J.P.Morgan

Supplier Minimum Control Requirements - 2025 Updates

December 2025

Supplier Minimum Control Requirements – 2025 Updates

Introduction

This change log references the JPMorgan Chase & Co. Minimum Control Requirements document (MCR), published in December of 2025. 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 – 2025 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 2025

* Indicates the removal of wording

** Indicates the addition of wording

Section 2: Changes to Specific Control Domains

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Governance Risk and Compliance	• Expands scope from risk assessment and remediation to comprehensive risk management and removes explicit mention of remediation efforts. • Adds identification and effectiveness to the scope of annual assessment. • Eliminates explicit guidance on handling unimplemented controls through risk-based prioritization, remediation, or acceptance. • Grammar and punctuation	• Addition of 1 new statements • Removal of 1 existing statements • Minor changes to 2 existing statements • Combined 2 existing statements	• **A documented risk management program must be in place to effectively evaluate, mitigate, and monitor risks across the technology environment. • *~~A risk-based process must be in place for prioritization and remediation or risk acceptance of controls that have not been adopted or implemented.~~ • The Information Security Program must be document**ed, 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. • Awareness training on security policies, responsibilities and obligations, must be communicated and socialized to *~~S~~**supplier *~~P~~**personnel*~~.~~**, including but not limited to, cybersecurity, technology, and data management. • A**n *~~risk~~ assessment must be performed annually to verify the **identification, implementation, **and effectiveness of controls that protect business operations and JPMC Confidential Information. • *~~The effectiveness of controls must be regularly validated through a documented risk assessment program and appropriately managed remediation efforts.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Physical Security	- No changes, retain 2024 MCR Wording	- N/A	- N/A
Environmental Security	- Adds the phrase "including applicable environmental controls, such as..." which clarifies that only relevant controls need to be implemented and introduces "such as" to indicate examples rather than an exhaustive list.	- Changes to 1 existing statements	- Facilities must maintain *~~appropriate environmental controls, including~~ **applicable environmental controls, such as fire detection and suppression, climate control and monitoring, power and back-up power solutions, and water damage detection.
Cryptographic Services and Data Loss Prevention	- Expanded and clarified encryption requirement for highly confidential and confidential data - New requirement added to encrypt all storage media containing JPMC data, not just highly confidential or confidential information. This broadens the scope of encryption requirements.	- Removed 1 existing statements and added portion to below - Addition of 1 new statements	- ~~All JPMC Highly Confidential and Confidential Information must be protected by industry (financial services) standard cryptography while in transit and at rest.~~ - **All storage media containing JPMC data, regardless of its classification, must be encrypted. Furthermore, highly confidential and confidential information must be secured with industry-standard encryption while in transit and at rest.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Identity and Access Management	• Scope narrowed to production systems, adds identity verification for resets, clarifies lockout, and expands MFA requirements. • Adds traceability to individual users and explicit assurance against shared accounts. • New requirement for identity verification during password resets.	• Change to 2 existing statements and 1 sub bullet	• A documented authentication and authorization policy must cover all **production *~~applicable~~ systems and networks and the provisioning of credentials including passwords and other secrets**. *, ~~supporting multi-factor authentication.~~ This policy must include password complexity **and identity verification for reset requirements, thresholds for lockout **for failed login attempts, **and thresholds for inactivity**. *~~, and assurance that no shared accounts are utilized.~~ **Policy must include Multi-factor authentication **(MFA) requirements and MFA must be implemented for: • Applications directly accessible from the internet**, including JPMC access to Supplier systems when federated identity management is not supported. • The administration of application access. • Each account provisioned must be uniquely identified **and traceable to an individual user with assurance that no shared accounts are utilized.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Configuration	• Expanded requirements now mandate risk-based network segregation, broader intrusion detection with centralized monitoring, comprehensive network architecture documentation, secure baseline configurations for all major asset types, and enhanced configuration management to address deviations. • New requirements have been added for DDoS and web application attack protection, outbound traffic inspection, strict separation of personal and corporate email domains, network access controls, and centralized logging and monitoring of security events.	• Change to 10 existing statements and 1 sub bullet • Added 3 new statements • Removal of 1 existing statements	• **The supplier must segregate networks based on risk profiles and have a governance process in place to approve and periodically review connectivity requests. *~~Information systems must be deployed with appropriate security configurations and reviewed periodically for compliance with Supplier's security policies and standards.~~ • **The supplier must have network access controls in place to prevent unauthorized devices from accessing the supplier's internal network. *~~Supplier must implement controls over its communication network to safeguard data.~~ • **The supplier must implement controls that allow for the detection and analysis of intrusion events. *~~Network and host-based intrusion detection and/or intrusion prevention systems must be deployed with generated events fed into centralized systems for analysis.~~ • **The supplier must document their network architecture and keep it up to date. *~~A network diagram, to include all devices, as well as a data flow diagram must be kept current.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Configuration - Continued	• Removed requirements include periodic review of security configurations, detailed malware scan/alert/update procedures, controls for email and instant messaging systems containing JPMC information, and preventive controls for blocking malicious email content and auto-forwarding.		• **The supplier must define, deploy, and manage secure baseline configurations for each major version of defined asset types and endpoints, which are based on industry best practices and the principle of least functionality. *~~Standard security configurations, using the principles of least functionality/privileges, must be established and security hardening demonstrated.~~ • **The supplier must employ configuration management mechanisms to identify and manage deviation from approved secure baseline configuration builds for in-scope asset types. *~~Drift or deviation from hardened builds/security configuration baselines must be identified, reported, and remediated.~~ • **The supplier must have malware protection mechanisms in place that protect endpoints, inbound and outbound connectivity, and email services. ~~*Preventive controls must block malicious messages and attachments as well as prevent auto- forwarding of emails. Malware protection mechanisms must exist to detect and/or prevent against malware and other threats.~~ ~~• *Malware protection mechanisms must be configured to perform real-time or scheduled scans of systems, and alert when malware is discovered.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Configuration - Continued			• *~~All devices and malware protection mechanisms must be kept up-to-date with latest anti-virus software and definitions.~~ • **The supplier must strictly separate personal email domains from corporate email domains, ensuring that all corporate actions and data are only associated with approved corporate email domains. *~~Supplier must have policies, procedures, and controls that ensure proper control of an electronic mail and/or instant messaging system that displays and/or contains JPMC information.~~ • **The supplier must implement controls to protect its infrastructure and services against distributed denial of service (DDoS) and web application attacks. • **The supplier must have controls in place to inspect and control network traffic leaving the supplier to block known malicious sites and activity. • **The supplier must log security events and feed them into a Security Event & Incident Management platform for the purpose of monitoring and alerting of suspicious cyber activity. • *~~Network devices must have internal clocks synchronized to reliable time sources.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Operations	• Enhanced requirements mandate the use of SIEM for centralized log management and threat detection, protection of log integrity, implementation of fraud and threat intelligence processes for suppliers and customers, mandatory digital forensics procedures, and regular cybersecurity exercises with stakeholder review. • Adds requirement for brand protection, governance for monitoring, and dedicated security operations function. • Removed the requirement to restrict access to non-corporate/personal email and messaging solutions, as well as the explicit obligation for notification and communication to JPMC regarding fraud and threat events.	• Change to 5 existing statements and 1 sub bullet • Added 3 new statements • Removal of 1 existing statements	• **The supplier must have a process for supporting and/or conducting forensic activities *~~Supplier should have a procedure for conducting digital forensics~~ including data collection, data/evidence preservation for future analysis, analysis, reporting of findings, and closure. • *~~A process should be~~ **The supplier must regularly conduct **cybersecurity exercises such as red teaming and social engineering **engagements to identify gaps in people, processes, and technology. Findings must be reported, reviewed and accepted by stakeholders. *~~in place to conduct attack simulations including social engineering exercises (e.g., phishing), red teaming, and tabletop exercises with appropriate reporting, remediation/acceptance, and tracking of findings.~~ • **The supplier must have a Security Information and Event Management (SIEM) system that allows for aggregation and correlation of security logs and data from multiple sources for the purpose of detecting and alerting on cyber related threats and malicious activity. *~~Security event logs from information systems must be collected, centrally managed, analyzed, and correlated for the purpose of detecting anomalous behavior that may indicate malicious events/incidents.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Security Operations - Continued			• **The supplier must have a defined retention schedule for security logs and protect the integrity of those logs. *~~Retention schedule for various logs must be defined and followed.~~` `• *~~A~~ **The supplier must have fraud and threat intelligence processes that protect the supplier and its customers from fraudulent activities and threats that might disrupt operations. *~~detection, prevention and mitigation program, processes and procedures for monitoring and reporting actual and suspected instances of fraud, and specific notification and communication, internally and to JPMC, must be established~~. • **The supplier must have a brand protection program that protects the supplier, its brands, and its customers from brand infringement activities. • **The supplier must have a governance process that ensures the effectiveness of its security monitoring processes. • **The supplier must have a dedicated security operations function that continuously monitors for cyber threats and events. • *~~Access to non-corporate/personal email and instant messaging solutions must be restricted~~.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Vulnerability Management	• Expands and clarifies the scope and structure of the program, with more detailed requirements. • Broadens identification methods and does not specify authenticated/unauthenticated scans or timing related to system provisioning. • Adds explicit use of CVSS for classification and expands prioritization to all vulnerabilities. • Adds governance and periodic evaluation of remediation effectiveness. • Adds new, detailed requirement for a formalized penetration testing program and governance. • Removes explicit requirements for scan types and timing related to system provisioning.	• Change to 4 existing statements • Addition of 1 new statements	• **The supplier must have a vulnerability management program that: • **Supports the *~~Supplier must include as part of their vulnerability management program,~~ the receipt of vulnerability related security alerts and intelligence from reputable external and internal sources to identify and monitor for vulnerabilities in their environment. *~~Vulnerability alerts are acted upon in a timely manner, and 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.~~ **Supports identification of vulnerabilities through vulnerability scanning, internal assessments, and external vulnerability identifications programs.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Vulnerability Management - Continued			• *~~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.~~ **Supports the prioritization, evaluation, and classification of all discovered vulnerabilities, including assessment of their criticality and impact based on the CVSS (Common Vulnerability Scoring System) industry standard. • **The supplier must have a vulnerability management program that: ◦ *~~Remediation actions must be documented, and their effectiveness validated through follow-up assessments.~~ **Governs the remediation of actionable vulnerabilities through a framework that also tracks and reports 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.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Vulnerability Management - Continued			- **The supplier must have a penetration testing program for the purpose of identifying security weaknesses in applications, infrastructure, and network security controls (e.g. firewall configuration, intrusion detection policies etc.). These assessments *~~Vulnerability scans (authenticated and unauthenticated) and penetration tests~~ must be performed **at defined intervals on in-scope applications, infrastructure, and network security controls. The penetration testing program must ensure the use of a standardized testing framework that incorporates industry best practices and must include a governance process which evaluates the effectiveness of the program. **~~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.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Privacy	• Adds regulatory compliance, review/update of procedures, protection of government IDs, expands scope of consent and notice	• Change to 6 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. **Ensure compliance with applicable data protection regulations and relevant local laws. • 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~~ **from such investigation. • Supplier must *~~have~~ maintain documented procedures for collecting, processing and disclosing Personal Information including any *~~restrictions imposed by law~~ legal restrictions, contractual arrangements and/or JPMC privacy policies. **Regularly review and update these procedures to reflect changes in regulations.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Privacy - Continued			• 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. **Additionally, ensure such IDs are protected from unauthorized access. • If Supplier collects Personal Information from any individual on behalf of JPMC, **including information collected via websites, Supplier must implement procedures to make *~~a~~ **the relevant JPMC privacy notice(s) available and obtain informed consent from individuals **(in line with regulatory requirements) prior to collecting Personal Information. • Provide complete and timely responses to JPMC, and take **necessary actions 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.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Development - SDLC	• No changes, retain 2024 MCR Wording	• N/A	• N/A
Technology Development – Third Party Software	• No changes, retain 2024 MCR Wording	• N/A	• N/A
Technology Operations	• Expanded the capacity management process to include planning • The change management process is enhanced to include recording as a required activity • The technology maintenance process is expanded to specify that maintenance must keep systems secure, stable, and up to date by addressing vulnerabilities, bug fixes, and feature enhancements.	• Change to 3 existing statements	• Suppliers must have a Capacity Management process documented *~~that~~ **to include **planning and monitoring of capacity headroom and performance to ensure availability; this process must be reviewed on an annual basis. • Suppliers must have a Change Management process documented *~~that~~ **to outline the planning, **recording, approvals procedure, testing, implementation, post validation, emergency change procedure, and retention of logs for audit purposes; this process must be reviewed on an annual basis. Any changes materially affecting JPMC services must be communicated to JPMC prior to implementation. • Suppliers must have a Technology Maintenance process documented for infrastructure assets *~~that~~ **to cover patch compliance and hygiene activities **to keep the systems secure, stable, and up to date by addressing vulnerabilities, bug fixes, and features enhancements. This process must be reviewed on an annual basis.

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

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Third Party Relationships	• The reference to "Minimum Control Requirements" is clarified to Supplier Minimum Control Requirements	• Change to 1 existing 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 **Supplier Minimum Control Requirements and Supplier Code of Conduct applicable to any such services.
Data Management	• Expanded scope to Highly Confidential information, clarified retention/inventory requirements • New requirements for de-identification in non-production environments and data localization and geographical compliance	• Change to 2 existing statements and 2 sub statements • Addition of 2 new 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 **C*~~c~~onfidential and **Highly Confidential information, assets, and associated services. • Business records are appropriately identified with the relevant **JPMC retention requirements. Data within such business records is **retained until the end of the retention period and then disposed of once the retention requirement has been met. • **JPMC Retention/Destruction Requirements *~~(and evidence of execution of those requirements)~~ • Use of Data **per contractual agreement *~~(and validation that it is not used beyond agreed terms)~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Data management - Continued			- **Supplier must ensure all Confidential and Highly Confidential production data is de-identified or declassified for use prior to moving it to any non-production environment (e.g., Environments used solely for the support of development, testing or evaluation of technology) - **Suppliers must have controls in place to ensure compliance with data localization laws by ensuring data is physically (original or in copy) stored within the required geographic boundaries and adheres to applicable regional or country safeguards.
Information & Technology Asset Management	- The technology asset registration policy and procedure is expanded to require maintaining a Software Bill of Materials (SBOM) for all software assets. - Removed requirements for technology asset provisioning and disposal, and secure asset transport	- Change to 1 existing statement - Removal of 2 existing statements	- Supplier must have a sufficient technology asset registration policy and procedure, including unique identifiers for all assets, appropriate classification, asset ownership, and asset location, including proper licensing and meeting all legal, regulatory, contractual, or support requirements, **and maintaining a Software Bill of Materials (SBOM) for all software assets. - *~~A technology asset provisioning and disposal program must be in place to include only procuring technology assets from appropriately sourced suppliers and disposing of/removing/deleting all technology assets in a secure manner when they reach end of life.~~ - *~~Supplier must ensure assets are transported in a secure manner.~~

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Incident and Event Management	- Expands scope to explicitly include "Technology and Cyber" incidents, clarifies prioritization, and adds data loss tracking. - Removed statement for security event/incident response policy and procedure	- Change to 3 existing statements - Removal of 1 existing statements	- Suppliers must have an Event Management process documented **to *~~that~~ ensure anomalous events are monitored, detected, analyzed and actioned for all production and disaster recovery applications and infrastructure. This process must be reviewed on an annual basis. - Suppliers must have a Problem Management process documented **to *~~that~~ ensure root cause analysis is performed for all incidents impacting production and disaster recovery applications and infrastructure, with permanent fixes implemented and reoccurrences of incidents minimized; this process must be reviewed on an annual basis. - Suppliers must have *~~an~~ **a Technology and Cyber Incident Management process documented that includes incident tracking, reporting, *~~classification,~~ prioritization **of incident response based on classification, internal escalation, remediation, *~~and~~ preservation of data, **and data loss tracking (if any) for all incidents impacting production and disaster recovery applications and infrastructure; this process must be reviewed on an annual basis. Supplier must notify and engage JPMC in compliance with the contract or applicable local regulations, if services to JPMC or JPMC data is impacted.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Incident and Event Management - Continued			• *~~Supplier must have a security event/incident response policy and procedure.~~
Business Resiliency	• Broader coverage for recovery planning and testing, not limited to listed categories. • Clarifies focus on effectiveness and execution. • Expands testing to all supporting elements, clarifies considerations for testing environments and recovery demonstration. • New requirement for comprehensive coverage in resiliency planning and testing.	• Change to 3 existing statements and 1 sub statement • Addition of 1 new statements and 6 sub statements	• 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 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 **service disruption caused by the following: • Disruption to **A*~~a~~pplication(s) • **Disruption to any other supporting elements required for providing services to JPMC • Supplier *~~I~~**identified significant deficiencies/failures/limitations **in their Recovery capabilities must be communicated to JPMC in a timely manner. • Supplier must *~~conduct~~ test*~~ing~~ of the effective**ness *~~operation of avenues~~ of **their communication **protocols to **contact all personnel and subcontractors associated with *Supplier recovery plans and **execution of Supplier planned recovery strategies *~~at~~ on a regular basis.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency - Continued			• Supplier must *~~conduct~~ test*~~ing~~ **all *of their planned Recovery Strategies to address disruption to **the services provided *~~assets upon which the Supplier depends to provide services ~~to JPMC. Testing must be conducted on a risk-based frequency**, and as a minimum include all planned Recovery Strategies related to service disruption caused by the following *~~by the Supplier for Site and Staff disruption, which at a minimum must~~: • **Disruption to Supplier Staff (*) • **Disruption to Supplier Site(s) (*) • **Disruption to Supplier Application(s) • **Disruption to Supplier sub-contractors • **Disruption to any other supporting elements required for providing services to JPMC (*) Considerations should encompass conducting tests on a production day or in production-like environments, and demonstrating recovery within established RTOs and service level requirements • *~~Supplier must test its planned recovery strategies for Site and Staff disruption on a risk-based frequency, and which at a minimum must:~~

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

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Business Resiliency - Continued			- *~~Be conducted on a production day or production like condition by the Supplier staff that provide the in-scope services to JPMC.~~ - *~~Demonstrate that the in-scope Supplier processes tested recover within the established RTOs and service level expectations (as defined in the relevant contracts).RTO established by the relevant LOB or CF that has contracted the service(s).~~ ● **Subcontractor disruption: - 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.

* Indicates the removal of wording

** Indicates the addition of wording

Supplier Minimum Control Requirements – 2025 Updates

Section 2: Changes to Specific Control Domains

Control Domain	Summary of Change	Subject of Change	Description
Technology Resiliency	- Expanded recovery planning to explicitly include data loss tolerance	- Change to 1 existing statements	- Identified resources and specific actions required to help minimize losses **(including data loss tolerance) in the event of a disruption to services provided to JPMC or resources supporting those services.
Organizational Security	- No changes, retain 2024 MCR Wording	- N/A	- N/A
Customer Contact	- No changes, retain 2024 MCR Wording	- N/A	- N/A

* Indicates the removal of wording

** Indicates the addition of wording