Comment Template for: NIST SP 800-63-4 Suite (Second Public Draft)

Please submit responses to dig-comments@nist.gov by October 7, 2024.

Organization:	*Kaspersky*
Name of Submitter/POC:	*Jochen Michels*
Email Address of Submitter/POC:	[redacted]

Comment #	Publication (Base, 63A, 63B, 63C)	Section	Page #	Line #	Comment (Include rationale for comment)	Suggested Change
1	63-Base	3.1	27	1075	It is crucial for RPs to include an assessment of the risks associated with third-party components, services, or vendors integrated into their identity systems when developing a comprehensive description of their online services. The potential vulnerabilities introduced by these external dependencies can significantly impact the overall security posture of the system.	Add an element to the list: "Description of all third-party components, services, or vendors integrated into their identity systems"
2	63-Base	3			Based on the company's experience in developing anti-theft solutions and protecting customers worldwide, we recommend including two additional controls in section 3: (1) Anomaly detection (2) Audits of third-party suppliers to ensure the implementation of their cybersecurity measures	Add the following control into the document: (1) Implement systems capable of detecting anomalous synchronization patterns that may indicate fraudulent activities. By continuously monitoring and analyzing authentication processes, organizations can identify abnormal behaviors, such as unusual login locations or frequency of synchronization requests, which may signal a potential compromise or fraud. (2) To ensure the integrity and compliance of third-party providers involved in the system, regular security assessments should be conducted by independent auditors. This ensures that all third-party providers adhere to the required security standards and guidelines, mitigating the risks introduced through external dependencies.