Supplier Minimum Control Requirements – 2021 Updates

December 2021

JPMorgan Chase & Co.

Supplier Minimum Control Requirements – 2021 Updates

Introduction

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in December of 2021. It specifies material changes made in this update cycle to facilitate comparison with the prior version. Use this change log as a guide and refer to the Minimum Control Requirements document itself for the exact wording of the controls.

Section 1: Holistic Changes to the Minimum Control Requirements

Supplier Minimum Control Requirements – 2021 Updates

Section 1: Holistic Changes

Subject of Change	Control Domain(s)	Description
Rename Data and Records Management	Data Records Management	• The Data and Records Management control domains have been renamed to “Data Risk Management” to be consistent with JPMC control domains.

Section 2: Changes to Specific Control Domains

Supplier Minimum Control Requirements – 2021 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Physical and Environmental Security	• Removal of 2 control statements	• ~~Addition or removal of assets from the facility must be documented and tracked.~~ • ~~Supplier must obtain approval from JPMC prior to allowing assets with JPMC Confidential Information to be removed from the facility~~.
Data Protection	• Minor change to 2 existing control statements • Relocation of 1 statement to Data Protection from Security Configuration	• JPMC Highly Confidential and Confidential Information must be protected and encrypted in transit and at rest (including in backup) as well as when shared with Supplier's subcontractors. • The ability to write to portable electronic media must be disabled where possible, and any exceptions must be documented.
Identity and Access Management	• Addition of 1 new control statement	• Federated identity management must be implemented for JPMC access to Supplier systems via industry standard security assertion markup language (SAML).
Security Configuration	• Removal of 1 control statement • Relocation of 2 statements to other domains	• ~~The production network must be isolated from the development and test environments.~~

Supplier Minimum Control Requirements – 2021 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Security Operations	• Change to 1 existing control statement • Addition of 1 new control statements	• A process should be in place to conduct attack simulations ~~on a segregated environment~~ including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with appropriate reporting, remediation/acceptance, and tracking of findings. • Access to non-corporate/personal email and instant messaging solutions must be restricted.
Vulnerability Management	• Change to 2 existing control statement	• Supplier must include as part of their vulnerability management program, the receipt of vulnerability related security alerts and intelligence from external and internal sources in order to identify and monitor for vulnerabilities in their environment. • Any critical vulnerabilities identified through intelligence gathering, vulnerability scans or penetration testing must be prioritized and remediated within a well-defined timeframe commensurate with the vulnerability risk.
Technology Development	• Change to 2 existing control statements	• The SDLC must include a Secure Design Review, and preventive and detective controls in line with industry standards (such as OWASP) to identify vulnerabilities and design flaws. • ~~A procedures~~ Governance must be established, documented, and enforced to remediate vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach.
Technology Operations	• Removal of 6 redundant control • Addition of 1 new control statement	• See MCR Document for specific language

Supplier Minimum Control Requirements – 2021 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
~~**Data**~~ ~~**Records Management**~~ **Data Risk Management**	• Merged control statements from Data and Records Management into one new control domain	• See MCR Document for specific language
Technology Asset Management	• Minor change to 1 existing control statement • Addition of 1 new control statement	• Supplier must maintain an appropriate technology asset inventory governance structure to include recorded changes to asset records, sufficient back up of asset registers, annual integrity validation of the asset registers, asset ownership recertification, timely asset register updates when asset records are altered, regular license audits of assets, procedures addressing lost/stolen assets, and remediation of unauthorized assets. • Supplier must ensure assets are transported in a secure manner.
Incident and Event Management	• Removal of 1 control statement	• ~~The incident management policy and procedures must include the responsibilities of Supplier Personnel and identification of parties to be notified in case of an information security event/incident.~~
Business Resiliency	• Addition of 1 new control statement • Change to 4 existing control statements	• See MCR Document for specific language
Technology Resiliency	• Addition to 3 existing control statements • Addition of 4 new control statements	• See MCR Document for specific language

Supplier Minimum Control Requirements – 2021 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Third Party Relationships	• Change to 1 existing control statement	• Supplier's subcontractors must be identified, assessed, managed, and monitored in accordance with the terms of the Master Agreement with JPMC, including compliance with JPMC's Minimum Control Requirements and Supplier Code of Conduct applicable to any such services.
Customer Contact	• Change to 2 existing control statements	• Customer contact agents must receive privacy training (~~e.g., addressing~~ addressing, e.g., proper handling of individual personal information in light of privacy laws and regulations), as may be specified in the relevant contract(s) ~~or~~ and/or as directed by JPMC. • Any complaints received regarding JPMC or any services provided for or on behalf of JPMC, must be reported to JPMC as may be specified in the relevant contract(s) ~~or~~ and/or as directed by JPMC.