DATASHEET

Compliance with CloudCheckr

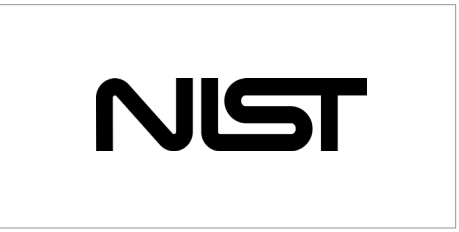
Introduction

Security in the cloud is about more than just monitoring and alerts. To be truly secure in this ephemeral landscape, organizations must take an active approach to assessing their infrastructure, assets, and policies to ensure compliance with regulations like HIPAA, FedRAMP, PCI, and more. Each regulation has its own set of requirements that must be met to achieve and maintain Authority to Operate (ATO)—and staying on top of these mandates can be a full-time job.

Fortunately, there are tools and services from organizations like the Center for Internet Security (CIS) and Allgress that help automate compliance validation. CloudCheckr has partnered with both the CIS and Allgress to make it easier for enterprises to get and stay in compliance. This document illustrates the regulations and standards that the CIS and Allgress track, and some of the specific features of CloudCheckr that can help organizations stay secure.

Who needs to comply?

Compliance is not just for federal organizations. The government has mandated specific standards for companies that work with health data, credit card transactions, or other Controlled Unclassified Information (CUI) such as financial aid information. These regulations work with a “carrot and stick” approach. If you want the opportunity to bid on lucrative government contracts, you will need to meet their standards. On the other hand, organizations that mishandle private information or don’t handle security breaches appropriately face severe penalties.



Compliance Mandates

DFARS (NIST 800-171)

DFARS stands for Defense Federal Acquisition Regulation Supplement. Non-federal organizations that provide services to U.S. Government Agencies such as government contractors; manufacturers; state, local, and tribal governments; colleges and universities; etc. must now provide documentation and evidence as to how they are protecting Controlled Unclassified Information (CUI). Example: Higher Education organizations that process data and provide services to the U.S. government in the form of federal financial aid administration or distribution, grant award for research, or contract award for services.

EXAMPLE 1: MAPPING OF NIST CONTROLS

NIST 171 / 3.1.1: Limit information system access		
Description	**References**	**CloudCheckr Implementation**
Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).	AC-2, AC-3, AC-17	CloudCheckr comes with native support for username/password-based authentication. Upgraded Enterprise plan users gain Single-Sign On (SSO) integration for one of the following SAML 2.0 compliant providers: PingOne, OneLogin, or Okta. Furthermore, combining authentication methods is supported. This provides the ability to allow some users to login via SSO and others a native username/password-based authentication.

HIPAA

HIPAA stands for Health Insurance Portability and Accountability Act and was a major turning point in how private health information could be handled. Developed in 1996, and revised in 2009 and again in 2013, HIPAA coincided with the rise of electronic medical records, when it became increasingly important that such personal data be protected. The constant revisions demonstrate how difficult it is to stay informed, and how important it is to rely on tools that are always up-to-date. HIPAA covers privacy (electronic, written, or oral), security (technical, physical, and administrative), enforcement (responsibilities and penalties), and breach notifications (individuals, HHS Secretary, and media).

Below are a few key monitoring and auditing tasks of the HIPAA-compliant enterprise IT team, and a few ways CloudCheckr helps organizations stay on top of them:

HIPPA Compliance with CloudCheckr

Key Tasks	CloudCheckr Support
Analyze and reduce attack vectors and surface	CloudCheckr offers dynamic environment scanning, port and protocol management, and automatic alerts for vulnerabilities. Scheduled reports offer hierarchical and exportable insights.
Assess the perimeter of the internal private networks	Our platform provides full visibility of VPCs to identify gateways, subnets, DHCP option sets, and more. VPC flow logs and traffic analysis are easily accessible, while CloudCheckr's summary and detailed reports ensure control of your environment.
Manage access control, including role definition, user group permissions, and actions	CloudCheckr simplifies tracking permissions and security groups by automatically mapping and grouping all user accesses. Reporting and alerting allows instantaneous visibility within individual and across multiple accounts. The full history is automatically saved. Users can confidently scale their environment as CloudCheckr ensures that they retain visibility into permissions regardless of scale.
Monitor external and internal threats (attacks and misconfigurations)	The CloudCheckr platform continuous monitors for misconfigurations to ensure infrastructure is stable and secure. Our best practice checks empower administrators to easily address issues and mitigate risks with the click of a button.

FedRAMP
Federal Risk Authorization Management Program

FedRAMP (NIST 800-53)
FedRAMP stands for Federal Risk and Authorization Management Program and regulates what government entities should look for when choosing cloud products and services.

Example 2: Mapping of FedRAMP Audit Controls

NIST 800-53 / Audit Reduction and Report Generation		
Description	**References**	**CloudCheckr Implementation**
The information system provides an audit reduction and report generation capability that:	AU-7	CloudCheckr offers user-defined detailed and summary reporting, across multiple cloud resource groups available on service and granular levels. Reports are fully customizable, with filtering, sorting, and export capabilities and automated controls are available. Audit records contain unalterable information, time stamp, and sequencing.

PCI

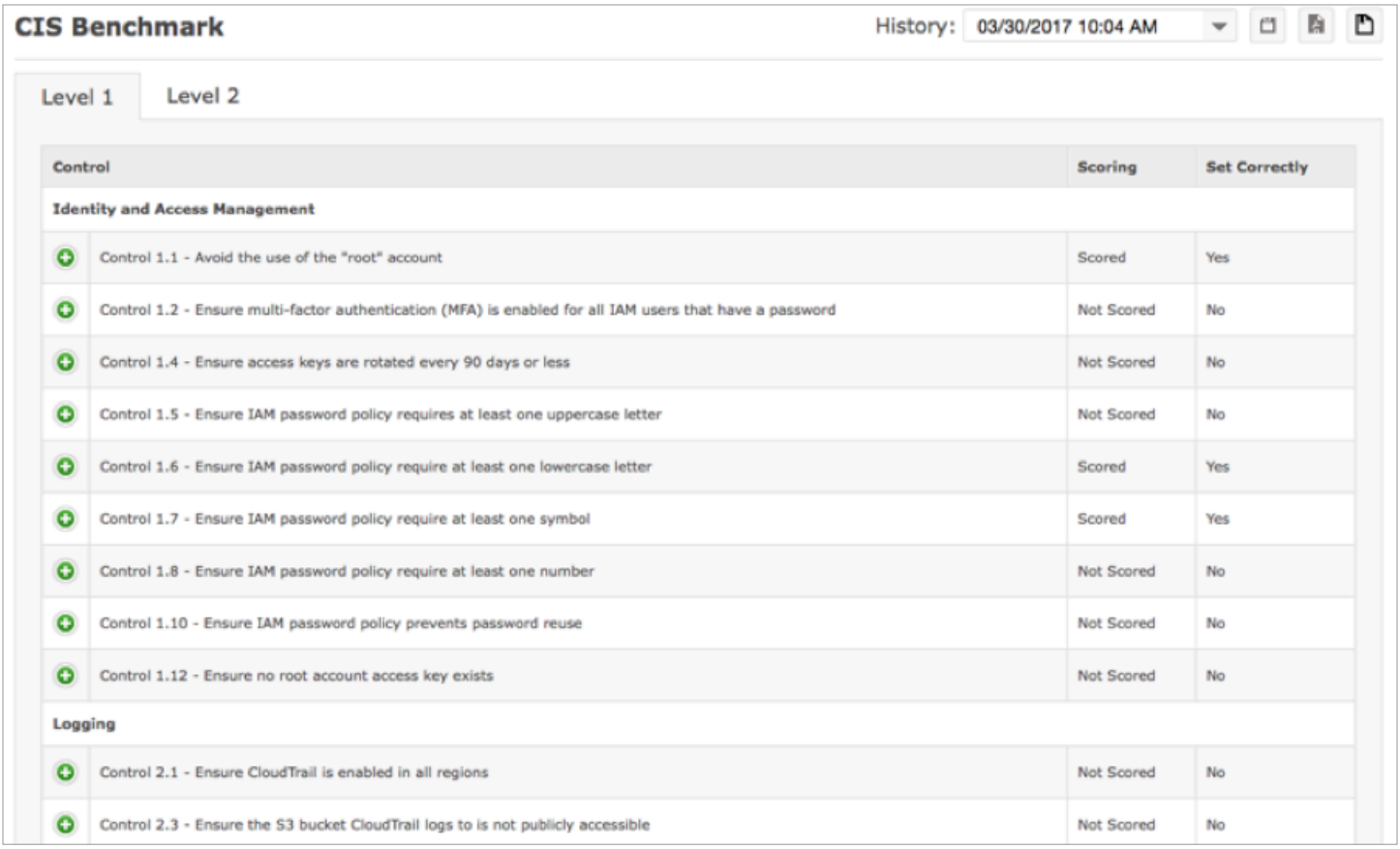
PCI is the security standard of the Payment Card Industry to ensure security of payment card information and monitor threats. Unlike federal regulations, PCI was created by a consortium including American Express, Discover, JCB International, MasterCard and Visa Inc. PCI is designed to protect customers as well as merchants and financial institutions.

Partners In Cloud Compliance

Center for Internet Security (CIS)

The Center for Internet Security was established by and is comprised of government agencies, colleges and universities, nonprofits, enterprises, IT consultants, and product vendors. Hundreds of security professionals worldwide have worked together to develop the CIS Benchmarks, a set of Best Practices covering operating systems, software and network devices.

CIS Benchmarks for cloud security are automatically integrated with the CloudCheckr's CIS Benchmark Report to ensure organizations are following best practices to be compliant with FISMA, PCI, HIPAA, and other regulations.



Control	Scoring	Set Correctly
Identity and Access Management		
Control 1.1 - Avoid the use of the "root" account	Scored	Yes
Control 1.2 - Ensure multi-factor authentication (MFA) is enabled for all IAM users that have a password	Not Scored	No
Control 1.4 - Ensure access keys are rotated every 90 days or less	Not Scored	No
Control 1.5 - Ensure IAM password policy requires at least one uppercase letter	Not Scored	No
Control 1.6 - Ensure IAM password policy require at least one lowercase letter	Scored	Yes
Control 1.7 - Ensure IAM password policy require at least one symbol	Scored	Yes
Control 1.8 - Ensure IAM password policy require at least one number	Not Scored	No
Control 1.10 - Ensure IAM password policy prevents password reuse	Not Scored	No
Control 1.12 - Ensure no root account access key exists	Not Scored	No
Logging		
Control 2.1 - Ensure CloudTrail is enabled in all regions	Not Scored	No
Control 2.3 - Ensure the S3 bucket CloudTrail logs to is not publicly accessible	Not Scored	No

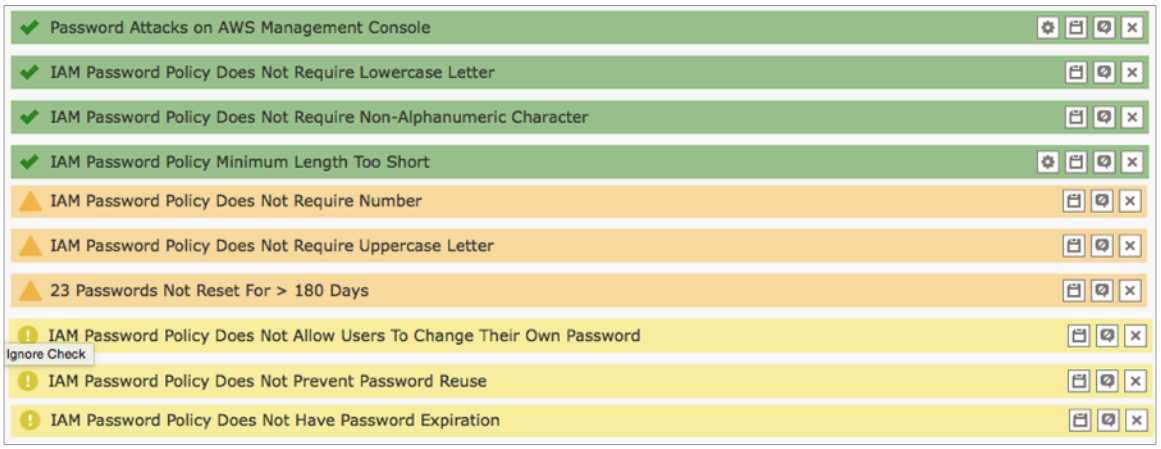
Allgress

Allgress is a commercial security software vendor that has made available, for free, their Allgress Regulatory Product Mapping (RPM) Tool. This graphical tool demonstrates all of the required controls for a particular regulation. The RPM Tool allows filtering by security vendor to see what controls are met by a particular vendor. Typically, no single software vendor can meet all the needs of a particular regulation, since many controls deal with items that don't specifically relate to software, such as physical security, training, off-site storage. However, it's best to find a vendor that meets as many of the software-specific controls as possible. This ensures a higher level of accountability and overall control of your environment.

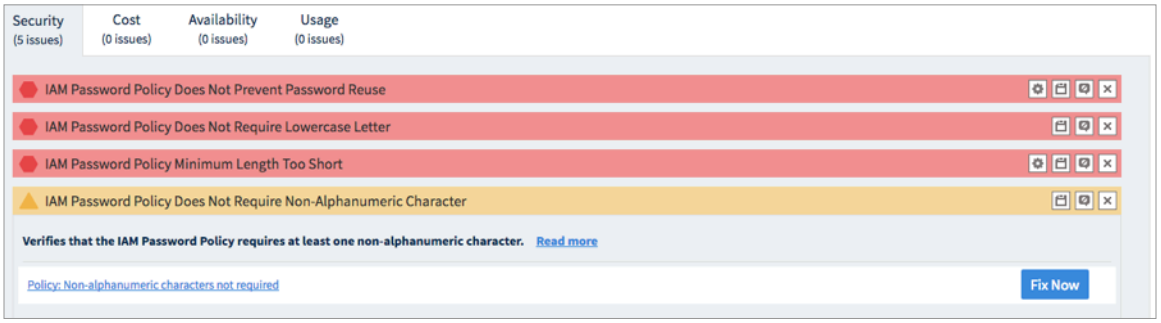
CloudCheckr is featured in the Allgress RPM Tool, covering more controls than any other partner with 41 of 130 security controls.

Regulation	# of Controls Met by CloudCheckr
DFARS (NIST 800-171)	41
FedRAMP (NIST 800-53)	41
PCI	14

CloudCheckr comes with over 450 Best Practice Checks, many of which map directly to regulatory Controls. For example, there are ten checks dedicated to ensuring an organization is enforcing a secure password policy, a key requirement for any security regulation.



Alerts are only part of the solution. Many of CloudCheckr's Best Practice Checks come with a "Fix Now" button. This enables the administrator to fix the configuration issue without any extra steps. In fact, some of these fixes can be automated via "AutoFix" so the very moment a Best Practice Check discovers a violation, it will be fixed, automatically. The promise of continuous, automated compliance is a reality with CloudCheckr.



About CloudCheckr

The CloudCheckr platform offers a single pane of glass across infrastructure to ensure total security and compliance, while optimizing cost and expenses. With continuous monitoring, 450 best practice checks, and built-in automation, CloudCheckr helps organizations to ensure compliance for highly regulated industries, with alerts, monitoring, and audits to meet FedRAMP, DFARS, HIPAA, PCI, and other security standards. With deeper intelligence across cloud infrastructure and a unified cloud management solution, organizations can prevent risks and mitigate threats before they occur. Get started at cloudcheckr.com/getstarted.

VISIT US ONLINE