Useful step, but the template should be more clearly need-to-know. As drafted, Fields 51, 63 and 75 can push controllers to disclose mechanism-level details: how a breach was detected, which systems and software were involved, where infrastructure is located, and what security controls were in place. That may go beyond what a DPA needs to assess risk and response, and it can create avoidable exposure if the notification is shared more widely. Please add stronger abstraction, clearer confidentiality safeguards, and guidance that allows functional reporting rather than architectural blueprints. This would better fit GDPR Art. 5(1)(c) and Art. 32, and align with the spirit of ISO/IEC 29100, ISO/IEC 29134 and ISO/IEC 27561 (POMME).