J.P.Morgan

Supplier Minimum Control Requirements - 2024 Updates

December 2024

Supplier Minimum Control Requirements – 2024 Updates

Introduction

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

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

Section 2: Changes to Specific Control Domains

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Governance Risk and Compliance	• Alignment with industry standard frameworks like COBIT and NIST for the Information Security Program. • New inclusion of a process for identifying, assessing, and complying with legal and regulatory obligations impacting the supplier technology environment.	• Addition of 2 new statements • Removal of 2 existing statements • Change to 2 existing statements	• **The Information Security Program must be document, reviewed, and implemented in alignment with industry standard frameworks (i.e. COBIT and NIST). All risks and controls must be documented, assessed, and aligned with industry standard frameworks. • **A process must exist to facilitate the identification, assessment, and compliance with legal and regulatory obligations impacting the supplier technology environment. • A risk-based *~~exception management~~ process must be in place for prioritization and remediation or risk acceptance of controls that have not been adopted or implemented. • Awareness training on security policies, responsibilities and obligations, must be communicated and socialized to Supplier Personnel. including but not limited to, cybersecurity, technology, and data management. *~~controls awareness training, must be communicated and socialized within the organization to Supplier Personnel~~. • *~~A documented set of security policies and procedures must govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of information, assets, and associated services.~~ • *~~Risks and controls must be documented, reviewed, updated to reflect relevant risk assessment results, and implemented in alignment with relevant framework and risk assessments~~.

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Physical ~~and~~ ~~Environmental~~ Security	• Physical Security and Environmental Security have been separated into distinct sections, providing more clarity and focus on each area.	• Separated Domain • Removal of 2 existing statement	• *~~Facilities must maintain appropriate environmental controls, including fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection~~. • *~~Environmental control components must be monitored and periodically tested.~~
~~Physical and~~ Environmental Security	• Physical Security and Environmental Security have been separated into distinct sections, providing more clarity and focus on each area.	• Separated Domain • Removal of 3 existing statement	• *~~Physical and environmental security processes and procedures must be in place for facilities with access to, or storage of, JPMC Confidential Information.~~ • *~~Personnel should be granted access to areas of the facility based on the principle of least privilege.~~ • *~~Physical access to facilities must be restricted, with all access recertified on a regular schedule.~~ • *~~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.~~

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
~~**Data Protection**~~ **Cryptographic Services and Data Loss Prevention**	• A new section in detailing requirements for cryptographic mechanisms and Data Loss Prevention (DLP) processes, including key lifecycle management and periodic assessments for data exfiltration risks.	• Change in Risk Area name • Addition of 4 new statements • Removal of 2 existing statements	• **Suppliers and dependent subcontractors must develop a data protection policy that covers at a minimum the use of cryptographic mechanisms (e.g., encryption, hashing, digital signatures, etc.), key lifecycle management, and permitted cryptographic algorithms and associated key lengths. • **The data protection policy must be reviewed against industry standards, applicable regulatory requirements, and best practices on a regular basis. • **All cryptographic keys must be managed throughout their lifecycle. • **Data Loss Prevention (DLP) processes, technology and/or solutions must be in place to detect and evaluate potential DLP events in order to protect sensitive data, including but not limited to non-public JPMC information, from being exfiltrated through user-initiated egress points such as email, websites, removable media, SaaS, vendor platforms, print, and messaging applications. • *~~The 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.~~ • *~~Appropriate technical configuration(s) for encryption must be implemented for portable media.~~

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Identity and Access Management	• Inclusion of more detailed requirements for privileged account management, such as privileged activity logging and post-activity review. • Additional mechanisms such as OpenID Connect for federated identity management, in addition to SAML are now included.	• Change to 4 existing statements	• Logical access policies must cover remote access, access request approval prior to access provisioning and periodic recertification of access. *~~and the accuracy of access provisioned.~~ • A privileged account management process and control policy must be documented, covering privileged (system or elevated user) and non-privileged (personal) account separation*~~, prohibiting the granting of privileged access to a personal account,~~ privileged account discovery **and inventory *~~into a central system~~, safeguarding of privileged accounts **and credentials, privileged activity *~~usage~~** logging and post activity *~~usage~~ review requirements, and assurance that non-interactive privileged accounts (e.g., system accounts) are not used interactively by *~~end~~ **human users. • External connectivity to the *~~JPMC~~ **Supplier network. • Federated identity management *~~must~~ **should be implemented for JPMC access to Supplier systems via industry standard, **e.g. security assertion markup language (SAML) **or OpenID Connect (OIDC) or other mechanisms that prevent JPMC workforce users from accessing Supplier systems from outside the JPMC network.

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Operations	- Emphasizes the need for a fraud and threat detection program and includes more detailed requirements for digital forensics and attack simulations.	- Removal of 2 existing statements	- *~~Supplier Personnel must be trained to identify and report suspected security weaknesses, suspicious activity, and security events or incidents.~~ - *~~Supplier must have a security event/incident response policy and procedure.~~
Incident and Event Management	- Added emphasis on training and awareness for supplier personnel in identifying and reporting security incidents, while maintaining the core requirements for incident management processes and engagement with JPMC	- Addition of 2 new statements	- **Supplier must have a security event/incident response policy and procedure. - **Supplier Personnel must be trained to identify, and report suspected security weaknesses, suspicious activity, and security events or incidents.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Vulnerability Management	• Introduction of a governance framework for vulnerability management and emphasizes tracking and reporting key metrics related to vulnerability management.	• Addition of 2 new statements • Change to 3 existing statements	• **Suppliers must maintain a governance framework that includes regular reviews and updates to vulnerability management policies, procedures, and tools, ensuring that the program remains effective and up-to-date with industry standards. • **Supplier must track and report key metrics related to vulnerability management, including but not limited to the number of vulnerabilities identified per scan, time taken for remediation, percentage of critical vulnerabilities remediated within SLA, and the success rates of remediation efforts. • …**Alerts are acted upon in a timely manner, threat intelligence is incorporated into the vulnerability management practices. • Vulnerability scans (authenticated and unauthenticated) and penetration tests must be performed against internal and external networks and applications periodically **or whenever significant changes occur, and prior to system provisioning for all systems that process, store, or transmit JPMC Confidential Information. **The scanning tools used must cover all in-scope systems and applications, and the results must be documented and reviewed for completeness. • …**Remediation actions must be documented, and their effectiveness validated through follow-up assessments.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Privacy	• More detailed requirements for handling Personal Information, including prompt notification to JPMC of any unauthorized processing or data breaches.	• Addition of 3 new statements • Removal of 2 existing statements • Change to 2 existing statements	• **Provide reasonable technical, organizational, personnel and physical measures to protect against the unauthorized or unlawful Processing of Personal Information and against the accidental loss and destruction of, or damage to, Personal Information. • **Promptly notify JPMC of any unauthorized or unlawful Processing, loss of, damage to or destruction of Personal Information; promptly take all necessary steps to investigate and remediate any security or confidentiality breach; promptly make available to JPMC any report generated in respect of such investigation. • **Supplier must not use government-assigned identification numbers (such as, but not limited to, Social Security Numbers or other national identifiers) as user IDs for logon to applications and systems • *~~Social Security Numbers or other national identifiers must not be utilized as User IDs for logon to applications.~~ • *~~Supplier's processing of Personal Information must not conflict with any applicable Laws.~~ • *~~Supplier must have procedures in place to~~ **Provide complete and timely responses to JPMC, and take actions necessary.. • If Supplier *~~will~~ collect**s Personal Information from **any individual*~~s~~ on behalf of JPMC Supplier must **implement *~~have procedures for making available~~ **to make a JPMC privacy notice **available and*~~/or~~ obtain*~~ing prior~~, informed consent from individuals **prior to collecting Personal Information.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Development - SDLC	• Newly included section on software supply chain security and incident response plans for third-party software vulnerabilities.	• Addition of 1 new statement • Removal of 1 existing statement • Change to 3 existing statements	• **The SDLC process must be adequately governed following a risk-based approach in-line with industry standards and frameworks, and continuously improve based on periodic assessments to ensure software is secure and suitable for production. • *~~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.~~ • Suppliers **must *~~operate an~~ develop, maintain *~~establish, document~~, and enforce a System Development Life Cycle (SDLC) process that enables the identification, tracking and remediation of defects, vulnerabilities, coding errors and design flaws prior to production. • …applicable to *~~any~~ all software and development framework *~~or model~~ used. • …identified and implemented to prevent software **obsolescence *~~from becoming obsolete~~.

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Development – Third Party Software	• A more detailed and proactive approach to managing third-party software, focusing on supply chain security, continuous monitoring, compliance, and incident response planning.	• Addition of 4 new statements • Change to 1 existing statement	• **Implement a software supply chain security program to assess and manage the risks associated with third-party and open-source software. This includes, but is not limited to, verifying the integrity and authenticity of software components and ensuring they are free from known vulnerabilities. • **Continuously monitor and manage software dependencies to ensure that all third-party and open-source components are up-to-date and free from known vulnerabilities. • **Establish an incident response plan for third-party software vulnerabilities, including processes for vulnerability disclosure, patch management, and communication with affected stakeholders. • Third party **software and open-source code *~~or software~~ used must be appropriately licensed, inventoried, and where commercially licensed, be fully supported by the vendor.

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Data Management	• Inclusion of more detailed requirements for data management, including structural correctness and compliance with global data privacy laws.	• Addition of 3 new statements • Change to 6 existing statements	• **Documented security policies and procedures that are reviewed on a periodic basis and must govern the receipt, transmission, processing, storage, control, distribution, retrieval, access, presentation, and protection of confidential information, assets, and associated services. • **Suppliers and dependent subcontractors that regularly provide data to JPMC must maintain and provide a data dictionary or equivalent data classification artifact, including any agreed-upon metadata for data provided to JPMC. • **Business records are appropriately identified with the relevant retention requirement. Data within such business records is disposed of once the retention requirement has been met. • …**specifications for the accuracy, timeliness, completeness, and structural correctness of the data. • **All JPMC data provided to and stored, both physically and digitally… • Is stored in secure locations that provide reasonable safeguards against hazards, that include, but are not limited to, the following **(Not limited to but including both physical and digital):

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Data management - Continued			• Supplier and dependent subcontractors must have controls in place to ensure JPMC data is **collected, created, stored, and processed in *~~accordance~~ **compliance with applicable laws, regulations, and contractual obligations, inclusive of relevant data use **restrictions *~~contractual obligations~~ and **all applicable global data privacy laws. • If Supplier or dependent subcontractor hosts data on behalf of JPMC, Supplier and dependent subcontractors must maintain and validate with JPMC (at least annually) a complete and accurate inventory of JPMC data with **at a minimum the following attributes: • **Description of Data • **Sensitivity and Criticality Classification of Data • Retention/Destruction Requirements (and execution of those requirements) • Location **of Data • **Use of Data • …**to maintain data provenance in accordance with Global Data Regulatory requirements.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency	• A more comprehensive and detailed approach to business resiliency, emphasizing regular updates, detailed recovery strategies, structured incident management, and communication of deficiencies.	• Addition of 4 existing statements • Removal of 3 existing statements • Change to 5 existing statements	• **Supplier must conduct testing of the effective operation of avenues of communication to all personnel and subcontractors associated with recovery plans and strategies at on a regular basis. • **Supplier must conduct testing of their planned Recovery Strategies to address disruption to assets upon which the Supplier depends to provide services to JPMC. Testing must be conducted on a risk based frequency by the Supplier for Site and Staff disruption, which at a minimum must: • **Supplier must conduct testing of their planned Recovery Strategies to address disruption to assets upon which the Supplier depends to provide services to JPMC. Testing must be conducted on a risk based frequency by the Supplier for Site and Staff disruption, which at a minimum must: • **Demonstrate that the in-scope Supplier processes tested recover within the RTO established by the relevant LOB or CF that has contracted the service(s).

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency - Continued			- **Assessment must be conducted on a risk based frequency by the Supplier to evaluate the sufficiency of their subcontractors resiliency controls Significant deficiencies and / or limitations in Supplier subcontractor Recovery capabilities must be identified and communicated to JPMC. - **Suppliers must also test on a risk based frequency their Recovery Strategies (e.g. manual work arounds or alternate processing with reference to supplier exit plans where applicable) for disruption to any critical subcontractor the Supplier uses to support JPMC. - *~~Business resiliency plans must identify key resources and address business interruptions of those resources supporting all JPMC services, including those provided by Supplier's subcontractors~~ - *~~The resiliency plans must have acceptable alternative work locations/strategies in place to ensure service level commitments are met.~~

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency - Continued			• *~~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 have~~ **Supplier must perform a Business Impact Analysis (BIA) to estimate the impact caused by disruptive failure to services provided for JPMC, which informs formal and **comprehensive Business Resiliency **(BR) plans to enable timely… • *~~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 to define a Recovery Time Objective (RTO) for all processes they utilize to support the services or functions being performed for JPMC~~. **Supplier business resiliency plans must be updated, reviewed and approved on a regular basis or as material changes occur within their operating environment.

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

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency - Continued			• *~~Business Resiliency recovery~~ **Supplier BR plans must have **Recovery **Strategies to adequately address **Supplier recovery in the event of disruption to the assets upon which the Supplier depends to provide services to JPMC. *~~the following disruption scenarios to meet~~ **The strategy must meet JPMC RTOs and service level expectations (as defined in the relevant contracts): **At a minimum Supplier BR Plans must consider Recovery Strategies for the following: • *~~Loss of~~ **Disruption to Staff • *~~Loss of~~ **Disruption to Site • *~~Loss of~~ **Disruption to Loss of application(s) *~~(where application disaster recovery is available)~~ • *~~Loss of~~ **Disruption to Supplier's subcontractors *~~(where subcontractor recovery is available)~~ • *~~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.~~ **Supplier must provide contact information to JPMC for use in the event of disruption to either party, and update JPMC when changes occur.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Resiliency	• A more structured and detailed approach to technology resiliency, focusing on comprehensive recovery action plans, detailed testing scenarios, and a robust crisis management framework.	• Removal of 2 existing statement • Change to 3 existing statements	• *~~Any change that could affect the recovery of the process or infrastructure, including significant changes in personnel, organizational structure, technology, location, or strategy must require a new test of the technology recovery plans affected by the significant change.~~ • *~~JPMC Confidential Information must be available upon request, in an industry standard format, so as to ensure portability and interoperability.~~ • The Supplier must ensure the *~~have formal technology recovery plans and~~ **adoption of a suitable *~~technical capability and implemented~~ recovery strategy*~~ies~~ for the technology service and provide suitable assurances of recovery *~~adopted to ensure appropriate~~ capabilities *~~are in place to limit impact~~ following a disruptive event (i.e. operational disaster or destructive cyber event where *~~both the primary~~ ~~(~~production environment*~~) and secondary (disaster recovery) systems or data~~ have been compromised *~~or destroyed. The formal technology recovery plans must include~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Resiliency - Continued			• **The supplier must define recovery action plans documenting specific recovery procedures to guide the failover of the technology service to the disaster recovery site or redeploy the service including data restoration. The plan should include the following: • *~~Details of a~~Approved recovery objectives (RTO, RPO, Maximum Tolerable Downtime). • *~~Procedures required to redeploy an application and restore associated data following a loss.~~ • *~~Processes and~~ Recovery procedures required… • Relevant Supplier’s subcontractors, including cloud hosting/service providers critical to executing the *~~recovery procedures~~ Plan • Recovery Action plans must be tested annually using sufficient methodologies *~~and frequencies which include testing long term strategies~~ to provide suitable assurances that recovery objectives can be achieved:

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2024 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Resiliency – Continued			• **The test must include a simulated disruption across the following scenarios: ■ **Loss of Application Deployment (Service or Site) requiring failover of the service to the recovery site ■ **Loss of Data requiring a restoration from immutable backup ■ **Loss of both production/DR environment requiring a full rebuild of the infrastructure environment, application redeployment and data restoration ■ **Where the test scope simulates a failure to the production environment, the ability to support business operational workloads in the recovery site must be a condition for determining a successful test.

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