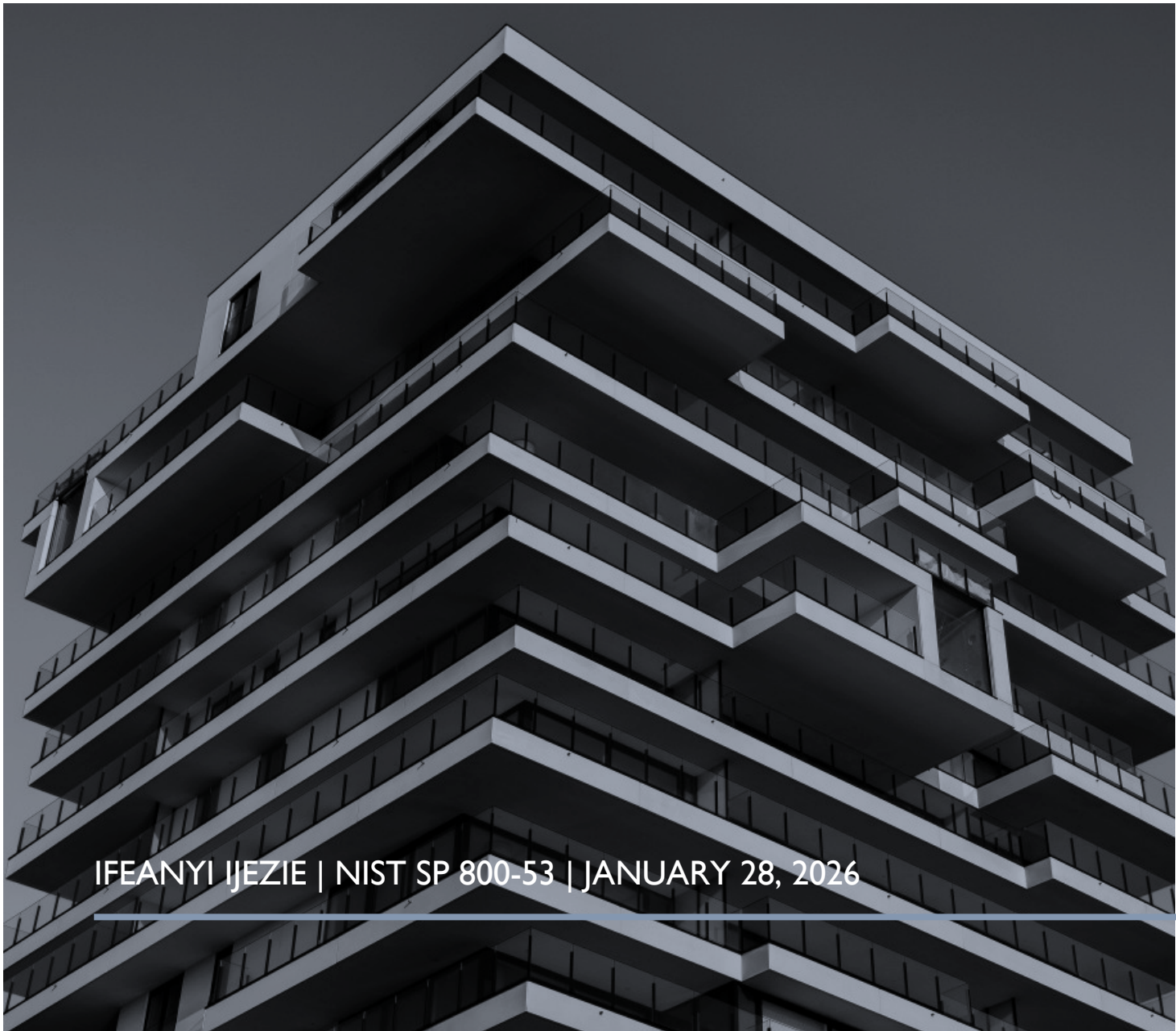
SCENARIO-BASED CYBER RISK ANALYSIS

PRIVILEGED ACCOUNT ABUSE



IFEANYI IJEZIE | NIST SP 800-53 | JANUARY 28, 2026

EXECUTIVE SUMMARY

This scenario-based cyber risk analysis evaluates the potential impact of privileged account abuse resulting from excessive permissions, inadequate oversight, or credential compromise. The analysis traces how misuse of elevated access could lead to unauthorized system changes, data exposure, operational disruption, and regulatory risk. Using a NIST-aligned quantitative risk model, the scenario was assessed as high impact with a moderate likelihood, resulting in a catastrophic inherent risk rating. The findings highlight weaknesses in access governance, privileged account monitoring, and enforcement of least-privilege principles. Based on the analysis, mitigation through strengthened access controls, regular access reviews, and enhanced monitoring is recommended to reduce the likelihood and duration of privileged account misuse.

SCENARIO OVERVIEW

This scenario evaluates the risk of privileged account misuse resulting from excessive permissions, inadequate oversight, or credential compromise. Privileged accounts provide elevated access to critical systems and data, making them a high-value target for attackers and a significant internal risk if misused. The objective of this analysis is to assess how improper management of privileged access could lead to unauthorized system changes, data exposure, or operational disruption. This scenario reflects a realistic threat affecting organizations with complex IT environments and limited access governance.

THREAT PATHWAY

A privileged user account is granted broad system access without adequate review or monitoring. Credentials for the account are either compromised through credential reuse, malware, or insider misuse. The attacker or insider uses the elevated privileges to access sensitive systems, modify configurations, disable logging, or exfiltrate data. Due to limited monitoring of privileged activity, the misuse is not immediately detected, increasing the duration and impact of the incident.

ASSETS AND DATA AT RISK

- Administrative and privileged user accounts
- Core production systems
- Sensitive customer and financial data
- Security configurations and audit logs
- Business-critical applications

(All assets above are foundational to business system confidentiality, integrity, and availability).

IMPACT ANALYSIS

Under the defined impact scale, a rating of 5 (Catastrophic) represents events that cause widespread operational disruption, significant financial loss, regulatory exposure, and long-term reputational damage. Abuse of privileged access could enable attackers to manipulate systems, disable security controls, access sensitive data, or disrupt critical services across the organization. Such an event would likely require extensive remediation efforts and could undermine customer and stakeholder trust. Based on these factors, the inherent impact of this scenario is assessed as Catastrophic (5).

LIKELIHOOD ANALYSIS

Likelihood is assessed on a five-point scale ranging from Low (1) to High (5). While privileged account abuse occurs less frequently than common threats such as phishing, it remains a credible risk in environments lacking formal access reviews, strong privileged access governance, and continuous monitoring. Given the presence of baseline access controls but gaps in oversight and detection, the likelihood of this scenario occurring is assessed as Medium (3).

RISK SCORING (INHERENT)

		Impact				
		5 Catastrophic	4 Significant	3 Moderate	2 Mild	1 Insignificant
Likelihood	1 Low	5 Moderate	4 Moderate	3 Low	2 Low	1 Low
	2 Low-Medium	10 High	8 High	6 Moderate	4 Moderate	2 Low
	3 Medium	15 Catastophic	12 High	9 High	6 Moderate	3 Low
	4 Medium-High	20 Catastophic	16 Catastophic	12 High	8 High	4 Moderate
	5 High	25 Catastophic	20 Catastophic	15 Catastophic	10 High	5 Moderate

Using the organization defined five-by-five impact and likelihood matrix, the inherent risk score for this scenario was calculated based on an impact rating of 5 (Catastrophic) and a likelihood rating of 3 (Medium). According to the matrix, this results in an inherent risk score of 15, which is classified as Catastrophic. This risk level indicates that privileged account abuse represents a significant threat to the organization and requires prioritization at a senior management level.

RISK TREATMENT OPTIONS

Potential risk treatment options for this scenario include:

- Implementing least-privilege principles for all privileged accounts
- Establishing formal privileged access reviews and approval workflows
- Monitoring and alerting on privileged account activity
- Implementing multi-factor authentication for privileged access
- Accepting residual risk following control implementation

(These options primarily reduce the likelihood of misuse and improve detection capabilities).

RECOMMENDED DECISION

The recommended risk treatment strategy is Mitigation. Enforcing least privilege, conducting regular access reviews, and monitoring privileged activity significantly reduce the likelihood and duration of privileged account abuse while maintaining operational effectiveness. Residual risk should be monitored through ongoing review of privileged access metrics and alerts for anomalous activity. This approach aligns risk reduction efforts with organizational risk tolerance and governance expectations.