DATASHEET

AWS MSP Partner Program Validation Checklist v3.2 Mapping

OVERVIEW

The AWS MSP Validation Checklist Mapping is designed to provide CloudCheckr partners with a practical means to validate the functional and operational benefits of CloudCheckr when measured against the AWS MSP v3.2 evaluation metrics. This version reflects the most recent program criteria, with improvements focused on raising the bar for both MSP Partner and Amazon Web Services (AWS) customer experiences.

SCOPE

This validation checklist mapping is meant to respond to the latest version of the AWS MSP evaluation matrix (version 3.2) which was released in January 2018. By definition, the AWS controls are subject to interpretation and revision. This mapping should be used, in conjunction with specific use-case knowledge, to fulfill the listed controls in the manner indicated.

1.0 Business Health

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
1.2 Financial Planning and Reporting	Partner has processes in place for financial planning, including forecasting, budgeting, and review of financial metrics and reports. Evidence must be in the form of records of financial planning and reviews, and records of collection and review of financial metrics.	CloudCheckr can provide AWS financial metrics to assist Partner with providing financial planning reports.

2.0 Partner Capabilities Overview

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
2.1 Company Overview	Partner has a company overview presentation to set the stage for customer conversations as applicable to its AWS MSP practice, in addition to demonstration capabilities. Presentation to contain information about next generation cloud managed services; how managed services are different in an AWS environment vs. traditional on premise or hosted managed services with emphasis on automation enabled by DevOps practices.	CloudCheckr provides presentation slides to supplement a Partner's presentation, covering CloudCheckr's robust history and relationship with AWS.
2.2 Next Generation Managed Service Viewpoint	Partner publicizes how managed services are different in an AWS environment vs. traditional on premises or hosted managed services with emphasis on automation enabled by DevOps practices. Evidence must be in the form of at least 4 examples of public facing materials (websites, blog posts, press articles, videos, etc.) containing information about next generation cloud managed services published within the last 12 months.	CloudCheckr provides web pages, blog articles, videos and webinars discussing the unique aspects of AWS, the Shared Responsibility Model and terminology.

4.0 Business Management

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
4.4 Supplier Management	**4.4.1** Partner has defined processes for selection and evaluation of suppliers (e.g., SaaS vendors or any other third parties to whom activities or services are subcontracted).	CloudCheckr has multiple competencies with AWS and was recognized as AWS re:Invent 2017 Partner of the Year.
	4.4.2 Where Partner uses SaaS solutions for systems that contain customer information or have access to AWS resources, Partner must show that due diligence has been carried out to assess the security compliance of these solutions with a focus on customer privacy and security. Evidence must be in the form of records of supplier selection and evaluation. As evidence of assessment of security compliance, Partner must show SaaS providers' security overview and documentation, authentication and authorization validation, MFA capabilities, overview of availability characteristics, data backup plan, and disaster recovery plan.	CloudCheckr's numerous Security Best Practice Checks include ensuring Multi-Factor Authentication is enabled. These features, combined with process documentation from the Partner, can demonstrate due diligence.
4.5 AWS Support Plan	All AWS accounts in which Partner is managing customer resources have Developer, Business, or Enterprise level of AWS Support. Evidence must be in the form of a list of AWS accounts managed by Partner and each account's corresponding support level.	CloudCheckr can detect the support level of an AWS customer and the associated Partner.

5.0 AWS Billing and Cost Management

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
5.1 AWS Billing and Cost Management Console	Partner uses AWS Billing and Cost Management service. AWS Billing and Cost Management is the service that Partners use to pay their AWS bill, monitor usage, and budget costs. Evidence must be in the form of demonstration of the AWS Billing and Cost Management console, including demonstration of the following capabilities: › Ability to download PDF Invoices from the Billing and Cost Management Console › Ability to enable Billing Reports › Ability to enable Billing Alerts › Ability to manage Cost Allocation Tags › Ability to explain the benefits of Cost Explorer › Ability to manage tax exemptions (when applicable)	The CloudCheckr Billing and Invoicing functionality integrates with the AWS Billing and Cost Management service to provide PDF invoices, billing reports, billing alerts, cost allocation tags, and manage tax exemptions.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
5.2 AWS Account Settings	Partner leverages the AWS Account Settings page to manage up to date contact and security information for both the payer and/or linked account(s) that Partner manages. Evidence must be in the form of demonstration of the Accounts Settings page, including demonstration of the following capabilities: › Ability to update the address information for an AWS Account › Ability to describe and set alternate contacts › Ability to set Security Challenge Questions › Ability to describe how to close an AWS Account › Ability to manage cancellation of services (e.g., Support)	The numerous CloudCheckr Best Practice Checks help ensure the account's contact and security information is up-to-date and managed. Users can be alerted and then they have the responsibility to update the information.
5.3 Third Party Billing Solutions	Partner leverages third-party ISV or Partner developed solutions for billing management and cost optimization to strengthen Partner's ability to provide proactive recommendations to customers.	CloudCheckr is the premier ISV for billing management and cost optimization to empower AWS Partners to provide proactive recommendations to customers.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
5.5 Reseller Partner Rebilling Capabilities	AWS Reseller Partners have the following rebilling capabilities: › Ability to explain the difference between a blended and unblended rate/cost › Ability to explain why rebilling with a blended rate is not advised › Ability to describe the nuances of the Cost and Usage Report, including: - Ability to explain key column names - Ability to show where to find reservation purchases - Ability to show where to find credit allocation • Ability to make billing suggestions based on the report results › Ability to explain how credit benefit is allocated to a consolidated bill › Ability to explain how Reserved Instance benefit is allocated to a consolidated bill	CloudCheckr assists with billing by providing Blended, Unblended, and List Pricing reports and allows the ability to create and add custom charges and apply credits as desired.
5.6 Reseller Account Controls	Partner uses Account Controls, including at least one of the following: › Block spend data › Block access to cost explorer › Prevent account unlinking	CloudCheckr accounts can be configured to restrict access to specific views (e.g. Security, Best Practice Checks, etc.)

6.0 Solution Design Capabilities

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
6.1.3	Details of the system performance, capacity management and availability measurement systems to be put in place to measure success of proposed design	Utilization reports can be generated in PDF and CSV format and emailed as desired.
6.1.4	Assessment of customer's security requirements and procedures with gap identification.	MSPs can leverage CloudCheckr's Best Practice checks and perimeter security assessment for operation verification. As an AWS certified competency partner in Security, with best-in-class configuration audit and security event monitoring, CloudCheckr helps continuously protect and detect the cloud infrastructure attack surface.
6.1.5	Detailed design shows that customer infrastructure is architected as per AWS security best practices as outlined in https://aws.amazon.com/whitepapers/aws-securitybest-practices.	In addition to Inventory reports and perimeter assessment, CloudCheckr provides 500+ Best Practice checks, and CloudTrail alerts for maintenance. Many of CloudCheckr's Security Best Practice Checks are aligned with the Center for Internet Security's compliance requirements.

8.0 Security

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
8.1 Security Management	**8.1.2** Partner has system that provides access to customer resources to its engineers based on the principle of least privilege. A process for defining and maintaining the appropriate level of access is in place. Access to critical or sensitive data (as defined by the customer) is further controlled by multi-factor or quorum authentication with access based alerts.	CloudCheckr can ensure Role-Based Access Control and Multi-Factor Authentication are enabled for IAM accounts.
	8.1.3 Partner has security policies and procedures to protect its customers' systems from attacks.	Partners are encouraged to protect their cloud infrastructure using CloudCheckr's security tools.
	8.1.4 Partner does not administrate AWS accounts by use of root account credentials.	This is another important Security Best Practice Check, which CloudCheckr addresses to ensure root (unrestricted) access is not used/abused.
	8.1.5 Partner has a documented Access Management Strategy, including but not limited to: AWS Identity and Access Management (IAM) users, federated roles, AWS Security Token Service (AWS STS) credentials, access keys, console passwords, and hardware or virtual multi-factor authentication (MFA) devices.	Partners are encouraged to leverage CloudCheckr to ensure Role-Based Access Control and Multi-Factor Authentication are enabled for IAM accounts. For additional details, review CloudCheckr's privacy policy and Security Practices at https://cloudcheckr.com/privacy-policy/ and https://cloudcheckr.com/data-security/

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
	8.1.6 Partner administrates AWS accounts through the use of federated roles in order to access AWS Console or issue temporary credentials, as opposed to provisioning individual IAM users and groups.	CloudCheckr support SSO (Single-Sign-On) and Role-Based Access Control.
	8.1.8 Partner ensures customers understand AWS security processes and technologies as outlined in https://aws.amazon.com/whitepapers/aws-securitybest-practices/. Evidence must be in the form of onboarding and educational documents provided to customers that specifically cover customer security considerations in the Partner's environment.	CloudCheckr provides training including webinars on Security and Automation including the Shared Responsibility Model.
8.2 Security Event Logging and Retention	**8.2.4** Partner has AWS CloudTrail enabled on all managed accounts and a process is in place to maintain log integrity.	CloudCheckr includes 500+ Best Practice Checks, including checks to ensure CloudTrail is enabled on managed accounts.

9.0 Service Desk Operations and Customer Support

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.5 Proactive Monitoring and Alerting	Partner has systems, tools, or applications capable of monitoring the performance of all AWS services that are part of the customer's managed service agreement. Proactive monitoring looks for patterns of events to predict possible future failures. (ITIL Service Operation) The monitoring and alerting functionality must also be accompanied by corresponding service desk functionality to take action on events/alerts according to SLAs/contractual obligations. Partners should show their capabilities within the following categories: Infrastructure monitoring, some examples include: › Amazon CloudWatch out-of-the-box metrics for AWS monitoring, alerting, and automated provisioning › Amazon CloudWatch custom metrics for application monitoring, alerting, and automated provisioning › Other 3rd party AWS infrastructure monitoring tools Service monitoring, some examples include: › Operating system monitoring tools for OS-level monitoring › Application monitoring tools for application-level monitoring › Simulated transaction monitoring tools for end-to-end system monitoring	CloudCheckr offers robust Reports, Best Practice checks, heat maps, CloudTrail and Config alerts, and Change Monitoring reports.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.6 Next Generation Monitoring Capabilities	**9.6.1** Partner must implement service intelligence monitoring capabilities that gather intelligence from heterogeneous monitoring and logging sources. One of the values a next-generation MSP brings to customers is its ability to manage AWS workloads that, if designed correctly, are dynamic, highly automated environments that can scale up down according to demand. To be effective, next gen MSPs must use new technologies that give visibility into the full environment, including application performance. Furthermore, given the dynamic and highly automated nature of AWS workloads, MSPs should leverage monitoring tools that scale instantly to adjust to changes in workloads being monitored.	CloudCheckr provides Best Practice checks, CloudTrail and Config alerts, and Change Monitoring reports.
	9.6.3 The solution should apply machine learning capabilities to monitoring and log data. Monitoring machine learning solutions can be used in a predictive fashion, identifying trends in data to trigger actions prior to an anomaly or threshold breach being detected. In logging, machine learning solutions can provide suggestions to operators investigating root cause of an incident by surfacing related log events from across an application landscape, while accepting feedback from the operator on the relevance of the data.	CloudCheckr is rolling out Machine Learning capabilities to further enhance our predictive reporting and recommendations.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.8 Continuous Compliance	**9.8.1** Next generation MSPs adopt a continuous approach to managing and monitoring compliance, both as it relates to new policies, audit requirements, and non-compliant changes within the environment. Partner provides continuous compliance solutions to its customers that apply to AWS managed resources. Examples include use of AWS CloudTrail or AWS Config to monitor changes to network configuration, access by IAM principals, or Amazon EBS encryption settings to ensure the system remains within policy.	Met via CloudCheckr's unified configuration audit, log event monitoring, and security alerts. CloudCheckr's best practice checks, which map to controls like CIS, NIST 800-53 and PCI DSS, help harden the configuration state and maintain integrity with continuous monitoring.
	9.8.2 Partner provides continuous compliance solutions to its customers to ensure compliance of resource level controls. Examples include ensuring CIS hardened instances remain hardened after deployment and maintaining log and configuration file integrity.	Met via CloudCheckr's unified configuration audit, log event monitoring, and security alerts. CloudCheckr's best practice checks, which map to controls like CIS, NIST 800-53 and PCI DSS, help harden the configuration state and maintain integrity with continuous monitoring.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.9 Event Management	**9.9.1** Partner has a process for detecting, categorizing, and taking action on all events. Events are generally: › Informational in nature (and should be logged) › Related to warnings (and should create alerts) › Exception-based; dealing with something acting out of normal pattern (and should trigger an incident) An event is defined as a change of state that has significance for the management of an IT service or other configuration item. The term is also used to mean an alert or notification created by any IT service, configuration item or monitoring tool. Events typically require IT operations personnel to take actions, and often lead to incidents being logged. Event management is the process responsible for managing events throughout their lifecycle.	Achieved through CloudCheckr's pre-built and configurable CloudTrail and config alerts.
	9.9.2 Partner can demonstrate the ability to programmatically add value to customers' operations by differentiating between monitoring events that require customer engagement and those that don't. Evidence must be in the form of examples of filtering and sending event information to customers.	Accomplished via automated prioritization in Best Practices and customizable alert notifications.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.12 Asset Management	Partner has a strategy for tracking and managing its AWS deployed assets. An asset is defined as any resource or capability that could contribute to the delivery of a service. A generic activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle. (ITIL Service Strategy/Service Transition) Partner's asset management strategy answers the following questions: › Is your organization leveraging AWS provided instance and service-specific metadata as part of its asset management strategy? › Is your organization leveraging custom resource tags to track and identify AWS resources? › Does your organization have a resource tagging strategy? › How will AWS assets be integrated with internal asset management systems?	CloudCheckr provides Inventory reporting, Multi account views, general reports. Specific cost and inventory tagging reports - including tagging rules with alerts tied to violations.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.13 Configuration and Change Management	**9.13.1** Partner has configuration and change management processes. Processes address the following questions specific to the AWS business: › How will your organization manage server images (e.g., Amazon Machine Images (AMIs))? › Will instances be automatically configured at launch or manually configured later? › How will patches and upgrades be applied? › Will applications be managed as homogeneous fleets? › How will your organization manage changes to OS hardening baselines, configure security groups or OS firewalls, and monitor their instances for intrusions or unauthorized changes?	CloudCheckr maintains CloudTrail and Config reports, plus Change monitoring reports. History is also available.
	9.13.3 Partner has a Configuration Management Database (CMDB). A Configuration Management Database is a database used to store configuration records throughout their lifecycle. (ITIL Service Transition) Evidence must be in the form of a demonstrable Configuration Management Database.	CloudCheckr maintains CloudTrail and Config reports, plus Change monitoring reports. History is also available.

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
9.14 Customer Reports	Partner provides web accessible customer reports. Reports should allow customers to self-select parameters such as devices and thresholds. Examples of reports provided are: › Incident management › Non-service affecting incidents › Performance analysis › Assets/resources › Exceptions	CloudCheckr reports can be customized and filtered and delivered as PDF, CSV and via email.

12.0 Customer Obsession

REQUIREMENT	APPLICABLE LANGUAGE	CLOUDCHECKR FULFILLMENT
12.2 Customer Review	**12.2.2** Partner regularly assesses customer infrastructure cost and highlights opportunities to optimize these costs to its customers through reporting. Evidence must be in the form of documentation from a customer review meeting (may be same example used above), including evidence that recommendations for infrastructure cost optimization were provided, e.g., using the Cost and Usage Report.	In addition to service-related reports, CloudCheckr maintains Change Monitoring reports. CloudCheckr generates Trending reports, Customizable inventory reports and Heat maps to spot trends.

ABOUT CLOUDCHECKR

CloudCheckr empowers certified MSPs, Resellers, System Integrators and Advanced Consulting Partners worldwide to run their cloud as a business. The CloudCheckr cloud management platform (CMP) unifies cost, security and governance for AWS deployments. Partners of all sizes trust CloudCheckr to manage and optimize public cloud environments so they can effectively grow their AWS practice, increase profitability, improve business operations and confidently meet the expectations of third-party validation audits for next-generation APN partners.

With CloudCheckr, partners can deliver differentiated products and services to AWS clients to help them:

- Save money in the cloud by automating cost allocation, optimize spending with analytics and streamlining billing and chargeback processes
- Mitigate security risks by proactively reducing the attack surface, continuously monitor security activity and demonstrate compliance
- Increase operational efficiency by reducing resource waste, increasing utilization and automating cloud cost and security management

CloudCheckr's CMP platform includes automated cost & expense management, security & compliance, asset management and resource utilization that supports most primary and secondary AWS services. Upon completion of the Registration Process and setting up of the necessary Credentials and Permissions, CloudCheckr will load valuable partner information about the who is spending money with AWS, what Services are being used, how are these Services being used, how are security controls being implemented, where are potential configuration vulnerabilities or concerning activities, and what has been the history of my AWS usage, costs, configurations, and controls.

For more information, visit us at **www.cloudcheckr.com**.

Cloud Checkr

342 N GOODMAN ST,
ROCHESTER, NY 14607

1-833-CLDCHCK

www.cloudcheckr.com