted user control or full device lockdown, even when disconnected from the corporate network. For example, Point-of-Sale terminals, servers and kiosks used by multiple users may have dedicated functions. Only specific, credentialed personnel should install new software, and the event should be logged for compliance purposes. Control Policies for these devices would be "full lockdown". No executables will run, whether malware or other, unapproved software, unless installed by an employee with appropriate privileges.

Blacklisting solutions lack the ability for organizations to enforce security policies beyond simple "don't execute files with this exact signature". New attacks, which lack signatures, will execute and infect devices, unknowing users will install unapproved software in violation of corporate policies and critical files remain vulnerable to unauthorized change. With thousands of new threats discovered each day, keeping these signatures up to date is a constant challenge.

SIMPLICITY IS THE KEY

Bit9 Control Policies are simple to establish and manage, and allow organizations to map usage policies directly to compliance standards directly to permissions on all devices. Control Policies can block all unknown or unwanted software, provide unrestricted access to new software, require approval to waive a policy temporarily and educate employees on restricted activities, all with an audited and documented log.

Control Policies can include:

- Full control over all applications on a gold image
- Automatic approval of new applications delivered through software management systems
- Which, if any new executables can run on each class of devices and users
- Which, if any removable media devices can be used, and by whom
- Which files can be changed, and by which people or processes

DOCUMENTATION OF CONTROLS

Putting policies in place is only a beginning, and of little use if an organization cannot provide evidence that the controls are enforced. For example, the PCI testing procedure for Requirement 12 states, "Review risk-assessment documentation to verify that the risk-assessment process is performed at least annually and upon significant changes to the environment." Bit9 provides auditors with a full audit trail of enforcement (blocked malware and unauthorized software), exceptions and policy communication. Every executable on every device is visible from Bit9's control panel, at any time. With Bit9, organizations can build Control Policies that support their businesses, meet compliance standards and simplify audits.

MANAGE YOUR BUSINESS WHILE BIT9 CONTROLS YOUR ENVIRONMENT

Compliance standards are intended to protect data from theft or manipulation. By starting with Control Policies that support business goals, organizations can improve their business practices while meeting compliance standards. Bit9 enforces and logs all activity on protected devices, freeing up IT resources while providing auditors the required evidence of compliance.

CONTROL 1 – CONFIGURATION MONITORING AND CHAIN OF CUSTODY

COMPLIANCE GOALS

- Protect critical information from exposure
- Prevent unauthorized changes to control files, including configuration and log files
- Establish an auditable chain of custody for all control file changes
- Real time monitoring and recording of all critical files

ENFORCING CONTROL POLICIES FOR COMPLIANCE

While personal and corporate information are the focus of most regulations, compliance professionals must also consider a third category of data they must monitor and protect - the operational information (security settings, procedures and configurations) used to ensure that the personal and/or corporate information is secure. These "Control Files" include configuration and log files that, when changed, expose the organization to security risk or indicate that an attack is in process.

RECOGNIZING LEGITIMATE AND MALICIOUS CHANGES

Some critical files need to change over time. Protected log files are updated, and configuration files are modified by authorized personnel. Bit9's Control Policies provide the intelligence to allow legitimate change by authorized users or systems, while blocking all other changes to critical files and providing a reputable audit trail of all changes. Bit9 can even prevent the creation of new files or renaming files in protected directories. This allows normal operations to proceed as usual, while preventing changes that could compromise your organization's compliance with appropriate standards. If changes are required that are out of scope with normal Control Policies, Bit9 provides exception workflow so changes can be requested, approved and logged.

NEAR REAL-TIME MONITORING AND AUDIT READY CHAIN OF CUSTODY

When Bit9 is installed, it automatically creates a complete inventory of applications and files on every system. This information is combined with the Bit9 Software Reputation Service (SRS) data, threat and malicious inventory, and IT trust data to help you proactively monitor your enterprise systems.

Through an advanced comparison of endpoint executables and settings, you can easily sift out any activity that is deemed untrustworthy or has a negative effect on your compliance posture. By utilizing threat and risk metrics across the enterprise, you can compare endpoints individually, or to a group of endpoints and get a snapshot of the status of the systems. More importantly, you get a view into the status of all activity across the enterprise and the ability to control assets and enforce compliance

UPDATE APPLICATIONS WHILE PREVENTING UNAUTHORIZED CHANGES

Part of any audit is providing evidence that applications are up-to-date, or that controls are in place to prevent to prevent subversion of those systems. Bit9's inventory reports allow organizations to identify out-of-date software quickly. Authorized software upgrades are simple with Bit9. Control Policies are aligned with IT-confirmed trusted sources, such as software publishers, internal software repositories, and software delivery or patch management solutions. At the same time, Bit9 can prevent unauthorized executables on systems waiting to be upgraded. This enables organizations to allow trusted software and updates to run with minimal administrative effort.

Figure 1 shows the file inventory across a specific system, all systems in the "Corporate" grouping, and all systems throughout an enterprise. Each system or group displays the mix of file types (executables, scripts and other) and a Bit9 Trust Rating for each. Low Trust files, or those that not previously evaluated, can be examined by "drilling down" through the Bit9 Management interface. Untrustworthy items can be disabled or triaged to identify provenance.

Figure 1.

Applicable Standards

- PCI-DSS – 2.2, 2.2.2, 2.2.5
- HIPAA - § 164.306 (1) § 164.308 (1 and 3), § 164.312 (b) and (c)(2)
- NERC - CIP-003-5 (R4), CIP-007-5 (R5)

CONTROL 2 – FILE INTEGRITY CONTROL AND MONITORING

COMPLIANCE GOALS

- Protect critical information from exposure
- Detect changes to critical files, including configuration and log files
- Real time monitoring and recording of all critical files

BIT9 HELPS MANAGE COMPLIANCE SCOPE

An important aspect of any compliance program is monitoring activity within systems and assets. While the goal is to prevent critical information from exposure, a monitoring program provides evidence to auditors that the appropriate controls are in place and operational.

Not all assets are equally critical, in particular when applied to a compliance standard. Segmenting those systems that are relevant to a particular standard from other assets narrows the scope of compliance efforts and reduces unnecessary information (noise). This makes regulatory reporting and the audit process simpler. Categorizing assets and focusing on those that are most critical also helps organizations from a security standpoint.

MAP ASSETS TO CONTROL POLICIES FOR COMPLIANCE

Bit9's Security Platform provides mappings and templates for file integrity control to enable monitoring and reporting that matches your Control Policies. This allows organizations to control and monitor critical files across many different operating systems. To manage scope better, you can easily add or remove specific systems and assets from the compliance requirements to secure the infrastructure, while avoiding the complexity of the applicable compliance metrics (e.g., PCI, HIPAA, etc.).

Creating rules that map to an organization's Control Policies is simple. Bit9 provides templates for common rules, and organizations can create and reuse custom rules. Rules allow organizations to identify asset types, determine what activities to deny by policy, and which users, systems or processes may modify critical files.

The screen (right) shows how Bit9 easily protects critical files. In this example, Bit9 monitors point-of-sale system log file to detect, alert and block any changes to the file (C:\POS Application Logs). Using the Process Exclusion function, administrators can allow specific processes to write to the log file, as required.

CORRELATED AND CONTEXTUAL LOGGING FOR SIEMS

Almost every asset in an organization produces log files, and monitoring disparate systems can be an administrative burden. To simplify enterprise-wide monitoring and reporting, Bit9 can integrate with an organization's existing monitoring solutions. Centralized reporting allows Bit9 to match your organizations auditing needs.

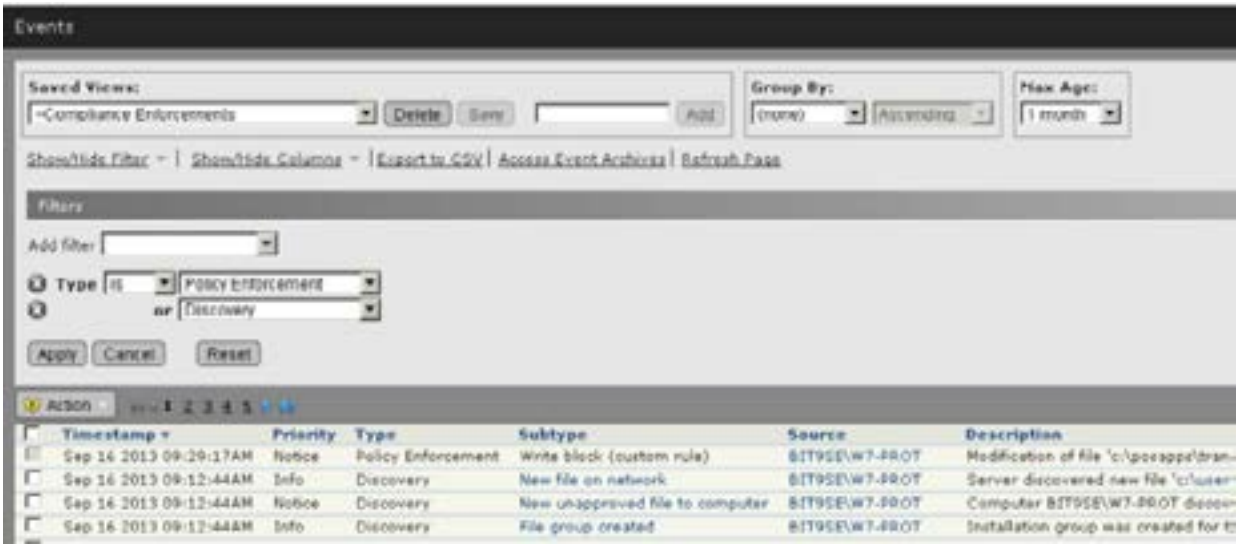
Rather than simply generate events, however, Bit9 correlates events prior to sending information, and provides important contextual information about each occurrence. This provides your compliance and security operations with specific event information, instead of simply data.

EVIDENCE AND ARTIFACTS FOR AUDITORS

A critical part of any audit is providing evidence and artifacts regarding any changes to critical assets, including the rationale for any such change. Bit9 provides this out of the box, maintaining a protected record of changes by asset, and how those changes correspond to specific Trust Policies and regulatory requirements.

Bit9 maintains a real time inventory of all file assets installed on an endpoint, users can centrally identify the presence or absence of vendor-supplied security patches. This real time business intelligence allows the review of event activity in numerous perspectives, such as:

- Track and automatically reconcile and validate changes against enterprise change management (CM) system requests
- Maintain archive version of configuration files for easy rollback
- Track changes to all systems and software and automatically reconcile with approved change requests
- Track changes by users to provide evidence of separation of duties across environments.



In the "Compliance Enforcements" view, a list of enforcement events confirms Bit9's file and asset enforcement by policy. This View can be used to demonstrate to auditors that you are enforcing Control Policies, and build context around your data by correlating those into the events that are critical to your business. This helps lower the administrative burden of compliance pre-assessment data gathering and produces a contextual report of all enforcements that are out-of-line with the compliance policy.

Applicable Standards

- PCI-DSS –2.2; 2.2.2; 2.2.5
- HIPAA – § 164.306 (1); § 164.308 (1)(i) A, B, C, D ; (3)(i) (A) § 164.312 (b); (c)(2)
- NERC – CIP-003- (R4) CIP-007-5 (R5)

CONTROL 3 – MALWARE PREVENTION AND CONTINUOUS COMPLIANCE VISIBILITY

COMPLIANCE GOALS

1. Ensure that malicious software cannot run on any corporate asset
2. Address threat from zero-day attacks
3. Provide evidence that controls map to corporate policies
4. Provide evidence of compliance and communication of policies
    a. Categorization of risk
    b. Rationale for changes to individual devices

STOP FIGHTING A LOSING BATTLE

All regulatory standards dictate that organizations must take steps to prevent malware from running on their systems. After years of deploying blacklist-based anti-virus software, the many attacks reported demonstrate clearly that this approach is not working. Whether it is through a phishing attack, visiting a compromised website or downloading malicious software, the majority of attacks are still caused by the execution of software that should not be allowed to run.

The reason is quite simple: organizations rely on negative-security products like traditional anti-virus that only prevent known malware from running. Since attackers have access to these products, they simply adjust their attacks to change signatures sufficiently to prevent detection (a variety of the so-called zero-day attacks). Once tested, they can conduct their attack confident it will avoid detection.

In addition, systems typically run legitimate commercial and open source applications that may not be malicious, but are simply not needed, or wanted. This could include peer-to-peer applications, games, music and personal software that affects compliance, security and acceptable use policies. Anti-virus software will allow these to run, while auditors view this as evidence of unmanaged controls.

START WITH AUDITABLE CONTROL POLICIES

The logical approach is the opposite of traditional anti-virus. Rather than allowing anything to run other than previously identified malware, organizations should understand what needs to run to support their business goals, and deny or audit all others. Control Policies, which map to compliance standards, can determine and enforce which applications and updates are allowed.

Bit9's security platform makes this effort simple. Establishing Auditable Control Policies better supports compliance goals and improves security. If a server, workstation or device is running the software it needs, Bit9 can stop any other software from executing, whether or not the anti-virus vendors have yet gotten around to identifying it as malware.

CHOOSE THE APPROPRIATE CONTROL POLICY

Since the Control Policies must also support normal business operations, not every system and user requires the same level of control. Specific, single function devices (servers, POS terminals, kiosks) are attractive targets for attack, and have no need for flexibility in what can execute beyond the required POS software. These systems can be fully locked down using Bit9.

In contrast, some users and systems require flexibility. Developers may require new libraries and build new executables, and executives may require the flexibility to install new software without approval from IT or security. Bit9 supports this policy – with oversight and auditing – to minimize changes in workflow while making acceptable use policies, reporting and audits straightforward.

Finally, a third set of users will require permission to make changes to systems. If unknown software is installed, tracking this for compliance and security purposes in necessary. In this mode, Bit9 will block the software from running, while prompting the user to request an override. Once authorization is provided, and logged, the new software will run normally.

TAKING A POSITIVE APPROACH

Positive Security means that the business applications that support your business will run unimpeded. Other software, whether legitimate but unapproved, or malware, can be stopped prior to execution. There is no need to join the race against time with hackers, since Bit9 prevents unapproved software from running regardless of its intent.

DOCUMENTED CONTROL MEANS SIMPLER AUDITS

With Bit9, it is simple to demonstrate your corporate Compliance Control Policies regarding malware and unwanted software, and how those Policies map directly to execution. Reports detailing blocked executables, exceptions and approved software updates are provided by device and by user.

Starting with a logical Trust Policy, Bit9 makes compliance easy while directly supporting business goals.

Applicable Standards

- PCI-DSS – 5.1, 5.2, 5.3, 5.4, 6.1, 6.2, 12
- HIPAA - § 164.308 (5)
- NERC – CIP-002 (R1, R2), CIP-007 (R4, R5, R6, R8)

CONTROL 4 – COMPLIANCE RISK ANALYSIS AND MEASUREMENT

COMPLIANCE GOALS

1. Demonstrate a Business as Usual practice to identify unknown and malicious software
2. A repeatable process for identifying, categorizing and measuring risk across corporate assets
3. Prevent malicious code from executing on endpoints
4. Provide evidence that controls map to established Compliance Trust Policies
5. Provide evidence of compliance and communication of policies

"YOU CAN'T MANAGE WHAT YOU CAN'T MEASURE."

An old management principal is that you must be able to understand a process and measure changes over time in order to manage that process. Visibility to both known and unknown applications running in an organization is required to meet compliance standards such as PCI 5.1 and HIPAA §164.308. If an organization has precise and repeatable processes in place for achieving this, auditing is simplified and effort supporting a standard is ultimately reduced.

For compliance professionals, this involves three activities:

1. Identifying the files and executables that reside on those assets subject to compliance standards.
2. Determining the relative risk of each file or executable
3. Monitoring and measuring changes (drift) from the desired profile over time

Cataloging all executables across an organization, determining which are necessary or optional, and the risk associated with each can seem nearly impossible. How does one determine the origin and validity of thousands of files on a single workstation, must less across an enterprise?

VISIBILITY AND INVENTORY

Bit9 makes identifying and assigning risk to assets simple. When installed, Bit9 automatically builds an inventory of applications on each asset in the organization and provides a consolidated report by asset, group and application. Prohibited or unknown applications can be disabled by device, group or globally to establish a baseline. Once a baseline is established, Bit9 provides continuous monitoring and enforcement of the baseline, and tracks changes ("drift") from the baseline, making reporting simple.

SIMPLE RISK RANKING AND TRUST RATINGS

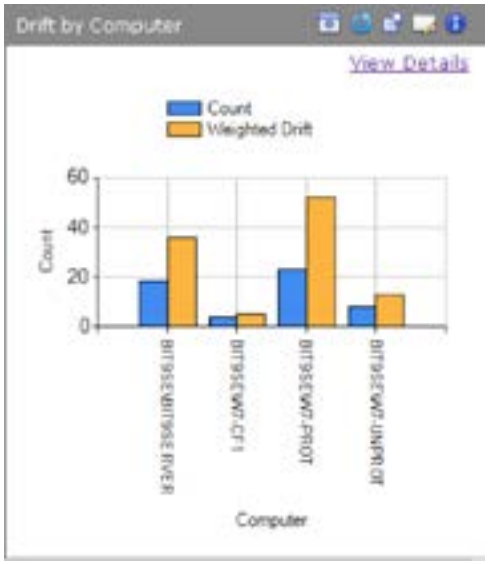
A formidable task for any organization is providing evidence that it knows what is running on its systems and can provide an unbiased risk rating to each executable. Only Bit9 provides compliance officers and auditors with a live inventory of any executable on any of your devices, including a full audit trail of what created it, when it was created, what it did, if it deleted or changed itself, and more.

For unknown executables, Bit9 provides its proven Software Reputation Service. Built over years of research, the Software Reputation Service constantly crawls the Internet looking for software and calculates trust ratings based on attributes such as age, prevalence, publisher, source, results of AV scans and more. When compared to your application inventory, it automatically ranks files as safe, unsafe or flags it for additional scrutiny.

CONTINUOUS AUDIT, ASSESSMENT AND ENFORCEMENT

Establishing a baseline of required applications is a good start, but these images may change, or drift, over time. Users with sufficient permissions may add applications, plug-ins and libraries. Servers may be moved or change function. Monitoring and controlling your executables over time is required for continued compliance.

Bit9 makes this simple as well, with continuous monitoring of every executable or file on every device in your enterprise. Trust Policies dictate what changes are allowed, and by which users or processes. Configurable dashboards can track drift over time, generate alerts and display snapshots of the critical information needed to manage your environment and see how it changes over time.



TRUST POLICIES PROVIDE CONTROL AND EVIDENCE OF COMPLIANCE

Bit9 provides organizations with the framework, tools and reporting to meet strict compliance requirements. Starting with Trust Policies, compliance officers can map permissions and restrictions to in-scope assets to control files and executables. Bit9's Software Reputation Service automatically assigns risk levels to each asset. Continuous audit and assessment features track changes over time, alerting internal personnel to non-compliant devices or applications immediately. With Bit9, visibility, detection, prevention and response are simple to manage.

Applicable Standards

- PCI – 2.4, 6.1, 6.2, 10.6, 11.5, 12.2, 12.3
- HIPAA - § 164.308 (1) and (8), § 164.310 (1) (b), § 164.312 (1) (b)
- NERC - CIP–002–3 (R1, R2, R3), CIP-003-3 (R1, R3, R4, R6), CIP-007-3a (R4, R6)

CONTROL 5 – SECURITY POLICY AWARENESS, ENFORCEMENT AND AUDIT

COMPLIANCE GOALS

1. Demonstrate that compliance policies are in place and audited
2. Provide evidence that policies have been communicated to employees/stakeholders
3. Provide evidence of enforcement and consumption of policies

DEMONSTRATE POLICY ENFORCEMENT

Creating Control Policies is necessary to achieve compliance with many regulatory standards. However, if an organization cannot demonstrate that those policies have been communicated and evidence of enforcement, audits can prove to be time consuming and difficult.

The following are questions those responsible for compliance should be asking:

- In a random sample of 10 devices, what applications and executables will an auditor find?
- Can you quickly provide explanations for why each application is running on each device?
- Can you demonstrate that outdated or insecure software is identified and blocked or updated across the organization?
- How are removable storage devices tracked and controlled to prevent unauthorized access to protected data?
- How do you prove ongoing and effective communications regarding your compliance policies?

ONGOING POLICY AWARENESS AND ENFORCEMENT

Bit9 provides organizations with the ability to communicate and enforce compliance policies as part of Business As Usual, adding a higher level of awareness and proof of compliance to the policy in question. Using Bit9's templates, end users can be stopped from installing unauthorized software or changing controlled files, while being directed to read and acknowledge their review of applicable corporate compliance and security policies.

POSITIVE DEVICE CONTROL

Portable media devices such as USB memory sticks are everywhere. While useful, they can also store protected information or be used to deliver malicious attacks. Most regulatory standards require organizations to provide evidence electronic media and physical devices are controlled to prevent unauthorized distribution.

Bit9 supports an organization's ability to regulate the use of USB ports and portable media. Device Control options allow administrators to block the use of USB ports on protected devices, or allow only specific, authorized devices.

EXCEPTION REQUESTS AND LOGGING

If exceptions are required, Bit9 provides auditable workflow to request, approve and track these actions. With Bit9's high-enforcement level, an end user is notified when an attempted application installation is outside of the internal security compliance policy. The application is blocked and the end user is notified and requested to both accept and acknowledge the policy. Once the end user clicks the necessary links, instructions or check boxes, he/she is allowed access to the endpoint. All of the associated audit information is archived within the Bit9 repository and is used to produce a full compliance report for the validation process, audit or assessment.

EVIDENCE-BASED COMPLIANCE

Audits are simpler if an organization's controls also provide real-time evidence of compliance – at any time. With Bit9, Compliance Control Policies are simple to create, and provide auditable evidence that the policies are communicated, consumed, enforced and tracked.

Applicable Standards

- PCI - 3.7, 5.4, 7.3, 10.8, 11.6, 12.1
- HIPAA - § 164.308(a)(5)
- NERC - CIP-004-3a (R1)

CONTROL 6 – DEVICE CONTROL

COMPLIANCE GOALS

1. Prevent unauthorized devices from accessing information in the protected environment
2. Prevent protected information from removal or disclosure
3. Provide evidence that compliance policies are communicated and enforced.

DO YOU CONTROL YOUR ENVIRONMENT?

Most regulatory standards require organizations to provide evidence that electronic media and physical devices are controlled. This includes "any other component or device located within or connected to…" the in-scope environment. This protects personal information such as credit cards and personal health information from unauthorized distribution.

While networked storage devices and other authorized components can be physically walled off, these requirements also cover any device within the covered environment, whether it is an authorized storage device or an employee's thumb drive. The ubiquity of the latter along with their ability to not only store data, but to also deliver attacks, makes control of these devices and USB ports critical to maintain compliance.

POSITIVE DEVICE CONTROL

Disabling or blocking all USB ports is an option. However, this could adversely affect conducting your business; authorized employees may need to access data or deliver updates using portable devices. Instead, organizations should have enforceable, auditable policies that control:

- Which authorized removable devices can be used
- Which authorized employees can use a removable device
- Which systems can be accessed by those removable devices

A Compliance Control Policy managed by Bit9 provides organizations with the flexibility to allow authorized users with authorized devices to conduct business, while logging all actions for audit purposes and blocking unauthorized users and devices. Bit9's device control features allow:

- Block writing data to an unapproved removable device
- Block reading data from an unapproved removable device
- Block execution from an unapproved removable device
- Allow, but audit and report, writes, reads an executions from removable devices

GRANULAR AND FLEXIBLE CONTROL

Bit9 provides the control organizations need to meet rigorous compliance standards, with the flexibility needed to meet business goals. Specific devices can be approved by make, model and serial number, and user authentication and authorization can be linked to your Active Directory or LDAP controls. This allows you to block unauthorized access to a USB port, while allowing, tracking and recording authorized access.

BIT9 CONTROLS MALWARE, APPLICATIONS, FILES AND DEVICES

Hundreds of organizations use Bit9's enterprise-ready solution to block malware, gain control over the applications and devices in their environment and manage the integrity of critical files. Building Compliance Control Policies is simple. The Policies enforce and audit all actions in your environment, providing auditors with the required evidence to prove compliance.

Applicable Standards

- PCI – 9.5; 11.5, 10, 12.3
- HIPAA - § 164.310 (d) (1)
- NERC – CIP-007 R2

CONCLUSIONS

Meeting GRC standards across an enterprise, while managing the systems, files and user permissions to meet organizational needs, is a difficult task. Involving the various stakeholders in building Compliance Control Policies educates the organization about what the regulatory requirements are, and importantly, why they are needed.

Locking down single function systems to prevent any unauthorized software from executing (not just known malware) protects these systems from traditional attacks and prevents inadvertent changes that could affect both compliance and security.

Flexibility is also needed. Providing managers and other users with ability to install new software on specific devices allows them to work unimpeded, but with full tracking and auditing of changes from the baseline image.

Finally, the ability to track, audit and act on any changes to the approved baseline – on any device at any time – provides compliance professionals with the ability to comply with multiple regulatory standards, provide evidence of adherence to documented policies and support an organization's business goals.

ABOUT BIT9 + CARBON BLACK

The combination of Bit9 + Carbon Black offers the most complete answer to the newer, more advanced threats and targeted attacks intent on breaching an organization's endpoints. This comprehensive approach makes it easier for organizations to see—and immediately stop—advanced threats. Our solution combines Carbon Black's lightweight endpoint sensor, which can be rapidly deployed with no configuration to deliver "incident response in seconds," and Bit9's industry-leading prevention technologies. Benefits include:

- Continuous, real-time visibility into what's happening on every computer
- Real-time threat detection, without relying on signatures
- Instant response by seeing the full "kill chain" of any attack
- Protection that is proactive and customizable

Bit9 + Carbon Black delivers a comprehensive solution for continuous endpoint threat security. This is why thousands of organizations worldwide—from 25 Fortune 100 companies to small businesses—use our proven solution. The result is increased security, reduced operational costs and improved compliance.

Bit9 + CARBON BLACK

266 Second Avenue
Waltham, MA 02451 USA
P 617.393.7400 F 617.393.7499
www.bit9.com