REZONATE

100 Breakthrough Prompts for Your Best User Access Review

User access reviews are vital for maintaining robust identity security and ensuring compliance across your cloud and SaaS environments. With the growing complexity of managing identities—both human and machine—security teams must continuously monitor and validate access to minimize risks like access creep, orphaned accounts, and unauthorized privileges.

Whether you're preparing for an audit or enhancing your organization's security posture, these 100 prompts will guide you through every aspect of access management. From admin privileges and authentication policies to managing OAuth tokens and service accounts, this checklist covers all the essentials to consider during a comprehensive user access review.

rezonate.io

Critical Access Basics

1 Who currently has admin or privileged access?

2 Are all administrators still in their roles, and do they require elevated access?

3 Are there any accounts with admin privileges that haven't been used in the last 90 days?

4 Do all users have access that matches their job responsibilities?

5 Which users have permissions exceeding their role requirements (access creep)?

6 Where are the inactive accounts?

7 Are there orphaned accounts from former employees that need removal?

8 Do contractors or third-party users still have active access?

9 Have temporary access accounts and privileges been deprovisioned after the allotted time?

10 What is your process for role changes and corresponding access adjustments?

Authentication and Authorization

11 Is Multi-Factor Authentication (MFA) enforced across all critical applications?

12 Are password policies strong and consistent across SaaS apps and cloud platforms?

13 Are there any users logging in from suspicious or unusual locations?

14 When was the last time this user's access was reviewed? By whom?

15 Are SSO (Single Sign-On) systems properly configured for all authorized applications?

16 Is least privilege being applied to all user accounts?

17 Are API keys restricted to the correct users and applications?

18 Are there expired API tokens or service accounts in use?

19 How frequently are authorization policies reviewed and updated?

20 Is there a clear process for deprovisioning unused access and accounts?

Identity Management

21 Are identity providers like Okta, Entra ID, or Google Workspace configured for automatic provisioning and deprovisioning?

22 How is user identity lifecycle management handled across platforms?

23 Are there any duplicate or conflicting user identities in different systems?

24 Are all identity policies aligned with company policies and regulatory requirements?

25 Are service accounts tied to specific identities, and are they necessary?

26 Are there any users with conflicting or overlapping roles?

27 Are shared accounts still in use? If so, why?

28 Are user profiles up to date and synchronized between cloud platforms and SaaS apps?

29 Are user groups and roles consistently applied across cloud and SaaS platforms?

30 How often are role memberships reviewed and updated?

Privileged Access Management (PAM)

31 How are privileged accounts monitored for excessive or suspicious activity?

32 Are privileged access accounts configured with least privilege?

33 Are there any dormant privileged accounts?

34 Is there a process for reviewing privileged access accounts regularly?

35 How is emergency access (break-glass accounts) managed and audited?

36 Which privileged accounts are not secured with MFA?

37 Are all privileged access sessions logged and monitored?

38 How are root access privileges handled in cloud environments?

39 Is there any privileged access that can be revoked or downgraded?

40 Are there any instances where privileged access is over-provisioned?

SaaS App Access Review

41 Are users provisioned directly into SaaS apps, or do they use SSO?

42 What user roles are currently assigned in each SaaS app?

43 Are there any active accounts that belong to former employees or contractors?

44 Are the roles defined in SaaS apps consistent with security policies?

45 Are there any users with custom permissions outside of standard roles?

46 How is access to sensitive data in SaaS apps restricted?

47 Do any SaaS apps allow broad, unrestricted access to internal or external users?

48 How often are access permissions reviewed for each SaaS app?

49 Are user access logs regularly reviewed in SaaS apps for anomalies?

50 Is access to SaaS app admin panels limited to necessary personnel only?

Machine Identity Access Review

51 How are OAuth tokens managed, and are they set to expire after appropriate time frames?

52 Are there any unused or stale service accounts that need deprovisioning?

53 Do service accounts follow the principle of least privilege?

54 How frequently are access keys and API tokens rotated?

55 Are API tokens tied to specific identities or applications to prevent misuse?

56 Are there any hard-coded credentials in applications or scripts that need removal?

57 How are secrets (e.g., API keys, and passwords) stored securely across platforms?

58 Are machine identities monitored for unusual access patterns or misuse?

59 Is there a process in place to automatically revoke or rotate compromised keys?

60 Are audit logs capturing all activities performed by service accounts and machine identities?

Policy Violations and Compliance Issues

61 Are all access management policies aligned with regulatory requirements (e.g., GDPR, HIPAA)?

62 Are there any instances of unauthorized access to sensitive systems?

63 How are access violations detected and reported?

64 Are there any access exceptions that need to be documented for audit purposes?

65 Are automated tools in place to flag policy violations in real time?

66 Are role-based access policies compliant with internal and external regulations?

67 How often are access control policies reviewed and updated to meet compliance?

68 Is there a clear audit trail for all access and privilege changes?

69 How are exceptions to access policies handled and reviewed?

70 Are any regulatory controls (e.g., SOX, PCI DSS) being violated with current access practices?

Access Creep and Orphaned Accounts

71 Are there any accounts that have gradually accumulated more permissions over time (access creep)?

72 Are user roles being reviewed to ensure access creep is prevented?

73 Are there orphaned accounts belonging to former employees or unmonitored systems?

74 How are orphaned accounts identified and removed from all platforms?

75 Are there any SaaS apps or cloud resources that have been accessed by users who no longer need them?

76 Are access reviews happening frequently enough to detect access creep?

77 Is there a process in place to handle accounts with minimal activity?

78 How are service accounts monitored for potential orphaned access?

79 Are orphaned accounts reported and flagged for immediate remediation?

80 Is there a formal review process to ensure old accounts don’t accumulate excessive permissions?

Audit Trail and Logging

81 Are all access changes logged with user identity and timestamp?

82 Are audit logs regularly reviewed for suspicious access changes?

83 Are access requests, approvals, and denials clearly documented?

84 How are access logs maintained to ensure audit readiness?

85 Are audit logs stored securely and accessible only to authorized personnel?

86 Is there a process in place to identify access pattern anomalies?

87 Are logs centralized from all SaaS apps and cloud platforms for consistent review?

88 How long are access logs retained to meet audit and compliance requirements?

89 Are access logs configured to capture all relevant events (e.g., login attempts, permission changes)?

90 How is access log integrity ensured across platforms?

Automating Access Reviews

91 Are there automated tools in place to review and report on user access?

92 How are automated workflows configured for access reviews?

93 Are automated access review reports consistent with company policies?

94 Do automated systems have proper triggers for deprovisioning orphaned accounts?

95 Is automated provisioning and deprovisioning being leveraged for all cloud and SaaS apps?

96 Can remediation be triggered or remediated during an access review project?

97 Are there automated alerts for access policy violations?

98 How often are automated access review tools tested for effectiveness?

99 Are privileged access reviews automated to ensure least privilege?

100 How does automation handle misconfigurations in cloud or SaaS access controls?

REZONATE

Simplify Your Access Reviews with Rezonate

Conducting a user access review can be time-consuming and complex, but it doesn't have to be. These 100 prompts help you identify critical gaps in identity management, privileged access, and machine identities, ensuring you stay compliant and secure.

With Rezonate, you can automate these reviews and gain full visibility into all identities. Plus, you can leverage Zoe, Rezonate's AI identity security assistant, to get actionable insights in minutes and ensure your access management aligns with best practices. Stay ahead of access risks and streamline compliance with Rezonate. Learn more about Rezonate's access review capabilities here.

Learn more at rezonate.io