Supplier Minimum Control Requirements – 2023 Updates

JPMorgan Chase & Co.

Supplier Minimum Control Requirements – 2023 Updates

Introduction

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in January of 2024. 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 – 2023 Updates

Section 1: Holistic Changes

Subject of Change	Control Domain(s)	Description
None	N/A	• No changes to the structure/format/etc. of the Supplier Minimum Control Requirements for 2023

Section 2: Changes to Specific Control Domains

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Technology Governance Risk and Compliance	• Update to 1 existing statement	• Security policies, *~~and~~ responsibilities **& obligations, including cybersecurity **and technology controls awareness training, must be communicated and socialized within the organization to Supplier Personnel.
Physical and Environmental Security	• Change to 1 existing statement	• Detective monitoring controls (e.g., CCTV, **intrusion alarm system) must be in place with a defined retention period. **CCTV must have a defined retention period.
Data Protection	• Removal of 1 statement • Change to 4 existing statements	• **All JPMC Highly Confidential and Confidential Information must be protected and encrypted **by strong cryptography in transit and at rest (including in backup). *~~as well as when shared with Supplier's subcontractors.~~ • **The *~~Supplier's~~ data protection policy must cover encryption, key and certificate lifecycle management, permitted cryptographic algorithms and associated key lengths, message authentication, hash functions, digital signatures, and random number generation. • **The data protection policy must be reviewed against industry standards on a regular basis. • **Appropriate technical configuration(s) for encryption must be implemented *~~Supplier must implement appropriate technical configuration for the protection of encrypted~~ for portable media. • ~~*Procedures around cookie management must be compliant with applicable laws and regulations.~~

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Identity and Access Management	• Change to 2 existing statement	• Documented logical access policies and procedures**, including those that support attribute-based or *~~must support~~ role-based **access, must ensure user access is commiserate with a user's job responsibility and must support "need-to-know" access based on the principle of least privilege, and ensure segregation of duties **and the prevention of toxic combinations during the approval and provisioning process. • A documented authentication and authorization policy must cover all applicable systems and networks and must include *~~password~~ provisioning *~~requirements, password~~ complexity and reset requirements, *~~password resets,~~ for passwords and other secrets in addition to thresholds for lockout attempts, thresholds for inactivity, and assurance that no shared accounts are utilized.
Security Operations	• Change to 1 existing statements	• Data loss prevention (DLP) technology, processes, and/or solutions must be deployed to protect against the exfiltration of JPMC information **through all channels of communication.

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Privacy	• Removal of 2 existing statements • Change to 4 existing statements	• *~~Privacy impact assessment must be conducted during the requirements phase of system development to evaluate the impact to Personal Information and review the scope of monitoring.~~ • *~~The privacy impact assessment~~ **Supplier's processing of Personal Information must not conflict with any applicable *~~local and other~~ Laws. • **If Supplier will collect Personal Information from individuals on behalf of JPMC supplier must have procedures for **making available a JPMC privacy notice and/or obtaining **prior, informed consent **from individuals. *~~users to collect Personal Information, giving users the ability to~~ • **Supplier must have procedures in place to provide complete and timely responses to JPMC, and take actions necessary to honor, individual rights requests, including but not limited to requests to access, correct, opt-out, delete, restrict, make portable, or object to the processing of Personal Information. • *~~A privacy notice or information banner must be in place, requiring acknowledgement by the end user whenever Personal Information is collected, transmitted, processed, or stored.~~ • **Supplier must have documented procedures for *~~around~~ collecting, **processing and disclosing Personal Information *~~as required by the Law must be defined and~~ including any restrictions **imposed by law, contractual arrangements and/or JPMC privacy policies *~~on disclosing that Information must be documented~~

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Technology Development - System Development Lifecycle (SDLC)	• Change of 1 existing statement • Removal of 1 existing statement	• SDLC governance must be established, documented, and enforced to identify and remediate defects, vulnerabilities, coding errors, and design flaws prior to production using a risk-based approach **and in line with industry standards and frameworks. • *~~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~~
Technology Operations	• No change to current intent of the controls- Consolidated 8 existing statements into 3 statements	• *See MCR for statement update for the consolidation of statements*

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description

Data ~~Risk~~ Management	• Change of CDAO category name
	• Enhancement to1 existing statement with examples
		• All JPMC data provided to and stored by Supplier and dependent subcontractors must be stored and retained in a manner that:
		  • Includes the capability to access and, **where required retrieve the data as needed.
		  • Avoids loss due to media decay or technology obsolescence.
		  • **Is stored in secure locations that provide*~~s~~ reasonable safeguards against *~~ordinary~~ hazards, **that include, but are not limited to, the following:
		  • **Ordinary hazards, such as power loss, minor fire, water, mildew, rodents, and insects
		  • Man-made hazards, **such as theft, accidental loss, sabotage, and commercial espionage
		  • Disasters, **such as fire, flood, earthquakes, hurricanes, and explosions

Information & Technology Asset Management	• Change of CDAO category name	• Name of the CDAO category was updated rom “Technology Asset Management” to “Information & Technology Asset Management
Incident and Event Management	• No change to current intent of the control - Consolidation of 4 statements into 3	• See MCR for statement update for the consolidation of statements

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description

Business Resiliency	• Change to 4 statements
	• Addition of 1 statement
		• Supplier must perform a Business Impact Analysis (BIA) **to estimate the impact caused by disruptive failure to services provided for JPMC so that appropriate Recovery Strategies can be developed *~~determine their business resilience process criticality and~~ to define a Recovery Time Objective (RTO) for all processes they utilize to support the services or functions being performed for JPMC.
		• Supplier recovery plans must be updated, reviewed and approved **by the Supplier's management at least annually or as material changes occur within Supplier's operating environment.
		• Resiliency plans**, including recovery strategies must be tested on a regular basis, noted deficiencies/failures should be addressed timely, and testing should:
		  • be conducted in conditions comparable to production
		  • demonstrate recovery within the established Recovery Time Objectives
		  • be tested annually
		• **Supplier must conduct testing of the effective operation of avenues of communication to all personnel and subcontractors associated with recovery plans and strategies at least annually.

* Indicates the removal of wording
** Indicates the addition of wording

Supplier Minimum Control Requirements – 2023 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Subject of Change	Description
Business Resiliency (cont'd)	• cont'd	• Any change that **may involve, but is not limited to, changes in Supplier's business strategy, service, process, assets, and regulatory/legal obligations that could result in significant changes to the BIA or plans and/or affect the recovery of the process or infrastructure, *~~may involve, but is not limited to, changes in Supplier's business strategy, service, process, assets, and regulatory/legal obligations, resulting in significant changes to the BIA or plans~~ must **be tested within a year of the **effective date of significant change.

Technology Resiliency	• No change to current intent of the control- Consolidation of 7 statements into 1 statement
	• Addition of 1 statement
		• See MCR for statement update for the consolidation of statements
		• **All service provided by the Supplier (Applications and associated hosts) must employ a backup policy to ensure the availability of data required for full application recoverability.
		  • **The policy must define datasets, frequencies, criteria for a successful backup, annual test requirements, offsite storage requirements, and retention periods.
		  • **The backup policy must be annually reviewed and recertified.

* Indicates the removal of wording
** Indicates the addition of wording