Access and Network Hardening Priorities

Example report

Kit Baroness | Security analysis example

Decision summary

The supplied risk assessment identifies four conditions: shared passwords, a default database administrator password, missing multifactor authentication (MFA), and firewalls without traffic-filtering rules. My analysis recommends three coordinated treatments: improve account and credential controls, introduce MFA, and define and maintain firewall policy.

The business concern is unauthorized access to accounts or data, with possible disruption to dependent services. These are exposure findings, not evidence that an intrusion occurred. The source contains recommendations; configuration exports, account inventories, activity logs, and completed tests were not supplied for independent verification.

Findings and risk reasoning

References below identify the supplied assessment and its recommendation sections.

Finding and reference	Risk scenario	Treatment
RISK-01 / R-S1: shared and default credentials	A known password or use of another person's credential could provide access while weakening accountability.	Replace the known default credential, establish individual accounts, and remove shared interactive access after dependencies are reviewed.
RISK-02 / R-S2: no MFA	A compromised password could be sufficient to access an important account.	Introduce MFA through a supported access path, beginning with privileged and externally accessible accounts.
RISK-03 / R-S3: no filtering rules	Unnecessary network communication could reach systems or services.	Define required traffic by service and direction, then implement and maintain the corresponding rules.

These priorities sequence treatment based on the exposure described. They are not numerical likelihood or loss estimates. A scored assessment requires an agreed rating method, asset scope, existing safeguards, and evidence about likelihood and impact; those inputs remain to be established.

Proposed delivery and acceptance

Proposed roles require assignment. No implementation or test below is recorded as complete.

Work package	Proposed owner	Observable completion condition
Correct credential and account exposure.	Identity and database owners	Default access no longer succeeds; authorized individual access works; required service dependencies remain functional.
Introduce MFA for the agreed account scope.	Identity owner	Approved users can complete sign-in; the tested password-only path is denied; recovery and emergency access are checked.

Work package	Proposed owner	Observable completion condition
Establish firewall rules for required traffic.	Network owner	Permitted service flows succeed, prohibited flows are denied, and monitoring records the expected results.

Each change needs a recorded before-state, a controlled deployment sequence, and a way to restore service if validation fails. Review the effective outcome, including inherited access or alternate access paths, rather than relying on the presence of a configured setting alone.

Remaining exposure and follow-through

The system owner should agree the scope, accountable roles, and delivery order. Any deferred treatment should have a reason, compensating measure, review date, and owner for the remaining exposure.

Replacement of a default password does not by itself establish that previous access was legitimate. MFA and network filtering also require review as accounts, applications, and traffic requirements change. Closure requires retained test results, service-owner acceptance, and a recorded decision on any unresolved findings.

Reference method

Risk reasoning follows NIST SP 800-30 Rev. 1. Control selection and validation can be tailored using NIST SP 800-53 Rev. 5 and SP 800-53A Rev. 5; a mapping alone does not demonstrate implementation or effectiveness.

https://doi.org/10.6028/NIST.SP.800-30r1

https://doi.org/10.6028/NIST.SP.800-53r5

https://doi.org/10.6028/NIST.SP.800-53Ar5