The following changes summarizes the Validation Checklists (VCLs) updates published on August 2nd, 2021.

Changes to Partner Hosted FTR

1. WAFR-001 – This control now allows use of alternate internally defined architecture review process.
2. ARC-003 – Added more details on how the requirement applies to AWS Organization.
3. SDAT-003 – This requirement now only applies to traffic outside of Partner's VPC.

Changes to Customer Deployed FTR

1. Removed Following Controls
    a. ARCH-003 - Architecture diagram(s) label where customer data is stored.
    b. DSEC-001 - The deployment guide must provide links to IAM and IAM best practices documentation.
    c. BAR-002 – BAR-006 – Step by step process for DR testing
    d. DAS-002 - The deployment guide provides step-by-step instructions for maximizing uptime and availability (e.g., autoscaling groups, multi-AZ, disaster recovery).
    e. DAS-003 - The deployment guide describes the different deployment configurations (e.g., for a solution that can be deployed single-AZ, multi-AZ, and/or multi-region, an explanation of the different deployment configurations as well as the pros and cons of each is included).
2. Added Following Controls
    a. INT-005 – Supported regions
3. Following controls have been updated
    a. ARCH-005 – Removed Security Groups, NACLs and ingress/egress mappings from this requirement.
    b. SIZ-001 – SIZ-004 – These controls have been simplified and now covers all AWS resources.

Changes to Technology Competencies

All Technology Competencies:

1. Following requirements have been modified:
    a. NETSEC-001 – This requirement has been updated to provide more guidance.
    b. OPE-006 – Additional details have been added to explain the requirement and differentiate it from OPE-005
2. Following requirements have been removed:
    a. OSSEC-004 - Use public key authentication for all Secure Shell (SSH) connections. This requirement has been removed because we don't recommend using SSH for routine tasks.

Changes to Consulting Competencies

SaaS Consulting Competency

1. Following requirements have been removed:
    a. SAASPR-001 - Focus Region
    b. SAASPR-001 - Focus Region
    c. SAASPR-003 - Focus Industries
    d. SAASPR-004 - Target Customer Tiers
    e. SAASPR-005 - Focus SaaS Use Cases
2. Following requirements have been added:
    a. SAASPR-001 – SaaS Business Practice Plan
3. Following requirements have been modified:
    a. SAASTA-014 – The requirement has been updated to provide more details.

Data & Analytics Consulting

1. A clarification is added in the prerequisites section to highlight that launched opportunities must be Partner sourced.

Migration Consulting

1. Controls from common and migration specific customer example requirements have been merged and further clarifications have been added.

The following changes summarizes the Validation Checklists (VCLs) updates published on March 15th, 2021.

Changes to FTR:

1. Following requirements have been added:
    a. IAM-012 - Use centralized identity

Changes to Technology Competencies

All Technology Competencies:

2. Requirements covered by FTR have been removed from competency VCLs. The list of removed requirements are in the Appendix of this document.
3. FTR requirement has been changed. All products must have a valid FTR conducted within 24 months of the application instead of 12 months. This is consistent with FTR expiry.
4. NETSEC-001 - The requirement to implement Security Groups to restrict traffic within the VPC has been removed.
5. NETSEC-003 – This requirement has been updated to provide more guidance on resources that can be in public subnets.
6. OSSEC-001 - More details on operating system and container image hardening have been added. The requirement now defines a benchmark (CIS or equivalent) to adhere to.
7. SECOPS-001 - Requirement to monitor changes now include all compute resources.
8. DOC-003 – This requirement now asks deployment guide as evidence.
9. Following requirements have been added:
    a. IAM-005 - Mitigation of exposed credentials
    b. IAM-006 - Use centralized identity
    c. IAM-007 - Authenticate API or UI requests

Security Competency:

1. Following requirements have been removed:
    a. SECID-002 - Identity and Access Control solution provides federated authentication and authorization for the AWS Command Line Interface (AWS CLI).
    b. SEC-007 - The solution uses IAM Access Analyzer for supported services.
2. Following requirements have been added
    a. SEC-008 - The solution supports multi-account deployment and baselining via AWS Organizations and/or AWS Control Tower.
    b. SECINF-005 - Network and Infrastructure Security solution has been verified to support running on AWS Outposts.
    c. SECINF-006 - Network and Infrastructure Security solution supports running on hosts running the Graviton processor.

d. SECHEP-007 - Host and Endpoint Security solution supports running on hosts running the Graviton processor.
e. SECHEP-008 - Host and Endpoint Security solution The solution can be deployed via AWS Systems Manager distributor.
f. SECCRP-005 - Data Protection and Encryption solution supports ingesting GuardDuty findings related to S3.
g. SECCRP-006 - Data Protection and Encryption solution supports ingesting findings from IAM Access Analyzer related to S3
h. SECLOG-004 - Logging, Monitoring, Threat Detection, and Analytics Solution supports capturing and displaying AWS resource specific metadata (tags, AMI, region, etc.) related to AWS resources displayed to customers.
i. SECID-006 - Identity and Access Control solution supports synching identities to AWS Single Sign-On.
j. SECVCA-007 - Infrastructure vulnerability scanning solutions support running on EC2 instances with the following operating systems: Amazon Linux 2, Microsoft Windows Server, Ubuntu Server, RedHat Enterprise Linux, Suse Enterprise Linux
k. SECVCA-008 - Infrastructure vulnerability scanning solutions support running on EC2 instances with the AWS Graviton processor.
l. SECVCA-009 - Vulnerability and Configuration Assessment solution supports ingesting findings from IAM Access Analyzer.
m. SECVCA-010 - Infrastructure vulnerability scanning solutions capture and display AWS metadata (tags, AMI, region, etc.) for the AWS resource that is being displayed to the customer.
n. SECAPP-003 - Customer deployed infrastructure-based solutions support highly available deployment architectures.

Retail Competency:

One additional requirement has been added:

RTL-004 - Payment Cart Industry (PCI) Data Security Standards (DSS) – Certification or SAQ

Changes to Consulting Competencies:

MSP Waiver:

Several competencies have waived few controls in the checklist for MSP because those controls are validated by MSP on-boarding. Some of these were not migrated to the new checklist format.

Following competencies have been updated with MSP waiver:

a. Data and Analytics
b. DCX
c. Government
d. Healthcare
e. Life science
f. Microsoft

g. Storage

Oracle Competency:

1. A new requirement has been added to clarify that the Oracle certifications provided must have been obtained within 18 months of the application.

SAP Competency:

1. A new requirement requesting following information has been added:
   EXMUC-002 – Solution Details
   a. SAP solutions involved
   b. OS platform(s) / DB platform(s)
   c. If migration of an existing environment, source infrastructure platform, source OS platform(s), and source DB platform(s)

Changes to Service Validation Programs:

All checklists:

Some issues (grammatical errors, duplicate requirements) have been addressed.

RDS Ready for Tooling:

More details have been added to few controls based on the feedback from the partners.
The following requirements have been added:

1. GIF-003 - Product Deployment
2. GIF-004 - Product Limitations and Limits
3. GIF-005 - Customer account access configuration

AWS Lambda Ready:

The following requirements have been added:

1. GIF-004 - Customer account access configuration
2. LEX-001 – Documentation
3. TES-001 - Invoke API Support
4. TES-002 - Credential handling and fallback
5. TES-003 - API Use
6. GVN-001 - Governance and compliance features

Appendix

Following requirements have been removed from the Technology Competency VCLs

1/ IAM – 001 resources are reviewed. (FTR - IAM-008)

Current Requirement: The AWS Partner has defined a standard process to review IAM resources (i.e., users and roles and their associated policies) in their accounts and ensure they adhere to the principle of least privilege. Any new IAM resources or updates to existing resources must be reviewed by someone other than the original author before being deployed to production. The AWS Partner must also have a mechanism in place to periodically review existing resources to 1) ensure that the policies are appropriately scoped and 2) remove any unused or unnecessary resources from the account.

2/ IAM-003 - Access is revoked for terminated individuals. (FTR – IAM-007)

Current Requirement: Mechanisms exist to ensure that access to all AWS accounts and other critical systems is revoked in a timely fashion for any individuals (employees, contractors, etc.) who leave the company or are otherwise terminated.

3/ IAM-004 - System credentials are not shared across users. (FTR – IAM-004)

Current Requirement: Each individual with access to the AWS Partner's systems has unique authentication credentials for routine use that are not shared between multiple users. This includes AWS IAM access keys, SSH private keys, and usernames and passwords.

4/ NETSEC-002 - Data that traverses the Internet is encrypted in transit. (FTR - SDAT-003)

Current Requirement: All Internet facing endpoints must use SSL/TLS or another standard mechanism to encrypt data that leave's the AWS Partner's network. Any connections between an Amazon VPC owned by the AWS Partner and any other private network outside of AWS must also be encrypted.

5/ SECOPS-002 - Data classification standard is in place. (FTR – SDAT-001)

Current Requirement: There must be a defined policy in place for classifying the sensitivity of all customer data processed and stored in the workload as well as a policy that defines the appropriate methods to use when handling data in each classification category. Evidence can be based on verbal attestation.

6/ SECOPS-003 - Sensitive data is encrypted. (FTR - SDAT – 002)

Current Requirement: Data classified as sensitive based on the data classification standard (see SECOPS-002) is encrypted at rest and in transit.

7/ SECOPS-010 - Production workloads are run in a dedicated AWS account. (FTR – AWS – 001)

Production workloads are segregated from non-production workloads at the AWS account level. AWS accounts used to run production services are not used for any other purposes.

Access to production accounts must be limited to individuals who have a business need to directly manage the production environment.

8/ REL-006 - Solution is resilient to availability zone disruption. (FTR – DR-004)
The solution must continue to operate in the case where all of the services within a single Availability Zone (AZ) have been disrupted.
Solutions may allow customers to choose a single AZ deployment (e.g., in order to reduce costs), but there must also be a high availability option available.
Solutions that do not support multi-AZ deployments must provide technical justification for why this is not feasible (e.g., the workload requires extremely low inter-node network latency.) Additionally, these solutions must also provide a Recovery Time Objective (RTO) of less than one hour in the event of an AZ disruption. For customer hosted solutions, the customer facing documentation should include details on how to recover from an AZ disruption. For SaaS solutions, control plane services must always continue to operate in the event of a single AZ disruption, and AWS Partner must provide a detailed explanation of the recovery mechanisms that are in place for the data plane in order to meet a one-hour RTO.

9/ REL-007 - Resiliency of the solution has been tested. (FTR – DR-004)

Current Requirement: The resiliency of the infrastructure to disruption of a single AZ has been tested, e.g., through a game day exercise, within the last 12 months.