CloudCheckr

DFARS (NIST-171) Mapping
with CloudCheckr

Amazon Web Services (AWS), combined with the Security and Compliance capabilities of CloudCheckr, represent a formidable force for meeting the DFARS (NIST-171) standard. CloudCheckr is an AWS Advanced Technology Partner with both AWS Government and Security Competency certifications. This document illustrates the specific features of CloudCheckr that can help organizations comply with DFARS.

Who needs to comply?

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.

About CloudCheckr

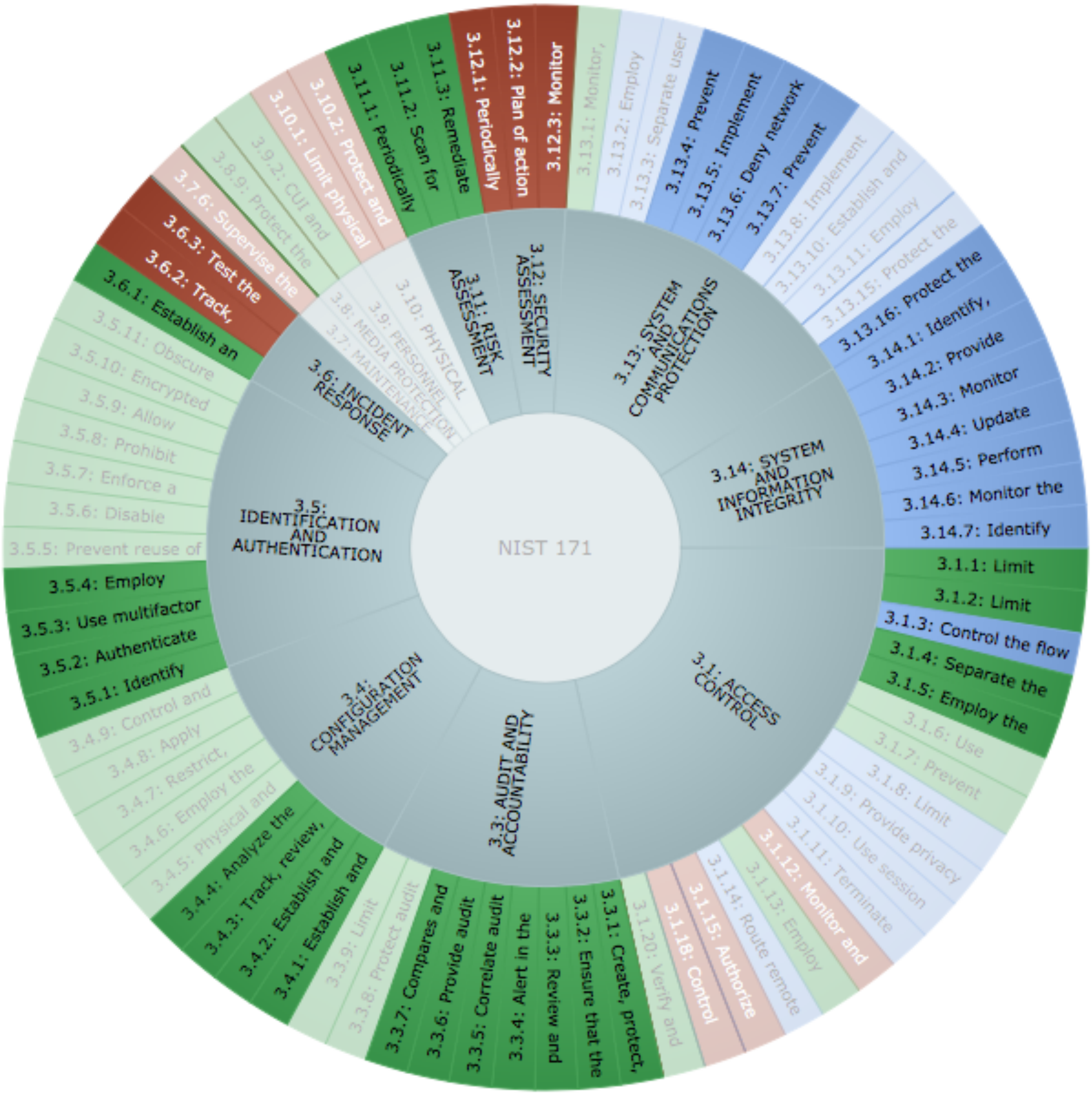
The CloudCheckr platform offers a single pane of glass across infrastructure to ensure total security and compliance, while optimizing cost and expenses. With continuous monitoring, 450 best practice checks, and built-in automation, CloudCheckr helps organizations to ensure compliance for highly regulated industries, with alerts, monitoring, and audits to meet NIST, 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**.

CloudCheckr

Allgress Regulatory Product Mapping Diagram

CloudCheckr Mappings for NIST 800-171



DFARS NIST-171 Requirements – CloudCheckr Mapping

NIST 171 / 3.1.1: Limit information system access

Description	References
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 Implementation
CloudCheckr comes with native support for username/password-based authentication for all pricing plans/tiers. By upgrading to the Enterprise plan, your organization will gain Single-Sign On (SSO) integration for one of the following SAML 2.0 compliant providers: PingOne, OneLogin, or Okta. This allows you to meet the security requirements of your organization by utilizing the various authentication options made available. Furthermore combining authentication methods is supported. This provides the ability to allow some users to login via SSO and others to use the native username/password-based authentication. Please be aware that the ability to use another SSO Provider may require additional customizations of CloudCheckr. Please contact sales (sales@cloudcheckr.com) for inquiries regarding support for SAML 2.0 compliant SSO Providers not listed. ENABLING & CONFIGURING SSO In order to enable Single Sign On, please contact a Support Engineer at support@cloudcheckr.com, who will start you out and guide you through the setup process. During this easy process, you will work with our Support Engineer to: Generate IdP metadata. Choose a default Role for any new users created by SSO. Validate that the authentication process is working smoothly with your environment. Please note: CloudCheckr's authentication is IdP-initiated, rather than SP-initiated. CloudCheckr will provision your users upon first-time logon, but it will still be your responsibility to enable specific permissions and account access for your CloudCheckr users. You can get more info on the user management process at the User Management and User Groups pages. See the following guides for configuring SSO in CloudCheckr using one of the natively supported SAML 2.0 compliant SSO providers. **PingOne:** http://support.cloudcheckr.com/single-sign-on-setup-pingone/ **OneLogin:** http://support.cloudcheckr.com/single-sign-on-setup-onelogin/ **Okta:** http://support.cloudcheckr.com/single-sign-on-setup-okta/ **Google:** http://support.cloudcheckr.com/single-sign-on-setup-google/ Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues. CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report.

NIST 171 / 3.1.2: Limit information system access

Description	References
Limit information system access to the types of transactions and functions that authorized users are permitted to execute.	AC-2, AC-3, AC-17

CloudCheckr Implementation

CloudCheckr comes with native support for username/password-based authentication for all pricing plans/tiers. By upgrading to the Enterprise plan, your organization will gain Single-Sign On (SSO) integration for one of the following SAML 2.0 compliant providers: PingOne, OneLogin, or Okta. This allows you to meet the security requirements of your organization by utilizing the various authentication options made available. Furthermore combining authentication methods is supported. This provides the ability to allow some users to login via SSO and others to use the native username/password-based authentication. Please be aware that the ability to use another SSO Provider may require additional customizations of CloudCheckr. Please contact sales (sales@cloudcheckr.com) for inquiries regarding support for SAML 2.0 compliant SSO Providers not listed.

ENABLING & CONFIGURING SSO In order to enable Single Sign On, please contact a Support Engineer at support@cloudcheckr.com, who will start you out and guide you through the setup process. During this easy process, you will work with our Support Engineer to: Generate IdP metadata. Choose a default Role for any new users created by SSO. Validate that the authentication process is working smoothly with your environment. Please note: CloudCheckr's authentication is IdP-initiated, rather than SP-initiated. CloudCheckr will provision your users upon first-time logon, but it will still be your responsibility to enable specific permissions and account access for your CloudCheckr users. You can get more info on the user management process at the User Management and User Groups pages. See the following guides for configuring SSO in CloudCheckr using one of the natively supported SAML 2.0 compliant SSO providers.

PingOne: http://support.cloudcheckr.com/single-sign-on-setup-pingone/
OneLogin: http://support.cloudcheckr.com/single-sign-on-setup-onelogin/
Okta: http://support.cloudcheckr.com/single-sign-on-setup-okta/
Google: http://support.cloudcheckr.com/single-sign-on-setup-google/

Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues. CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view.

Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report.

NIST 171 / 3.1.3: Control the flow of CUI in accordance with approved authorizations

Description	References
Control the flow of CUI in accordance with approved authorizations.	AC-4
CloudCheckr Implementation	
Within CloudCheckr you can set up your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues. CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report. CloudCheckr also integrates with AWS CloudTrail which provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities.	

NIST 171 / 3.1.4: Separate the duties of individuals

Description	References
Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	AC-5
CloudCheckr Implementation	
CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report.	

NIST 171 / 3.1.5: Employ the principle of least privilege

Description	References
Employ the principle of least privilege, including for specific security functions and privileged accounts.	AC-6, AC-6(1), AC-6(5)
CloudCheckr Implementation	
CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Reference: 1. http://cloudcheckr.com/wp-content/uploads/2015/09/Using-CloudCheckr-to-Secure-Amazon-Web-Services.pdf	

NIST 171 / 3.3.1: Create, protect, and retain information system audit records

Description	References
Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity.	AU-2,AU-3, AU-3(1), AU-6, AU-12
CloudCheckr Implementation	
CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.	

NIST 171 / 3.3.2: Ensure that the actions of individual information system users

Description	**References**
Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	AU-2, AU-3, AU-3(1), AU-6, AU-12
CloudCheckr Implementation	
CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.	

NIST 171 / 3.3.3: Review and update audited events.

Description	**References**
Review and update audited events.	AU-2(3)
CloudCheckr Implementation	
CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.	

NIST 171 / 3.3.4: Alert in the event of an audit process failure.

Description	**References**
Alert in the event of an audit process failure.	AU-5
CloudCheckr Implementation	
CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.	

NIST 171 / 3.3.5: Correlate audit review, analysis, and reporting processes

Description	**References**
Correlate audit review, analysis, and reporting processes for investigation and response to indications of inappropriate, suspicious, or unusual activity.	AU-6(3)
CloudCheckr Implementation	
CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.	

NIST 171 / 3.3.6: Provide audit reduction and report generation

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Provide audit reduction and report generation to support on-demand analysis and reporting.</td><td>AU-7</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.</td></tr>
</table>

NIST 171 / 3.3.7: Compares and synchronizes internal system clocks

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Provide an information system capability that compares and synchronizes internal system clocks with an authoritative source to generate time stamps for audit records.</td><td>AU-8, AU-8(1)</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">CloudTrail provides activity monitoring capability for the AWS management plane. CloudTrail records every call into the AWS API. Everything done in AWS is accomplished using the API, including when tools such as the AWS Management Console are used. So you can be confident any activity taken in AWS is recorded into the CloudTrail logs. CloudTrail logs are written into an S3 bucket as JSON files. A separate file is written every five minutes. Additionally, a different file is created for each AWS account and each region. Realistically, looking directly into the CloudTrail files is not a practical task. You need to use a tool to consume and understand what is contained in these files. The CloudTrail UI provides basic functionality to look up events for up to seven days, but undoubtedly you will require access to events from prior periods or more powerful search capabilities. One of the easiest ways to keep track of your CloudTrail configuration is by using the CloudCheckr Best Practice checks.</td></tr>
</table>

NIST 171 / 3.4.1: Establish and maintain baseline configurations

Description	References
Establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles.	CM-2, CM-6, CM-8, CM-8(1)

CloudCheckr Implementation
CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.

NIST 171 / 3.4.2: Establish and enforce security configuration settings

Description	References
Establish and enforce security configuration settings for information technology products employed in organizational information systems.	CM-2, CM-6, CM-8, CM-8(1)

CloudCheckr Implementation
CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.

NIST 171 / 3.4.3: Track, review, approve/disapprove, and audit changes

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Track, review, approve/disapprove, and audit changes to information systems.</td><td>CM-3</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.</td></tr>
</table>

NIST 171 / 3.4.4: Analyze the security impact of changes prior to implementation.

Description	References
Analyze the security impact of changes prior to implementation.	CM-4

CloudCheckr Implementation

CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.

NIST 171 / 3.5.1: Identify information system users

Description	References
Identify information system users, processes acting on behalf of users, or devices.	IA-2, IA-5

CloudCheckr Implementation

Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues.

For each of the AWS accounts you will be monitoring, you will need to configure read-only access for CloudCheckr. There are two methods to do this:

1. Create an Access Key and a Secret Key for each AWS account. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with-cloudcheckr/adding- credentials-in-cloudcheckr/creating-an-aws-user-group-and-policy/

2. Create a trust relationship from each account to our Cross-Account Role. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with- cloudcheckr/adding-credentials-in-cloudcheckr/cross-account-roles/ After configuring an AWS account in CloudCheckr, you can click the Update button and CloudCheckr will begin monitoring your AWS account and building reports based on its findings.

NIST 171 / 3.5.2: Authenticate (or verify) the identities of those users, processes, or devices

Description	References
Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	IA-2, IA-5

CloudCheckr Implementation

Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues.

For each of the AWS accounts you will be monitoring, you will need to configure read-only access for CloudCheckr. There are two methods to do this:

1. Create an Access Key and a Secret Key for each AWS account. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with-cloudcheckr/adding- credentials-in-cloudcheckr/creating-an-aws-user-group-and-policy/

2. Create a trust relationship from each account to our Cross-Account Role. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with- cloudcheckr/adding-credentials-in-cloudcheckr/cross-account-roles/ After configuring an AWS account in CloudCheckr, you can click the Update button and CloudCheckr will begin monitoring your AWS account and building reports based on its findings.

NIST 171 / 3.5.3: Use multifactor authentication

Description	References
Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts.	IA-2(1), IA-2(2), IA-2(3), IA-2(8), IA-2(9)

CloudCheckr Implementation

Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues. For each of the AWS accounts you will be monitoring, you will need to configure read-only access for CloudCheckr.

There are two methods to do this:

1. Create an Access Key and a Secret Key for each AWS account. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with-cloudcheckr/adding- credentials-in-cloudcheckr/creating-an-aws-user-group-and-policy/

2. Create a trust relationship from each account to our Cross-Account Role. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with- cloudcheckr/adding-credentials-in-cloudcheckr/cross-account-roles/ After configuring an AWS account in CloudCheckr, you can click the Update button and CloudCheckr will begin monitoring your AWS account and building reports based on its findings. CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report.

NIST 171 / 3.5.4: Employ replay-resistant authentication mechanisms

Description	References
Employ replay-resistant authentication mechanisms for network access to privileged and non-privileged accounts.	IA-2(8), IA-2(9), IA-4
CloudCheckr Implementation	
Within CloudCheckr you can setup your AWS accounts to enable you to view security details, reports, and a complete inventory of resources. You will need to register each of your AWS accounts in CloudCheckr. Start by gathering up a list of all the AWS accounts that you will need to monitor for security issues. For each of the AWS accounts you will be monitoring, you will need to configure read-only access for CloudCheckr. There are two methods to do this: 1. Create an Access Key and a Secret Key for each AWS account. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with-cloudcheckr/adding- credentials-in-cloudcheckr/creating-an-aws-user-group-and-policy/ 2. Create a trust relationship from each account to our Cross-Account Role. For instructions on this, click this link: http://support.cloudcheckr.com/getting-started-with- cloudcheckr/adding-credentials-in-cloudcheckr/cross-account-roles/ After configuring an AWS account in CloudCheckr, you can click the Update button and CloudCheckr will begin monitoring your AWS account and building reports based on its findings. CloudCheckr allows you to tag AWS accounts and map those together to create groups of AWS accounts. These groups are known in CloudCheckr as Multi-Account Views. You can also create a Multi- Account View for all AWS accounts, from which you can see all your AWS accounts (and best practice checks) in a single view. Follow the steps here (http://support.cloudcheckr.com/cloudcheckr-project-tag-userguide/) to get your Multi-Account Views up and running. Once that is completed, best practice checks will be pulled from all the tagged AWS accounts into a single Best Practices report.	

NIST 171 / 3.6.1: Establish an operational incident-handling capability

Description	References
Establish an operational incident-handling capability for organizational information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities.	IR-2, IR-4, IR-4, IR-5, IR-6, IR-7

CloudCheckr Implementation
CloudCheckr has alerting capabilities specifically for CloudTrail events. These can be found under the Alerts section in the left hand navigation bar. We have included built-in alerts which are designed to help you keep track of the security of your account. To enable these, simply flip the toggle to “On”. If you click on the alert you can specify an email address, PagerDuty key, or SNS topic that the alert will be sent to. Below is a sample list of our built-in alerts along with their descriptions. Review the list and enable the built-in alerts that are critical or high importance levels. Review the other built-in alerts to determine if they are important to your security team. Using CloudTrail Logs to Investigate Activity When you find yourself needing to track down who did what in an AWS account, having to use the AWS Management Console or manually read through the CloudTrail logs is impractical. For instance, say you want to see all the IAM users that have been added in the past month to an AWS account. It is entirely impractical to look through all the log files to find the event CreateUser. Search capability like this requires loading data into a database that can be queried. Another example: assume that you need to find all IAM policy modifications for the past three months in a specific AWS account. To effectively do this you must first gather up all the AWS events that would result in an IAM policy modification. Next, you would have to find a way to search over 200,000 CloudTrail files (a new file every 5 minutes to 9 different regions). When investigating activity in an AWS account, we recommend starting with the Security/CloudTrail/Common Searches report. Similar to CloudTrail built-in alerts, this screen is compiled of search options which will help guide you to picking the right options to filter by. This page includes the following searches: 1. Find who created, started, stopped, terminated an EC2 Instance 2. Find AWS management console login attempts 3. Find unauthorized access attempts 4. Find all activity for a specific IAM user 5. Find all activity for a specific IP address 6. Find IAM users created in a time period For example, if we wanted to see the data from the last option, “Find IAM users created during a time period”, select the date and the hour to begin the search and the date and the hour to end the search and select ‘Search’. CloudCheckr will translate this into the event CreateUser. The results will show any IAM user created during that time span.

NIST 171 / 3.6.2: Track, document, and report incidents

Description	References
Track, document, and report incidents to appropriate organizational officials and/or authorities.	IR-2, IR-4, IR-4, IR-5, IR-6, IR-7

CloudCheckr Implementation

CloudCheckr has alerting capabilities specifically for CloudTrail events. These can be found under the Alerts section in the left hand navigation bar. We have included built-in alerts which are designed to help you keep track of the security of your account. To enable these, simply flip the toggle to "On". If you click on the alert you can specify an email address, PagerDuty key, or SNS topic that the alert will be sent to. Below is a sample list of our built-in alerts along with their descriptions. Review the list and enable the built-in alerts that are critical or high importance levels. Review the other built-in alerts to determine if they are important to your security team. Using CloudTrail Logs to Investigate Activity When you find yourself needing to track down who did what in an AWS account, having to use the AWS Management Console or manually read through the CloudTrail logs is impractical.

For instance, say you want to see all the IAM users that have been added in the past month to an AWS account. It is entirely impractical to look through all the log files to find the event CreateUser. Search capability like this requires loading data into a database that can be queried. Another example: assume that you need to find all IAM policy modifications for the past three months in a specific AWS account. To effectively do this you must first gather up all the AWS events that would result in an IAM policy modification. Next, you would have to find a way to search over 200,000 CloudTrail files (a new file every 5 minutes to 9 different regions). When investigating activity in an AWS account, we recommend starting with the Security/CloudTrail/Common Searches report. Similar to CloudTrail built-in alerts, this screen is compiled of search options which will help guide you to picking the right options to filter by.

This page includes the following searches:

1. Find who created, started, stopped, terminated an EC2 Instance
2. Find AWS management console login attempts
3. Find unauthorized access attempts
4. Find all activity for a specific IAM user
5. Find all activity for a specific IP address
6. Find IAM users created in a time period For example, if we wanted to see the data from the last option, "Find IAM users created during a time period", select the date and the hour to begin the search and the date and the hour to end the search and select 'Search'. CloudCheckr will translate this into the event CreateUser. The results will show any IAM user created during that time span.

NIST 171 / 3.6.3: Test the organizational incident response capability.

Description	References
Test the organizational incident response capability.	IR-3, IR-3(2)

CloudCheckr Implementation

Testing/Auditing Security Groups Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups.

The two main network security controls in AWS are Security Groups and Network ACLs.

1. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules.
2. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured. The security department can start by reviewing best practice checks. Setup a Multi-Account View to include all AWS accounts, and allow time for the Multi-Account View to collect all results across the accounts.

We recommend looking across your entire organization for any issues with the best practice checks below:

1. EC2-VPC Security Groups Inbound Rules Set To All IPs And All Ports
2. EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports
3. DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address
4. Redshift Security Groups Inbound Rules Allowing Traffic From Any IP Address These checks are finding Security Groups that have no limitations on access at all. A no limitations setting is rarely appropriate. It's highly recommended that you prohibit this as a corporate policy and then monitor for someone inadvertently configuring a group with it. Chances are that many of your AWS accounts will have many of these by default. The results of these best practice checks look like this: 1. Group: StandaloneSG | ID: sg-4c82c17f | Port Range: 80,443,0-ALL,8-ALL | Instances using this security group: 2 | Region: US West (Oregon) The results contain the number of instances using this Security Group so you can prioritize which ones to track down and shutdown first. Many security groups may be overly-permissive, but might not be assigned to any resources. It is recommended you remove these, but you might prioritize these below fixing security groups that are wide-open and have resources assigned to them. As well, for each result you will see "X Ignore Item". If you deem that it is appropriate for a specific security group to be wide open, you can choose to ignore this result. You can always resume monitoring the specific security group later if needed by selecting the "Show Ignore" checkbox above.

NIST 171 / 3.11.1: Periodically assess the risk to organizational operations

Description	References
Periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of CUI.	RA-3

CloudCheckr Implementation
Reviewing the Perimeter of your AWS Environment Moving from a data center to the public cloud requires rethinking how you do assessments of your perimeter security. For this reason CloudCheckr provides the Perimeter Assessment Report. This report will give you information on any publicly accessible resource in each of the available AWS regions. You can find this report under Security/Perimeter Assessment. Within this report, a + symbol next to a region indicates that there are publicly accessible resources within that region. If you expand a region, it will show you which AWS services have publicly accessible resources and, if you expand the service, it will give you the specific resource and details on the controls around the service and resources. Resources may be intentionally public. For instance, a web server may well require open access to the Internet. This report helps you to gather the complete list to review and ensure ONLY what is meant to be exposed is. We suggest you review this report and validate any publicly accessible resources are meant to be exposed as such. Within each region, you will see the list of publicly accessible resources not within a VPC. Verify each and the security groups associated with them to make sure they are appropriately restricted. Ideally you would move resources that can be run from within a VPC into a VPC. These resources types include EC2, RDS, Redshift, Elastic IPs, and ElastiCache. Some resources, such as S3 and DynamoDB, can't be moved into a VPC. You will also see the VPCs that are publicly accessible. Underneath the VPC you can review the NACL to see which rules are allowing public access on which ports. One level down, CloudCheckr lists the Subnets within each VPC, and the public resources within each subnet. Additionally, CloudCheckr will show the list of security group rules associated with the instances. This is a lot of information, but it gives you a way to pull all the various controls (VPCs, Security groups, public IP addresses) into a single place to understand if and how access to a resource is restricted (or not). As we stated earlier, before an application goes into production, you should review the security configuration, starting with Security Best Practice checks. You should also review the privileges and access controls of all the components of the resources. The perimeter assessment report is a good way to start. Get an inventory of the resources from the application team, including the S3 buckets, list of databases, VPCs being used, EC2 instances, auto scaling groups, etc. From this list you use the Perimeter Assessment report to ensure these resources are not publicly accessible unless they are meant to be. For instance, let's show an example of an application inventory that includes two S3 buckets, one SQS Queue, one RDS database, and five EC2 instances within a VPC. Start by determining the appropriate access of these resources. For instance, one of the S3 buckets might be marketing materials meant to be publicly available to potential customers. The other bucket contains backups of database files. One of the EC2 instances is a webserver and should be available to potential customers over HTTPS on port 443. Open the Perimeter Assessment, expand the region the S3 buckets are within, and verify that only the one S3 bucket shows up under "Publicly Accessible S3 Buckets". Verify that the SQS Queue does not show up under "Publicly Accessible SQS Queues". Next expand the VPC and ensure the RDS database does not show up under "RDS DB instances with a public IP". Check that only the webserver shows up under "EC2 instances with a public IP" and that the security groups of the instance are limited to port 443.

NIST 171 / 3.11.2: Scan for vulnerabilities in the information systems

Description	References
Scan for vulnerabilities in the information system and applications periodically and when new vulnerabilities affecting the system are identified.	RA-5, RA-5(5)
CloudCheckr Implementation	
CloudCheckr provides the Perimeter Assessment Report. This report will give you information on any publicly accessible resource in each of the available AWS regions. You can find this report under Security/Perimeter Assessment. Within this report, a + symbol next to a region indicates that there are publicly accessible resources within that region. If you expand a region, it will show you which AWS services have publicly accessible resources and, if you expand the service, it will give you the specific resource and details on the controls around the service and resources. Resources may be intentionally public. For instance, a web server may well require open access to the Internet. This report helps you to gather the complete list to review and ensure ONLY what is meant to be exposed is. We suggest you review this report and validate any publicly accessible resources are meant to be exposed as such.	

NIST 171 / 3.11.3: Remediate vulnerabilities

Description	References
Remediate vulnerabilities in accordance with assessments of risk.	RA-5
CloudCheckr Implementation	
CloudCheckr provides the Perimeter Assessment Report. This report will give you information on any publicly accessible resource in each of the available AWS regions. You can find this report under Security/Perimeter Assessment. Within this report, a + symbol next to a region indicates that there are publicly accessible resources within that region. If you expand a region, it will show you which AWS services have publicly accessible resources and, if you expand the service, it will give you the specific resource and details on the controls around the service and resources. Resources may be intentionally public. For instance, a web server may well require open access to the Internet. This report helps you to gather the complete list to review and ensure ONLY what is meant to be exposed is. We suggest you review this report and validate any publicly accessible resources are meant to be exposed as such.	

NIST 171 / 3.12.1: Periodically assess the security controls

Description	References
Periodically assess the security controls in organizational information systems to determine if the controls are effective in their application.	CA-2, CA-5, CA-7

CloudCheckr Implementation

Testing/Auditing Security Groups Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups.

The two main network security controls in AWS are Security Groups and Network ACLs.
1. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules.
2. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured. The security department can start by reviewing best practice checks. Setup a Multi-Account View to include all AWS accounts, and allow time for the Multi-Account View to collect all results across the accounts.

We recommend looking across your entire organization for any issues with the best practice checks below:

1. EC2-VPC Security Groups Inbound Rules Set To All IPs And All Ports
2. EC2-Classic Security Groups Inbound Rules Allowing Traffic from All IPs and All Ports
3. DB Security Groups Inbound Rules Set To Allow Traffic From Any IP Address
4. Redshift Security Groups Inbound Rules Allowing Traffic From Any IP Address These checks are finding Security Groups that have no limitations on access at all. A no limitations setting is rarely appropriate. It's highly recommended that you prohibit this as a corporate policy and then monitor for someone inadvertently configuring a group with it. Chances are that many of your AWS accounts will have many of these by default.

The results of these best practice checks look like this: 1. Group: StandaloneSG | ID: sg-4c82c17f | Port Range: 80,443,0-ALL,8-ALL | Instances using this security group: 2 | Region: US West (Oregon) The results contain the number of instances using this Security Group so you can prioritize which ones to track down and shutdown first. Many security groups may be overly-permissive, but might not be assigned to any resources. It is recommended you remove these, but you might prioritize these below fixing security groups that are wide-open and have resources assigned to them. As well, for each result you will see "X Ignore Item". If you deem that it is appropriate for a specific security group to be wide open, you can choose to ignore this result. You can always resume monitoring the specific security group later if needed by selecting the "Show Ignore" checkbox above. You can also perform ad hoc searches of Security Groups from CloudCheckr. For instance, you should audit your security groups to verify public access to common database ports are shutdown. You can do this within the report Security/Security Groups/Common Searches. Option 2 is labeled "Find Security Groups that allow database access from all IP Addresses". Click "Search" and you will have a list of Security Groups that match the search filter. Analyzing Network ACLs Network ACLs are the firewalls of the VPC. You can set rules that allow or deny access to a port or IP range in a NACL. NACLs have some advantages over Security Groups. For instance, rules applied to NACLs are guaranteed to cover all resources in the subnet, whereas a Security Group applies only to the instances it is explicitly applied to it. Relying on Security Groups exclusively is problematic because someone could inadvertently create an EC2 instance in the VPC and associate an improper Security Group to it, leading to it being compromised. This creates an attack point into your VPC that can be used to leapfrog to other instances in the VPC even if they do not have public IP addresses. The disadvantage of NACLs is that they are stateless. If you allow traffic into a subnet, you must specifically allow the outbound traffic for the ephemeral ports of the return traffic. This can be complex to manage and requires opening large ranges of ports. Read more on this topic here: http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_ACLs.html CloudCheckr provides capabilities to search NACLs to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with dozens of VPCs. The security team should be reviewing the NACLs of all VPCs to make sure they are appropriately configured. The security department can start by reviewing best practice checks. Setup a Multi-Account View to include all AWS accounts and allow time for the Multi-Account View to collect all results across the accounts. We recommend looking across your entire organization for any issues with the best practice checks below: 1. Network ACLs Allowing All Inbound Traffic 2. Ineffective Network ACL Deny rule The first check finds NACLs that have no limitations on access at all. This is rarely appropriate. t's highly recommended that you prohibit this as a corporate policy and then monitor for someone inadvertently configuring one. Chances are that your AWS accounts will have many of these by default. The results of this best practice checks look like this: Network ACL ID: acl-b6b390d3 | VPC: vpc-d5361ab0 | Region: US East (Northern Virginia) | Rule #: 100 | Port Range: ALL | IP Range: 0.0.0.0/0 | Type: ALLOW Inbound

NIST 171 / 3.12.2: Plan of action for vulnerabilities

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems.</td><td>CA-2, CA-5, CA-7</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment.</td></tr>
</table>

NIST 171 / 3.12.3: Monitor information system security controls

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.</td><td>CA-2, CA-5, CA-7</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment.</td></tr>
</table>

NIST 171 / 3.13.4: Prevent unauthorized and unintended information transfer

Description	References
Prevent unauthorized and unintended information transfer via shared system resources.	SC-4
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups. The two main network security controls in AWS are Security Groups and Network ACLs. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured.	

NIST 171 / 3.13.5: Implement subnetworks for publicly accessible system components

Description	References
Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.	SC-7
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups. The two main network security controls in AWS are Security Groups and Network ACLs. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured.	

NIST 171 / 3.13.6: Deny network communications traffic by default

<table>
<tr><th>Description</th><th>References</th></tr>
<tr><td>Deny network communications traffic by default and allow network communications traffic by exception (i.e., deny all, permit by exception).</td><td>SC-7(5)</td></tr>
<tr><th colspan="2">CloudCheckr Implementation</th></tr>
<tr><td colspan="2">The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups. The two main network security controls in AWS are Security Groups and Network ACLs. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured.</td></tr>
</table>

NIST 171 / 3.13.7: Prevent remote devices from simultaneously establishing non-remote connections

Description	References
Prevent remote devices from simultaneously establishing non-remote connections with the information system and communicating via some other connection to resources in external networks.	SC-7(7)
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Security groups are one of the primary methods used for securing traffic to an EC2 instance, RDS database, Redshift cluster, or ElastiCache cluster. EC2-VPC Security groups can be used to secure any of these resources if they sit in a VPC. If any of these resources are outside of a VPC, you must use security groups that are specific to the resource type. For instance, for RDS you would have to use DB Security Groups. The two main network security controls in AWS are Security Groups and Network ACLs. Security groups: Assigned directly to an instance or resource. Rules are stateful, meaning traffic returned from a valid request is allowed irrelevant of the security rules. Network ACLs: Assigned to an entire subnet in a VPC. Rules are stateless, meaning rules must be defined for return traffic as well. CloudCheckr provides capabilities to search Security Groups to find ones that are wide open or overly-permissive. An organization may have hundreds of AWS accounts with hundreds of Security Groups. The security team should be reviewing these Security Groups to make sure they are appropriately configured.	

NIST 171 / 3.13.16: Protect the confidentiality of CUI at rest.

Description	References
Protect the confidentiality of CUI at rest.	SC-28
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. Network ACLs are the firewalls of the VPC. You can set rules that allow or deny access to a port or IP range in a NACL. NACLs have some advantages over Security Groups. For instance, rules applied to NACLs are guaranteed to cover all resources in the subnet, whereas a Security Group applies only to the instances it is explicitly applied to it. Relying on Security Groups exclusively is problematic because someone could inadvertently create an EC2 instance in the VPC and associate an improper Security Group to it, leading to it being compromised. This creates an attack point into your VPC that can be used to leapfrog to other instances in the VPC even if they do not have public IP addresses.	

NIST 171 / 3.14.1: Identify, report, and correct information

Description	References
Identify, report, and correct information and information system flaws in a timely manner.	SI-2, SI-3, SI-5

CloudCheckr Implementation

CloudCheckr provides capabilities to search NACLs to find ones that are wide open or overly- permissive. An organization may have hundreds of AWS accounts with dozens of VPCs. The security team should be reviewing the NACLs of all VPCs to make sure they are appropriately configured. The security department can start by reviewing best practice checks. Setup a Multi-Account View to include all AWS accounts and allow time for the Multi-Account View to collect all results across the accounts. Once you have CloudTrail enabled properly, you need to begin monitoring it. CloudTrail logs are valuable for forensic purposes, but it is even more importance to monitor the logs to know when something unusual or suspicious happens. In order to monitor CloudTrail, you will need to translate the API events into meaningful terms.

For instance, to monitor for security group changes you need to look for the following list of AWS API events:

- CreateSecurityGroup DeleteSecurityGroup AuthorizeSecurityGroupEgress AuthorizeSecurityGroupIngress
- RevokeSecurityGroupEgress RevokeSecurityGroupIngress CreateCacheSecurityGroup DeleteCacheSecurityGroup
- AuthorizeCacheSecurityGroupIngress RevokeCacheSecurityGroupIngress CreateDBSecurityGroup
- DeleteCacheSecurityGroup AuthorizeDBSecurityGroupIngress RevokeDBSecurityGroupIngress
- CreateClusterSecurityGroup DeleteClusterSecurityGroup AuthorizeClusterSecurityGroupIngress
- RevokeClusterSecurityGroupIngress

In order to effectively know what to look for, you will need a complete and comprehensive list of events to monitor for. As you see in the above example, the hardest part of monitoring is understanding what to monitor for. AWS often offers multiple events that, from a user's perspective, have very similar appearing outcomes.

NIST 171 / 3.14.2: Provide protection from malicious code

Description	References
Provide protection from malicious code at appropriate locations within organizational information systems.	SI-2, SI-3, SI-5

CloudCheckr Implementation

The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.

NIST 171 / 3.14.3: Monitor information system security alerts

Description	References
Monitor information system security alerts and advisories and take appropriate actions in response.	SI-2, SI-3, SI-5
CloudCheckr Implementation	
CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment.	

NIST 171 / 3.14.4: Update malicious code protection

Description	References
Update malicious code protection mechanisms when new releases are available.	SI-3
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.	

NIST 171 / 3.14.5: Perform periodic scans of the information system

Description	References
Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.	SI-3
CloudCheckr Implementation	
The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type. CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment.	

NIST 171 / 3.14.6: Monitor the information system

Description	References
Monitor the information system, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.	SI-4, SI-4(4)
CloudCheckr Implementation	
CloudCheckr provides over 100 security checks for AWS. Out of the box, CloudCheckr will perform a review of the security settings of your AWS management plane and save it into Best Practices results. Access to those results can be reviewed historically to determine when a security issue arose. Users can also manually kick off scans after remediation to verify changes. Using CloudCheckr, the security team can review security for the entire AWS environment. CloudCheckr will automatically generate and distribute daily reports showing how the environment compares to a prepackaged library of security best practice checks. However, for exceptionally large or dynamic environments, managing security reviews for all AWS accounts on a daily basis may be overwhelming. In this case, we recommend setting up your complete AWS environment and monitoring specifically for best practice checks that are marked with an Importance level of High. You can configure CloudCheckr to automatically notify the security team of only those security issues. CloudCheckr can also be setup to review the security in more depth for specific AWS accounts. This may be easier for a security team to manage than attempting for the entire environment. The Best Practices reports shows the details of each issue discover. To find the report, navigate to the Best Practice on the left menu and select the Security tab. Best Practice checks are order and color-coded to their importance level. CloudCheckr will send you nightly updates of new violations discovered thru Best Practice checks. You can customize this email by setting the specific email address, time of the email, Importance levels, and check type.	

NIST 171 / 3.14.7: Identify unauthorized use of the information system.

Description	References
Identify unauthorized use of the information system.	SI-4

CloudCheckr Implementation

CloudCheckr provides capabilities to search NACLs to find ones that are wide open or overly- permissive. An organization may have hundreds of AWS accounts with dozens of VPCs. The security team should be reviewing the NACLs of all VPCs to make sure they are appropriately configured. The security department can start by reviewing best practice checks. Setup a Multi-Account View to include all AWS accounts and allow time for the Multi-Account View to collect all results across the accounts. Once you have CloudTrail enabled properly, you need to begin monitoring it. CloudTrail logs are valuable for forensic purposes, but it is even more importance to monitor the logs to know when something unusual or suspicious happens. In order to monitor CloudTrail, you will need to translate the API events into meaningful terms.

For instance, to monitor for security group changes you need to look for the following list of AWS API events:

- CreateSecurityGroup DeleteSecurityGroup AuthorizeSecurityGroupEgress AuthorizeSecurityGroupIngress
- RevokeSecurityGroupEgress RevokeSecurityGroupIngress CreateCacheSecurityGroup DeleteCacheSecurityGroup
- AuthorizeCacheSecurityGroupIngress RevokeCacheSecurityGroupIngress CreateDBSecurityGroup
- DeleteCacheSecurityGroup AuthorizeDBSecurityGroupIngress RevokeDBSecurityGroupIngress
- CreateClusterSecurityGroup DeleteClusterSecurityGroup AuthorizeClusterSecurityGroupIngress
- RevokeClusterSecurityGroupIngress

In order to effectively know what to look for, you will need a complete and comprehensive list of events to monitor for. As you see in the above example, the hardest part of monitoring is understanding what to monitor for. AWS often offers multiple events that, from a user's perspective, have very similar appearing outcomes.