When a failed health check was marked successful, what remained untested?

New York Stock Exchange | United States | Trading-system disruption 2023 | SEC order 2026

MISSING OPENING AUCTIONS	LULD PAUSES	TRADES BUSTED	SEC PENALTY
2,824 securities	**84 securities**	**More than 4,000**	**$9 million**
S01	S01	S01	S01

DOCUMENTED EVENT

During planned maintenance on 23 January 2023, NYSE staff mistakenly ran shutdown commands against an already-shut production system, leaving the Pillar disaster-recovery system active. A health check against Pillar DR failed because maintenance was incomplete and the DR system was still operating. The SEC order finds that staff investigated only the first reason and manually marked the failed check as successfully resolved without full investigation, escalation or supervisory approval. Data from the still-active DR system later returned through market-data infrastructure and caused production to treat opening auctions as completed for 2,824 securities. NYSE issued a 'STATUS: NORMAL' update at 9:48am and did not identify missing auctions until about 10:09am. The event led to 84 trading pauses and more than 4,000 busted trades. The SEC imposed a $9 million penalty. [S01]

NFRISK SCENARIO ADAPTATION - NOT AN EXTERNAL FINDING

A disaster-recovery environment is activated for maintenance. Its automated health check fails for more than one reason, but staff explain the familiar exception, manually mark the control successful and proceed. The backup environment remains active and sends state data that production trusts. Dashboards show components as available, while no control verifies whether the critical business outcome - a complete opening, settlement, calculation or customer process - actually occurred.

STRESS-TEST QUESTIONS

01 Can a failed automated control be manually marked successful, and what evidence and second-line approval are required before that override?

02 What control confirms that recovery environments are inactive and cannot send authoritative state into production after tests or maintenance?

03 Do monitoring procedures verify completion of the critical business process, or only component availability and job status?

04 How quickly would abnormal outcomes overturn a 'normal' systems assessment, and who can declare the original assessment unreliable?

CONNECTED RISK

Operational Resilience (primary)
Data & Control Integrity (contributing)
Technology & Change Risk (contributing)

FRAMEWORK RELEVANCE

Regulation SCI lens: monitor critical systems for potential SCI events
The SEC found that NYSE's written policies and procedures did not establish monitoring to determine whether opening auctions had occurred, as required for SCI systems supporting the opening of trading. [S01]

SEC order: outcome monitoring and controlled override
The order records remedial measures including monitoring whether auctions ran, a second approval before a failed health check can be marked successful, and controls to confirm the DR environment is inactive. [S01]

NFRISK PRACTITIONER INTERPRETATION

A control result should not be converted from failed to passed by narrative alone. Overrides need complete causal investigation, independent approval and evidence that every failed condition has cleared. Resilience monitoring must also verify business outcomes, not only component health. A technically available system can still omit the process it exists to perform, and authoritative state can be corrupted when recovery and production environments share uncontrolled feedback paths.

PRIMARY-SOURCE REGISTER

S01 US Securities and Exchange Commission (2026)
In the Matter of New York Stock Exchange LLC, Release No....

EVIDENCE BOUNDARY Official findings are separated from the institutional scenario, framework interpretation and NFRisk practitioner view.