Risk Assessment Guide Adapted from NIST SP 800-53: AC-6

v1.0.1

Author:

Eldon Gabriel

July 11, 2025

TABLE OF CONTENTS

REVISION HISTORY

Version	Date	Author	Description of Changes
v1.0.0	02/22/2025	Eldon G.	Initial draft.
v1.0.1	07/11/2025	Eldon G,	Added Section 2.0: Conclusion and Key Takeaways.

Disclaimer: This document is adapted from NIST SP 800-53 AC-6. The original publication is publicly available from the National Institute of Standards and Technology (NIST).

SECTION 1.0: RISK ASSESSMENT GUIDE

Adapted from NIST SP 800-53 AC-6

1.1 Overview

The principle of least privilege (PoLP) requires that users, systems, and applications be granted only the minimum level of access necessary to perform their job functions. Implementing least privilege reduces the risk of unauthorized access, data breaches, and insider threats.

1.2 Control Objectives

- Ensure access is restricted based on user roles and responsibilities.
- Limit administrative privileges to authorized personnel only.
- Regularly review and adjust access controls as needed.

1.3 Implementation Guidelines

- **Role-Based Access Control (RBAC):** Assign access permissions based on predefined roles within the organization.
- **Separation of Duties:** Ensure that critical functions are divided among multiple individuals to prevent conflicts of interest.
- **Privileged Account Management:** Restrict the number of privileged accounts and implement multi-factor authentication (MFA) for elevated access.
- **Access Reviews:** Conduct periodic reviews of user access rights and revoke unnecessary permissions.
- **Logging and Monitoring:** Implement continuous monitoring of access logs to detect unauthorized or suspicious activity.
- **Just-In-Time (JIT) Access:** Use time-bound access permissions to grant privileges only when necessary.

1.4 Risk Considerations

- **Failure to enforce least privilege** can lead to unauthorized access and data exfiltration.
- **Excessive privileges** increase the attack surface, making systems more vulnerable to exploitation.
- **Lack of monitoring** may result in undetected security incidents.

1.5 Compliance Requirements

Organizations must ensure adherence to regulatory frameworks such as:

- **NIST SP 800-53:** AC-6
- **ISO/IEC 27001:** Access control policies
- **PCI DSS:** Restricting access based on business need-to-know

SECTION 2.0: CONCLUSION

2.1 Key Takeaways

- The Principle of Least Privilege (PoLP) minimizes security risks by limiting user access to only what is necessary.
- Using RBAC, MFA, access reviews, and monitoring strengthens access control.
- Excessive privileges and unused accounts open doors for attacks.
- Regular audit checks and setting time limits on access help enforce least privilege consistently.
- Following NIST SP 800-53 AC-6 helps keep a strong, regulatory-aligned security posture.