Public■Facing Database Vulnerability Assessment (NIST SP 800■30 Rev. 1)

Executive Summary

This assessment evaluates the risks introduced by an e■commerce company’s database server that has been publicly accessible on the internet for three years. The database supports globally distributed, remote employees who routinely query customer prospect data. Public exposure significantly increases the attack surface and the likelihood of data exfiltration, service disruption, or integrity loss. Using NIST SP 800■30 Rev. 1, I identified credible threat sources and events, estimated likelihood and impact, and proposed prioritized, actionable controls to remediate and mitigate the risk while preserving business objectives.

System Description & Scope

The information system consists of a remotely hosted database server (PaaS/IaaS) queried by employees over the public internet. Components include the DB instance, administrative console, application users, network ingress/egress rules, and supporting identity services. In scope for this assessment are risks to the confidentiality, integrity, and availability of data on the database server and its management plane. Physical data center security and non■database internal IT assets are out of scope.

Purpose

The purpose of this assessment is to quantify and communicate risks associated with operating a business■critical database that is reachable from the public internet. The database underpins customer acquisition workflows and contains sensitive prospect and potentially customer■identifiable information. A compromise would degrade trust, impair revenue operations, trigger legal/contractual exposure, and disrupt remote employee productivity. Securing this asset aligns directly with business goals: protecting customer data, meeting compliance expectations, and ensuring reliable global access.

Threat Sources & Threat Events

Based on NIST SP 800■30 Rev. 1, the following credible threat sources and corresponding threat events were selected for risk estimation. Each entry includes a qualitative likelihood (1–3) and severity (1–3), with overall risk = likelihood × severity.

Threat Source	Threat Event	Likelihood (1–3)	Severity (1–3)	Risk (L×S)	Rationale (summary)
External cybercriminals scanning internet-exposed services	SQL injection / unauthorized queries leading to bulk data exfiltration	3	3	9	Public exposure + internet■facing que
Insider (malicious or negligent) or compromised employee	Abuse of excessive privileges to modify or export sensitive records	2	3	6	Remote access with weak IAM and br
Opportunistic attackers / botnets	Denial■of■Service (DoS) against the DB endpoint or management API	2	2	4	Public endpoints are discoverable and

Approach (Qualitative Risk Estimation)

I performed a qualitative assessment per NIST SP 800■30 Rev. 1, selecting threat sources/events with clear feasibility and business impact given a publicly reachable database. Likelihood reflects exposure (open internet surface, common weaknesses such as SQLi, credential reuse) and observed attacker behaviors. Severity considers data sensitivity, regulatory impact, operational dependency, and reputational damage. Prioritization favors high■impact exfiltration and integrity risks over transient availability loss.

Remediation & Mitigation Strategy

To reduce risk rapidly while maintaining productivity, implement the following controls (defense■in■depth) aligned to the identified threats: • **Eliminate public exposure**: place the database on private networking only (VPC/subnet), restrict ingress via firewall/ security groups, and require access through a company VPN, ZTNA, or IP allow■listing. • **Harden authentication & authorization**: enforce SSO with MFA; apply least■privilege IAM roles and row/column■level security; rotate credentials and disable shared accounts. • **Application & query security**: mandate parameterized queries/ORM, deploy a WAF with SQLi rules, and sanitize inputs; validate DB configuration baselines and patch regularly. • **Data protection**: encrypt data at rest with KMS■managed keys; require TLS 1.2+ in transit; implement robust backup/ restore with periodic recovery testing (RPO/RTO targets). • **Monitoring & response**: enable audit logging for queries/privileged actions; stream to a SIEM for alerting on anomalous access, large exports, or mass updates; define escalation runbooks. These measures directly address the top■ranked risks (exfiltration and unauthorized modification) and materially reduce the attack surface and blast radius.

Prioritized Implementation Roadmap

1) **Immediate (0–2 weeks)**: remove public ingress; enable MFA/SSO; rotate DB credentials; enforce TLS; start audit logging. 2) **Near■term (2–6 weeks)**: implement IP allow■list/VPN or ZTNA; least■privilege roles; WAF with SQLi rules; backups with encryption and tested restores. 3) **Mid■term (6–12 weeks)**: parameterize all queries; baseline hardening and automated patching; SIEM detections and playbooks; periodic access reviews and secret rotation cadence.

Key Takeaways

Running a business■critical database on the open internet creates unacceptable exposure. A qualitative NIST■aligned assessment shows the highest risks stem from data exfiltration and unauthorized modification, both with severe business impact. Practical network isolation, strong IAM, secure coding, encryption, and continuous monitoring provide a clear path to risk reduction while preserving distributed employee access.