From: Andrew Freund ████████████████████████████████
Date: Tuesday, August 23, 2022 at 1:14:04 PM UTC-4
Subject: Feedback on 03.03.04
To: 800-171comments@list.nist.gov <800-171comments@list.nist.gov>

Hi NIST,

Below are some comments on NIST 800-171 Security Requirement 03.03.04.

Please don't hesitate to reach out if you have any questions.

NIST 800-171 Rev 2 Requirement 03.03.04 is the same requirement as NIST 800-53 Rev 5 AU-05 (a), once you remove the parameter inserts from AU-05 (a) and the word 'within'. Despite that, NIST 800-171a Rev 2 contains an assessment objective (03.03.04[b] - types of audit logging process failures for which alert will be generated are defined) that NIST 800-53a Rev 4 & 5 doesn't contain. In doing so, this make the assessment objectives for NIST 800-171 Rev 2 Requirement 03.03.04 more stringent than NIST 800-53 Rev 5 AU-05 (a).

Below are some potential options to resolve the discrepancy and make the assessment objectives consistent

**Option 1**

Update NIST 800-53a AU-05 to include NIST 800-171a Rev 2 assessment objective 03.03.04[b].

AU-05                Determine if:

AU-05_ODP[01]          personnel or roles receiving audit logging process failure alerts are

defined;

AU-05_ODP[02]        types of audit logging process failures for which alert will be generated are defined;

AU-05_ODP[03]        time period for personnel or roles receiving audit logging process failure alerts is defined;

AU-05a.        <AU-05_ODP[01] personnel or roles> are alerted in the event of an <AU-05_ODP[02] audit logging process failure> within <AU-05_ODP[03] time period>;

**Option 2**

Update NIST 800-171a and remove assessment objective 03.03.04[b].

03.03.04        Determine if:

03.03.04[a]        personnel or roles to be alerted in the event of an audit logging process failure are identified.

03.03.04[b]        identified personnel or roles are alerted in the event of an audit logging process failure.

Cheers,

**Andrew Freund**

**Founder & CEO**